
36th Annual
National CLE Conference®
Intellectual Property



The nonprofit educational arm of the
Colorado and Denver Bar Associations

36th Annual National CLE Conference®

Intellectual Property

Published by:

CONTINUING LEGAL EDUCATION IN COLORADO, INC.

1900 Grant Street, Suite 300
Denver, Colorado 80203-4301

Phone: (303) 860-0608

Toll free: (888) 860-2531

Fax: (303) 860-0624

E-mail: cle@cobar.org

Web site: www.cobar.org/cle

Continuing Legal Education in Colorado, Inc. (CLECI) publications are intended to provide current and accurate information about the subject matter covered and are designed to help attorneys maintain their professional competence. Publications are distributed with the understanding that CLECI does not render any legal, accounting, or other professional service. No representation or warranty is made concerning the application of the legal or other principles discussed by the authors to any specific fact situation, nor is any prediction made concerning how any particular judge or other official will interpret or apply such principles. The proper interpretation or application of the principles discussed is a matter for the considered judgment of the individual legal practitioner, and CLECI disclaims all liability therefore. As with any legal textbook or other secondary authority, attorneys dealing with specific legal matters should also research fully current, primary authorities.

©2019 by Continuing Legal Education in Colorado, Inc. All Rights Reserved. No part of this publication may be reproduced in any form or by any process without permission in writing from Continuing Legal Education in Colorado, Inc.

IRS CIRCULAR 230 NOTICE. To ensure compliance with requirements imposed by the IRS, unless specifically indicated otherwise, any tax advice contained within this manual was not intended or written to be used, and cannot be used, for the purpose of (i) avoiding tax-related penalties under the Internal Revenue Code, or (ii) promoting, marketing, or recommending to another party any tax-related matter addressed herein.

Source Code: LEI-IP010219L

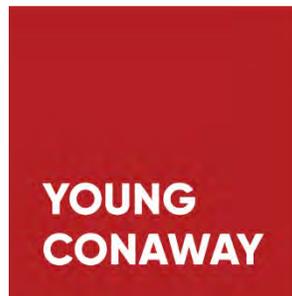
36th ANNUAL NATIONAL CLE CONFERENCE

SPECIAL THANKS TO OUR 2019 SPONSORS

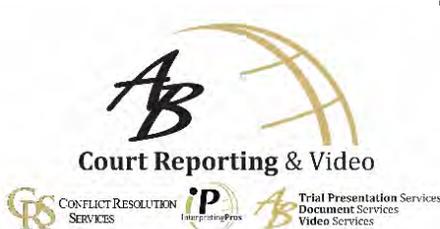
PLATINUM



GOLD



SILVER



FINNEGAN



THE EXPERTS
Robson Forensic



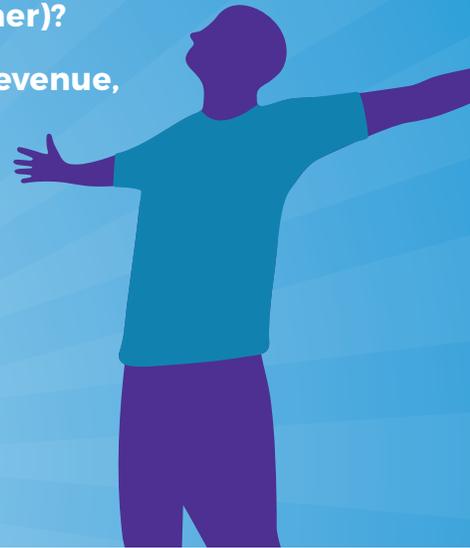


Do you want your Law Firm to give you **FREEDOM?**

30 consecutive days away from working in your Business?

More than \$1.5MM in Gross Revenues (per owner)?

A team that's got your back, bringing you more revenue, more profit, more clients, and more peace of mind while you're away?



Welcome to the National CLE Conference! The PREP ACADEMY is a service of How to Manage a Small Law Firm. Attendees in our track will learn how to step beyond the job they have built for themselves, and achieve FREEDOM in their law firm.

We welcome all attendees to come to one, or all, of our sessions! Fair warning, though ... in past years those who have come, have been reluctant to leave! Our message, our teaching, and our proven success with law firms across the United States are compelling. Previous attendees have made dramatic changes to their businesses, and their lives after attending our sessions and working with us.

IF YOU ARE YOU A LAW FIRM OWNER WITH A PRACTICE THAT IS

- ➔ Running without proper systems for your staff to follow?
- ➔ Does not have consistent, predictable revenues?
- ➔ Has insufficient financial controls in place?
- ➔ **And/or is making you feel like you are stuck?**

THEN THIS PROGRAM WAS DESIGNED FOR YOU

The Academy leads the way to FREEDOM for law firm owners, across the country, in just 18-30 months (or less, for many of the lawyers in our program).



Through a curriculum of tried and tested strategies and tools, members of the Academy build, one block at a time, the systems and structure you need to achieve a business that gives the Freedom you dream of.

During this week, we will teach you everything law school didn't - about owning a business that actually works for YOU, instead of working in a business that owns you.

WELCOME TO THE 36TH ANNUAL CONFERENCE!

About Us

Young Conaway's clients range from national and international corporations to small businesses and individuals needing legal assistance. Many of our clients are colleagues from major law firms throughout the U.S. and around the world.

Young Conaway has played a leading role in many groundbreaking cases and has helped shape legislation and case law in Delaware for half a century. Our attorneys routinely appear before federal and Delaware state courts and agencies.

Headquartered in Wilmington, Delaware, Young Conaway's office provides easy access to the United States District Court and Bankruptcy Court for the District of Delaware, the Delaware Supreme Court, the Court of Chancery, and the Superior Court. In addition to its Wilmington headquarters, Young Conaway has an office in New York, New York.

Our Practice Areas

Young Conaway's 105 attorneys provide a wide range of services including:

- Bankruptcy
- Business Planning and Transactions
- Commercial Real Estate, Land Use, and Zoning
- Corporate Counseling
- Employee Benefit
- Labor & Employment
- Litigation (Corporate, Commercial and Intellectual Property)
- Taxation, Trusts and Estates

Recent Accolades

Forty-two Young Conaway attorneys were selected by their peers for inclusion in *The Best Lawyers in America*® 2019 edition, published by Woodward/White, Inc. Since 1983, *The Best Lawyers in America*® along with *U.S. News & World Report* also ranked Young Conaway as a Tier 1, Best Law Firm for 2019.

The 2018 edition of *Chambers USA - America's Leading Lawyers for Business* recognized 23 Young Conaway attorneys as leaders in their respective fields.



Litigation In Delaware

Contact:

Melanie K. Sharp, Esquire
Chair-Commercial Litigation
msharp@ycst.com
Office: 302.571.6681
Mobile: 302.584.2568

Enjoy the Conference!



Dear Attendees,

On behalf of all AB staff and family we welcome you to the 2019 CLE & Ski Conference.

AB Court Reporting & Litigation Support Services has been a part of the Colorado and national legal services community since 1960. Over the past 5 decades we have steadily grown into one of the most reliable and reputable firms throughout the U.S. We are large enough to handle the most challenging litigation demands, yet remain a family owned business that focuses on providing personalized service to each of our clients.

We are confident you will find the conference both educational and informative and we look forward to meeting you. Please feel free to contact us if you have any questions regarding any of our litigation supports services:

Court Reporting

Legal Video

Trial Presentation Services

Interpreting and Translation

Mediation & Arbitration

Commercial Video

Document Services / E-Discovery

Transcription

Sincerely,

J.P. & Carrie Prins

“Experience Excellence”

When Results Matter!



A Warm Welcome

We look forward to meeting you at the 2019 National CLE Conference in Snowmass. Epic Web Results is a leading Internet Marketing firm working exclusively with attorneys nationwide.

Are you currently spending too much on your website? Are you getting the results you had hoped for? Can you get in touch with your current marketing firm easily enough?

Throughout the conference, we hope you will stop by our booth and get to know us while we are learning more how we can help to benefit and enhance your law practice.

About Us

At Epic Web Results, we offer the most comprehensive Internet Marketing experience possible for attorneys. We are your one-stop shop for all your Internet Marketing needs.

Founded on the belief that results are the most important aspect for his clients, Jon Reiter, the Founder and CEO of Epic Web Results set forth to create one of this country's top results-oriented marketing agencies for law firms by focusing on the customers needs and the results they are receiving.

Services Offered:

- ✓ Managed Hosting
- ✓ Website Design & Development
- ✓ Search Engine Optimization
- ✓ Social Media Marketing
- ✓ Mobile Websites
- ✓ Video Production & Optimization
- ✓ Pay-Per-Click/Google AdWords
- ✓ Content Development and Optimization
- ✓ E-books and books written for our clients
- ✓ Blogging
- ✓ Google Maps
- ✓ Local Directories
- ✓ Automated Review Systems

Company History & Strength

- ✓ Founded 2010
- ✓ Increase business two-fold every year since founding due to success of clients Internet marketing campaigns
- ✓ Moved into newly purchased and renovated DTC office building August 2013
- ✓ 95+ % retention rate
- ✓ Results Oriented Culture – We Succeed When You Succeed

Conference Team

Jon Reiter

Founder & CEO of Epic Web Results

Joe Sheftel

Sr. Director of Legal Marketing Nationwide

Finnegan, Henderson, Farabow, Garrett & Dunner, LLP
Protect. Advocate. Leverage.[®] Champion Your Ideas[®]

Welcome to the National CLE Conference! Finnegan is delighted to sponsor the quality programming and networking consistently delivered by this conference each year. We hope you will join Erika Arner for “The Interplay Between IPRs and Other PTAB Trial Proceedings and Litigation -- Strategy and Lessons.”

Established in 1965, Finnegan is one of the largest IP law firms in the world. With offices in the United States, Asia, and Europe, Finnegan practices all aspects of patent, trademark, copyright, and trade secret law, representing clients on IP issues related to U.S. and European patent and trademark law, international trade, portfolio management, the Internet, cybersecurity, e-commerce, government contracts, antitrust, and unfair competition. Finnegan offers full-service IP legal and technical experience in virtually every industry and technology: biotechnology, pharmaceuticals, biologics and biosimilars, chemicals, electronics, semiconductors, computers and software, automotive, aerospace and aviation, industrial manufacturing, consumer products, medical devices, clean energy and renewables, robotics, and 3D printing.

We have more than 340 professionals focused on intellectual property, plus nearly 500 support staff, including legal assistants, and docketing, research, litigation support, and information technology specialists. Other notable aspects of our firm include:

- 300+ professionals with scientific degrees
- 65+ professionals with Ph.D.'s
- 200+ professionals registered to practice before the USPTO
- 30+ professionals who are former USPTO examiners
- U.S. Specialty IP Firm of the Year, 2018 (*Managing Intellectual Property* North American IP Awards)
- U.S. Trade Mark Contentious Firm of the Year,” 2018 (*Managing Intellectual Property* Americas IP Awards)
- “Milestone Case of the Year: *Aqua Products v. Matal*,” 2018 (*Managing Intellectual Property* Americas IP Awards)
- U.S. ITC Firm of the Year, 2018 (*Managing Intellectual Property* Americas IP Awards)

Our clients' businesses and IP assets are global, and protection of these assets is increasingly challenging. With offices around the world and decades of experience assisting multinational companies, Finnegan has the resources and experience to formulate and execute global strategies. Our professionals are multilingual and multicultural, and they work with clients in real time around the clock and around the world.

For more information, please visit www.finnegan.com.



Welcome to the 36th National CLE Conference! We are honored to be among the select businesses sponsoring this conference.

We look forward to connecting with many of you during the next few days, learning about your business, and if you'd like, discussing how our law firm can be a strategic partner to help you navigate the legal concerns that keep you up at night.

Who We Are

Michael Best is a full-service law firm with a nationally recognized IP practice. With more than 150 IP attorneys and technical professionals, in 13 offices across the nation (including three locations in Colorado), our practitioners provide the full range of IP services in patent, trademark and copyright law, including prosecution, portfolio management, licensing, enforcement, clearance, defense and litigation in the U.S. and around the globe. Our group's deep, broad array of expertise means we can tailor a legal team to meet your exact needs. As a full-service firm, we also provide expert counsel in areas such as Labor & Employment, Corporate, Energy, Environmental, Healthcare, Litigation, and Tax law, among other specialties.

What Sets Us Apart

- **Our Approach:** We work in collaborative, cross-practice teams to anticipate and meet our clients 21st century needs. Clients praise our 'highly responsive' approach.
- **Client Experience:** Legal work doesn't happen in a vacuum. We work hard to understand your organization and goals to help you minimize legal risk and maximize competitive advantage.
- **Cost-Efficiency:** Our Engineer, Scientist & Agent Program provides significant cost savings.
- **Global Partner:** As a member of Lex Mundi, the world's leading network of independent law firms, we can provide clients with in-depth legal experience in more than 100 countries.

Please ask us for more information about our services, or visit us at www.michaelbest.com to learn more. We look forward to serving you next!

Sincerely,

A handwritten signature in blue ink that reads 'Scott Alter'.

Scott M. Alter
Partner
IP Program Co-Chair

A handwritten signature in blue ink that reads 'Derek C. Stettner'.

Derek C. Stettner
Partner

The Nation's Largest Forensic Firm Serving both Plaintiff & Defense Lawyers Is Right Here in Denver

We are excited to be in attendance for the LEI National CLE & Ski Conference. We hope we will have an opportunity to connect and discuss how Robson Forensic can provide a unique forensic solution for your most complex and contentious litigation.

Please contact Matt Kemp in our Denver office to discuss case-specific solutions.



Matt Kemp
Denver, CO

A Forensic Engineering Firm

Robson Forensic is a Forensic Engineering Firm, this is an important distinction worth understanding.

We do not outsource our forensic work or merely locate experts; at Robson Forensic we hire technical professionals and provide them with the necessary tools and guidance to become highly effective testifying experts.

We maintain state of the art laboratory facilities, our technical library rivals that of many universities, and our forensic equipment is maintained with obsessive zeal.

You can expect a higher level of technical proficiency, service, and professionalism when working with our firm.

WE STAND BEHIND OUR EXPERTS AND OUR WORK.

Areas of Practice

Admiralty / Maritime	Meteorology
Aquatics	Police Practices
Architecture	Premises Safety
Aviation	Product Liability
Biomechanics	Questioned Documents
Civil Engineering	Railroad & Trains
Crash Reconstruction	Sports & Recreation
Dram Shop	Structural Engineering
Electrical Engineering	Supervision & Education
Elevator & Escalator	Tire Failure Analysis
Environmental	Toxicology
Equine Science	Trucking & Warehousing
Fire & Explosion	Vehicle Engineering
Food Safety	Video & Imagery Analysis
Healthcare	Workplace Safety
Highway Engineering	
Human Factors	
Mechanical Engineering	
Medical Device & Pharma	
Metallurgical Science	



Colorado Bar – 36th Annual National CLE Conference
January 2, 2019

Dear Conference Attendee,

On behalf of Soberlink, welcome to Colorado Bar's 36th Annual National CLE Conference. We are honored to be a sponsor of this great event.

Soberlink supports accountability for sobriety and child safety through a comprehensive alcohol monitoring system. Combining a breathalyzer with wireless connectivity, the portable design and technology includes facial recognition, tamper detection and real-time results and reports. Soberlink provides documented proof of sobriety that reduces litigation and creates peace of mind during parenting time.

Soberlink's benefits include:

- Comprehensive reporting for [reduced court time and litigation](#)
- Compact, portable design allowing for [discreet testing](#)
- Tamper detection and facial recognition for [accurate, reliable test result](#)
- Automated alerts and reminders for [increased access and ease of use](#)
- Time stamps and real-time reporting provide [documented proof of sobriety](#)
- Concerned party can monitor anytime, anywhere fostering [peace of mind](#)

Please visit our booth to learn about our [direct to client](#) Family Law Programs and more.

Sincerely,

Mike Fonseca
National Sales Manager

AGENDA

PROGRAM CO-CHAIRS:

Scott M. Alter

Michael Best & Friedrich LLP
Denver, CO

David H. Bernstein

Debevoise & Plimpton LLP
New York, NY

Wednesday, January 2, 2019

3:00 – 7:00 p.m.

Registration

4:30-6:30 p.m.

Annual Trademark and Copyright Updates

SESSION ONE

Developments in Copyright Law

Evan M. Rothstein, Arnold & Porter Kaye Scholar LLP, Denver, CO

SESSION TWO

Developments in Trademark Registration Practice

Hope Hamilton, Holland & Hart LLP, Boulder, CO

SESSION THREE

Developments in Trademark Litigation

David H. Bernstein, Debevoise & Plimpton LLP, New York, NY

Thursday, January 3, 2019

7:00 – 9:00 a.m.

Essential Updates

SESSION ONE

Trade Secrets Law Update

Peter Brody, Ropes & Gray LLP, Washington, DC

SESSION TWO

Advertising Law Update

Laura Brett, Director, National Advertising Division, Advertising Self-Regulation Council, Washington, DC

SESSION THREE

Right of Publicity Update

Megan K. Bannigan, Debevoise & Plimpton LLP, New York, NY

4:30 – 6:30 p.m.

Plenary Session - More Fun with Ethics at the Movies

Larry J. Cohen, Ph.D., J.D., Cohen's Counsel, Bethel, VT

6:30 p.m.

Wine Reception

Friday, January 4, 2019

7:00 – 7:40 a.m.

Practical Strategies from Corporate Counsel on the Scope of Intellectual Property Protection

Scott Piering, Vice President and Chief Intellectual Property Counsel, Spectrum Brands, Inc., Middleton, WI

7:40 – 8:20 a.m.

The ACPA, UDRP and URS: Navigating the Alphabet Soup of Domain Name Dispute Resolution

Paula L. Zecchini, Cozen O'Connor, Seattle, WA

8:20 – 9:00 a.m.

Developments in European IP Law, and the Expected Impact of Brexit
Nick Aries, Bird & Bird LLP, London, UK

3:20 – 4:20 p.m.

Bonus Plenary Session - CTE and Mild Traumatic Brain Injury: An Update and a Litigator's Protocol
Larry J. Cohen, Ph.D., J.D., Cohen's Counsel, Bethel, VT

4:30 – 5:15 p.m.

The Top Ten Patent Issues to Know About the U.S. Patent and Trademark Office
Drew Hirshfeld, Commissioner for Patents, US Patent and Trademark Office, Washington, DC

5:15 – 6:00 p.m.

Building a Strong Patent Portfolio: Views from In-House
Steve Mackenzie, Senior Counsel, Intellectual Property and Intellectual Property Litigation, Koch Companies Public Sector LLC, Wichita, KS
David McKenzie, Associate General Counsel, IP Legal, WD, a Western Digital Company, San Jose, CA
Cynthia S. Mitchell, Senior Corporate IP Counsel, Zimmer Biomet, Denver, CO

6:00 – 6:45 p.m.

The Fast-Changing World of Software-Related Patents: Critical Issues You Need to Know
Scott Alter, Michael Best & Friedrich LLP, Denver, CO
Edward R. Tempesta, Vice President – Senior Counsel – Intellectual Property, Mastercard, New York, NY

Saturday, January 5, 2019

7:00 – 7:45 a.m.

Patent Law Update – 2018 in Review
Dennis D. Crouch, Associate Professor of Law, University of Missouri Law School, Columbia, MO

7:45 – 8:30 a.m.

Beyond the Looking Glass: Getting in Front of the Next Generation of Patent Prosecution Cases

Derek C. Stettner, Michael Best & Friedrich LLP, Waukesha, WI, and Chicago, IL

8:30 – 9:15 a.m.

The Interplay Between IPRs and Other PTAB Trial Proceedings and Litigation — Strategy and Lessons

Honorable Kara Stoll, Circuit Judge, Court of Appeals for the Federal Circuit, Washington, DC

Erika Arner, Finnegan, Henderson, Farabow, Garrett & Dunner LLP, Washington, DC

4:30 – 5:30 p.m.

Corporate Counsel Panel: What's Keeping Corporate Counsel Awake at Night

Monica Adjemian, Attorney, Microsoft Corporate, External and Legal Affairs, Seattle, WA

Toni Y. Hickey, Chief Intellectual Property Counsel, Cummins, Inc., Indianapolis, IN

Heath Hogle, Chief Patent Counsel, Dolby, San Francisco, CA

Shelley Mixon, Agilent Technologies, Inc., Colorado Springs, CO

Brian Platt, Director of IP Litigation, Nagra, Wenatchee, WA

5:30 – 6:45 p.m.

A Dialogue Between Bench and Bar

Honorable Kimberly Ann Moore, Circuit Judge, Court of Appeals for the Federal Circuit, Washington, DC

Honorable Kara Stoll, Circuit Judge, Court of Appeals for the Federal Circuit, Washington, DC

Honorable Leonard P. Stark, Chief Judge, United States District Court, District of Delaware, Wilmington, DE

Ian Gershengorn, Jenner & Block, Former Acting Solicitor General and Deputy Solicitor, Washington, DC

John M. Whealan, Intellectual Property Advisory Board Associate Dean for Intellectual Property Law Studies, GW | Law, The George Washington University, Washington, DC

Deanne E. Maynard, Morrison Foerster, Washington, DC

Sunday, January 6, 2019

Plenary Session

7:00 – 9:00 a.m.

Cyber-Rights and Cyber-Wrongs: Legal Ethics in a Digital Age

Sherman W. Kahn, Mauriel Kapouytian Woods LLP, New York, NY

Joseph V. DeMarco, DeVore and DeMarco LLP, New York, NY

BIOGRAPHICAL INFORMATION

PROGRAM CO-CHAIRS

Scott Alter is a partner in Michael Best & Friedrich's Denver office. He is an experienced intellectual property attorney whose practice focuses on software, electronics, internet, telecommunications, cloud computing, medical device, financial, and semiconductor technologies. A skilled global patent strategist, he also has significant expertise in patent eligibility, joint and indirect infringement, and indefiniteness. In every matter he handles, Scott strives to obtain practical results for his clients. Scott has served as an expert witness in litigation concerning data encryption technology. Before becoming a lawyer, he worked at IBM as a computer programmer. Prior to joining the firm, Scott was a partner in the Colorado office of a national law firm.

David Bernstein is chair of the Intellectual Property Litigation Group at Debevoise & Plimpton LLP in New York, and an adjunct professor of law at New York University Law School and George Washington University Law School, where he teaches Advanced Trademark Law. He received an A.B. *magna cum laude* from Princeton University's Woodrow Wilson School of Public and International Affairs in 1985, an M.Sc. from the London School of Economics and Political Science in 1986, and his J.D. from Yale Law School in 1989. Mr. Bernstein has served as Counsel and Director of INTA, and has chaired its International Amicus, Emerging Issues, and Programs Committees, and has co-chaired its Annual Meeting.

FACULTY

Monica Adjemian is an experienced attorney whose practice has focused on all aspects of intellectual property, including patent, trademark and copyright matters, and international intellectual property issues. Monica currently works as in-house counsel for Microsoft, overseeing patent portfolio development and management for XBOX and all gaming at Microsoft, previously supporting a variety of product areas such as, Word, PowerPoint, Sway, OneNote, To-Dos, Skype for Business, and educational offerings. Before taking her career in-house at Microsoft, Monica worked out of Silicon Beach, California, representing clients from the high-tech, manufacturing, and entertainment industries and specializes in a variety of technologies including semiconductors, LEDs, lighting systems, mobile applications, medical imaging devices, systems and software, electronic devices, pool/spa systems, e-commerce systems and software, and video game systems and software. Monica received a Bachelor of Science in Computer Science from the University of Southern California (USC) and a Juris Doctorate degree from Pepperdine University School of Law.

Nick Aries is a UK and European IP partner co-heading international law firm Bird & Bird's San Francisco representative (non-US law) office. Nick advises on EU and UK trade mark, copyright, design, and trade secrets matters, with a particular interest in IP issues arising out of online and other digital businesses. Being in the US means Nick can be contacted on EU/UK IP matters by US clients and practitioners at a time convenient to them, and makes face to face interaction for advice, updates and training on such matters possible. Nick is an Advisory Board member of the SFIPLA, a member of the SVIPLA and chairs the International and Legislative sub-committee of INTA's Copyright Committee.

Erika Arner former leader of Finnegan's patent office practice, focuses on patent office trials, patent prosecution management, client counseling, and litigation, with an emphasis on electronic technology, computer software, and the Internet. Ms. Arner has represented patent owners and petitioners in over 100 post-grant review (PGR) and inter partes review (IPR) trials before the Patent Trial and Appeal Board (PTAB) of the U.S. Patent and Trademark Office (USPTO), serving as lead counsel in over 50. She has also argued and won appeals from PTAB trials to the U.S. Court of Appeals for the Federal Circuit, many of which involve issues of first impression in this emerging area of patent law. In addition to her extensive experience in patent office practice, Ms. Arner is a well-known authority in the area of business method patents and patent-eligibility jurisprudence. She represented the petitioners before the U.S. Supreme Court in *Bilski v. Kappos*, and has advised clients on issues related to patentable subject matter before the Federal Circuit, U.S. district courts, and the USPTO. Ms. Arner is a frequent author and lecturer on business method and computer-related patents and practice before the PTAB.

Megan Bannigan

Laura Brett, Assistant Director, National Advertising Division (“NAD”) of the Advertising Self-Regulatory Council. Laura joined NAD in April 2012 and has handled a variety of cases involving advertising in digital media, including the review of the adequacy of disclosures in digital formats and, in particular, in native advertising. In addition to speaking at seminars on the issues surrounding advertising in social media, Laura has published articles on the ethical standards of advertisers in social media and native advertising and participated on a panel at the FTC's Native Advertising Workshop in December 2013. Prior to joining NAD, Laura specialized in litigation matters in her own private practice and at Willkie Farr & Gallagher. In addition to Laura's professional experience, she has served on the board of not-for-profit organizations and served as Deputy Mayor on her local City Council. Laura graduated with a B.A. from Trinity College in Hartford, CT, and received her law degree from Fordham University School of Law.

Peter Brody has been successfully litigating intellectual property cases and other complex disputes in federal and state courts across the United States for over 30 years. A member and former chair of Ropes & Gray's intellectual property litigation group, Peter has litigated every type of IP case – patent, copyright, trade secret, trademark, and false advertising - as well as a wide range of constitutional, administrative, and contract disputes. Peter also has substantial experience in alcoholic beverage laws and regulations. In addition to his trial and appellate practice, Peter has served as lead counsel in numerous domestic and international arbitrations, as well as hearings and proceedings before federal and state administrative agencies. Peter's broadbased litigation experience enables him to see the big picture and to present complicated and technical matters in a clear and easy to understand manner. His extensive knowledge of intellectual property law, careful case preparation, and skilled advocacy are valued by leading companies in a wide array of business sectors, including alcoholic beverages, consumer electronics, pharmaceuticals and medical devices, financial services, food, and personal care. Peter is also an active member of the firm's social media group. He routinely advises clients on trademark and copyright protection and enforcement in the social media arena, best practices for protecting confidential information and trade secrets from disclosure on social media sites, and federal and state regulation of advertising and promotion via social media. Peter also helps clients protect themselves from – and respond to – incidents of doxing (doxxing). In addition, Peter serves as an editorial adviser to Bloomberg BNA. Peter also lectures and writes extensively on social media, intellectual property and alcoholic beverage law and practice. He currently serves as the President of the U.S. Chapter of the International Wine Lawyers Association.

Larry Cohen is a certified specialist in injury and wrongful death litigation who has focused in his nearly thirty-two years of law practice on serious medical injury and emotional damages cases, including especially brain injury claims. He received his J.D. from Northwestern University in 1985, and has been admitted to practice in Arizona since 1985. Mr. Cohen also has a Master's degree and a Ph.D. from Syracuse University and has participated in a post-doctoral program in clinical neuropsychology. He continues as a member of the adjunct faculty at the Sandra Day O'Connor College of Law at Arizona State University where he has taught courses in professional responsibility, pretrial practice and professional liability. He taught and did research at the University Michigan School of Law and at the University of Illinois-Chicago, and taught on the adjunct faculties of the Arizona Summit School of Law, the Arizona School of Professional Psychology, now Argosy University, Midwestern University, and Norwich University. Mr. Cohen speaks nationally to groups of lawyers, other professionals, insurance companies, governmental entities, risk managers and other interest groups about litigation and trial practice matters, legal ethics, alternative dispute resolution, and issues in brain damage, law and medicine and law and psychology. He has received awards from the Maricopa County Bar Association, the State Bar of Arizona and the State Bar of New Mexico for excellence in continuing legal education. He also received a President's Award from the State Bar of Arizona for contributions in continuing legal education. He has for many years been listed by Southwest Super Lawyers and Arizona's Finest Lawyers as among the best lawyers in

Arizona and has been recognized by the National Association of Distinguished Counsel as among the top one percent of lawyers in the United States.

Dennis Crouch is Associate Professor of Law at the University of Missouri School of Law. Prior to joining the MU Law Faculty, he was a patent attorney at McDonnell Boehnen Hulbert & Berghoff LLP in Chicago, Illinois, and taught at Boston University Law School. He has worked on cases involving various technologies including computer memory and hardware, circuit design, software, networking, mobile and internet telephony, automotive technologies, lens design, bearings, HVAC systems, and business methods. He is also the editor of the popular patent law weblog: <http://patentlyo.com/Patently-O> . Professor Crouch received his BSE in mechanical engineering *cum laude* from Princeton University, where he also earned a certificate in engineering management systems. He then earned his JD *cum laude* from the University of Chicago Law School. While at the University of Chicago, he was a Microsoft, Merck, & Pfizer scholar and a member of the Olin program in law and economics. Prior to attending law school, Professor Crouch worked as a technical consultant for manufacturing firms in New England, as a research fellow at NASA's Glenn Research Center, as a software developer at the Mayo Clinic's department of biomedical imaging, and as a Peace Corps Volunteer in Ghana, West Africa. Dennis Crouch grew up on a farm near Pittsburg, Kansas.

Joseph V. DeMarco is a founding partner in the law firm of DeVore & DeMarco LLP where he specializes in litigation and counseling in complex matters involving information privacy and security, theft of intellectual property, computer intrusions, on-line fraud, and the lawful use of new technology. His years of experience in private practice and government handling the most difficult cybercrime investigations and disputes have made him one of the nation's leading experts on Internet crime and the law of data privacy and security. From 1997 to 2007, Mr. DeMarco served as an Assistant United States Attorney for the Southern District of New York, where he founded and headed the Computer Hacking and Intellectual Property Program, a group of prosecutors dedicated to investigating and prosecuting violations of federal cybercrime laws and intellectual property offenses. Under his leadership, cybercrime prosecutions grew from a trickle in 1997 to a top priority of the United States Attorney's Office, encompassing all forms of criminal activity affecting e-commerce and critical infrastructures including computer hacking crimes; transmission of Internet worms and viruses; electronic theft of trade secrets; web-based frauds; and criminal copyright and trademark infringement offenses. As a recognized expert in the field, Mr. DeMarco was also frequently asked to counsel prosecutors and law enforcement agents regarding novel investigative and surveillance techniques and methodologies. In 2001, Mr. DeMarco served as a visiting Trial Attorney at the Department of Justice Computer Crimes and Intellectual Property Section in Washington, D.C. Since founding DeVore & DeMarco LLP in 2007, Mr. DeMarco has represented corporations and organizations in various industries in litigation, investigation and counseling matters concerning the law of data privacy and security. He is on the National Roster of approved neutrals of the American Arbitration Association (AAA) and of Federal Arbitration, Inc. (FedArb), where he adjudicates disputes between businesses involving data privacy, high-

technology, and related commercial law issues. He speaks frequently on the benefits of ADR in data security and privacy litigation. Since 2002, Mr. DeMarco has served as an adjunct professor at Columbia Law School, where he teaches the upper-class *Internet and Computer Crimes* seminar. He has spoken throughout the world on cybercrime, e-commerce, and IP enforcement, including at the Practising Law Institute (PLI), the National Advocacy Center, and the FBI Academy in Quantico, Virginia. He has also served as an instructor on cybercrime law to judges at the New York State Judicial Institute. Prior to joining the United States Attorney's Office, Mr. DeMarco was a litigation associate at Cravath, Swaine & Moore, where he concentrated on intellectual property, antitrust, and securities litigation. Between law school and Cravath, Mr. DeMarco served as a Law Clerk to the Honorable J. Daniel Mahoney of the United States Court of Appeals for the Second Circuit. Mr. DeMarco holds a J.D. *cum laude* from New York University School of Law where he was an Articles Editor of the *NYU Law Review* and a member of the Order of the Coif. He received his B.S.F.S. *summa cum laude* from the School of Foreign Service at Georgetown University. He is currently a member of several bar and professional associations, including the: International Bar Association (Technology Committee), International Association of Korean Lawyers (Regional Governor, New York), New York State Bar Association, Commercial and Federal Litigation Section (Co-chair, *Internet and IP Committee*, 2009-present), New York City Bar Association (Co-Chair, *Information Technology and Cyber-Law Committee*) and Connecticut Bar Association (Federal Practice Committee). Mr. DeMarco is a *Martindale-Hubbell* AV-rated lawyer for Computers and Software, Litigation and Internet Law, and is listed in *Chambers USA: America's Leading Lawyers for Business* in Privacy and Data Security law. He has been named as a "SuperLawyer" in Intellectual Property Litigation. He is a member of the Professional Editorial Board of the *Computer Law & Security Review*; serves on the Board of Advisors of the *Center for Law and Information Policy* at Fordham University School of Law; and is a member of *Business Executives for National Security*. Mr. DeMarco has received numerous professional awards, including the U.S. Department of Justice *Director's Award for Superior Performance* and the *Lawyer of Integrity Award* from the Institute for Jewish Humanities. In addition to his professional activities, he enjoys parenting, hiking, squash, golf, reading, and listening to classical piano music.

Ian Gershengorn is chair of Jenner & Block's Appellate and Supreme Court Practice and is one of the Nation's premier Supreme Court and appellate advocates. Before rejoining Jenner & Block, Ian served in the Office of the Solicitor General at the US Department of Justice from 2013 to 2017, first as Principal Deputy Solicitor General and then as Acting Solicitor General of the United States. While at the Solicitor General's Office, Ian argued 13 cases at the US Supreme Court and two cases before the D.C. Circuit en banc. He also supervised the government's briefing in a range of high-profile cases, including those involving the Affordable Care Act, election law, immigration, the Religious Freedom Restoration Act, and same-sex marriage. Prior to his service in the Solicitor General's office, Ian served from 2009 to 2013 as the Deputy Assistant Attorney General in charge of the DOJ's Federal Programs Branch. In that role, he led the district court defense of the Affordable Care Act, personally arguing the principal district court challenges to the constitutionality of the Act. Since returning to

Jenner & Block in September 2017, he has argued cases throughout the country, including in the Courts of Appeals for the First, Seventh, and Eighth Circuits, and the Indiana Supreme Court. Ian graduated *magna cum laude* from both Harvard College and Harvard Law School. After law school, he clerked for Judge Amalya Kearsse on the U.S. Court of Appeals for the Second Circuit and for Justice John Paul Stevens of the U.S. Supreme Court.

Hope Hamilton is a Partner in Holland & Hart's Trademark and IP Litigation Groups. She regularly counsels clients on strategic trademark protection and enforcement, with a focus on helping clients resolve disputes prior to litigation. When litigation is inevitable, Hope has a track record of success and has obtained important rulings that have helped shape trademark law. Clients have noted Hope's creativity in approaching litigation and her overall responsiveness, efficiency, effectiveness, and expertise in her field. Hope's practice also includes pre-litigation trademark and copyright enforcement, particularly in connection with internet and keyword advertising, social media, domain names, and e-commerce. Clients also seek Hope's counsel on trademark and trade dress selection, clearance, prosecution, registration, and maintenance.

Toni Hickey

Drew Hirshfeld is Commissioner for Patents for the U.S. Patent and Trademark Office. He was appointed to this position in July 2015. As Commissioner for Patents, Mr. Hirshfeld manages and leads the patent organization as its chief operating officer. He is responsible for managing and directing all aspects of this organization which affect administration of patent operations, examination policy, patent quality management, international patent cooperation, resources and planning, and budget administration. In his previous role as Deputy Commissioner for Patent Examination Policy, Mr. Hirshfeld served as an authority on patent laws, rules, and examining practice and procedure, and provided administrative oversight and direction for the activities of the Office of Petitions, Office of Patent Legal Administration, and the Office of the Manual of Patent Examining Procedure. Further, Mr. Hirshfeld established patent examination and documentation policy standards for the Commissioner for Patents. Prior to serving as Deputy Commissioner for Patent Examination Policy, Mr. Hirshfeld was the Chief of Staff to the Under Secretary of Commerce for Intellectual Property and Director of the USPTO. Mr. Hirshfeld began his career at the USPTO in 1994 as a Patent Examiner. He became a Supervisory Patent Examiner in 2001, and was promoted to the Senior Executive Service in 2008 as a Group Director in Technology Center 2100, Computer Architecture and Software. Mr. Hirshfeld received a Bachelor of Science from the University of Vermont, and a J.D. from Western New England College School of Law.

Heath Hogle is Vice President and Chief Patent Counsel at Dolby in San Francisco, where he has global responsibility for patents, trademarks and copyrights. In this role he has consistently driven year-over-year growth in Dolby's patent licensing programs. He has significant experience in building strategic IP portfolios and licensing programs. Mr. Hogle serves on the council of the American Bar Association IP section, on the board of IPO, and is past president of the San Francisco IP Law Association. He holds a JD (cum laude), an MS and a BS (cum laude) from the University of Minnesota.

Sherman W. Kahn acts as an arbitrator and represents clients in international arbitration proceedings presenting complex technical and commercial issues and has arbitrated under the ICC, AAA, ICDR, JCAA, and other arbitration and dispute resolution rules. He has sat as panel chair, sole arbitrator, and wing arbitrator in numerous international and domestic arbitrations with subject matter including IT outsourcing, software development, mining, patent infringement and other IP issues, as well as trademark licensing, unfair competition and trade disparagement, and commercial issues. Sherman provides advice regarding clause drafting and pre-dispute issues in connection with major construction and infrastructure projects. He is a member of the International Centre for Dispute Resolution (ICDR) Panel of Arbitrators, the American Arbitration Association Roster of Commercial Arbitrators and the CPR Distinguished Panel of Neutrals. He is a Fellow of the Chartered Institute of Arbitrators (FCIArb) and a member of the Silicon Valley Arbitration and Mediation Center Tech List. Sherman also acts as a mediator and is a member of the Southern District of New York and New York Supreme Court Commercial Division, mediation panels. Sherman has twenty years of experience in patent litigation. He has litigated patent matters involving complex technologies, such as programmable logic devices, microprocessors and controllers, memory devices, construction equipment, medical devices, supercomputers, LCD & PDP display devices, LED Lighting, various computer software products, and networking technologies as well as biotechnology inventions. Sherman also litigates IT outsourcing, trade secret, trademark, copyright, and antitrust matters. Sherman advises clients regarding information security and privacy issues for compliance and in privacy-related regulatory proceedings and litigation. Sherman represents clients in FTC and state attorney general investigations of privacy, information security and advertising practices.

David McKenzie is Associate General Counsel, in the IP legal department at Western Digital. He also serves as the Legal IP representative to the Western Digital Open Source Committee. Practicing since 2000, David is an experienced IP practitioner with a knack for explaining complex technology and complex legal issues simply and understandably. David manages part of the memory technology patent portfolio for Western Digital. David's technical experience runs from computer software to flash memory storage hardware and circuitry. David's corporate IP experience includes a small high tech storage startup, a fortune 500 flash storage company, and now a fortune 200 storage company. He enjoys advising engineers on innovation, patents, and open source compliance. When not at work, David enjoys time with his family and tinkering with the latest software, programming, and DIY hardware systems such as Python, Android, Linux, and Raspberry Pi systems.

Stephen MacKenzie is Senior Counsel IP and IP Litigation at Koch Companies Public Sector, which is the Legal, Government, and Public Affairs division for Koch Industries, Inc. based in Wichita, Kansas. Steve focuses his practice on prosecution strategy, IP management and counseling, M&A, and licensing. Prior to joining Koch, Steve worked in private practice as a patent litigation attorney in Wilmington, Delaware.

Deanne Maynard, for more than 20 years, she, co-chair of Morrison & Foerster's Appellate and Supreme Court practice, has briefed and argued significant appeals in the United States Supreme Court and appellate courts across the country. She has argued 14 cases before the Supreme Court and filed over 100 briefs in that Court. Ms. Maynard's appellate practice is nationwide. She has particular experience in the Federal Circuit, where she has argued more than 30 appeals, representing both patentees and defendants, on a variety of technologies. Ms. Maynard also appears regularly in the Ninth Circuit, where she has argued 15 appeals. Before joining Morrison & Foerster, Ms. Maynard served as an Assistant to the Solicitor General at the U.S. Department of Justice for five years. She previously was a partner at another major law firm. After law school, Ms. Maynard clerked twice on the Supreme Court: one Term for Justice Stephen Breyer in his first year on the Court, and another Term for retired Justice Lewis Powell and Justice John Paul Stevens. Ms. Maynard graduated magna cum laude from Harvard Law School, where she was an editor of the Harvard Law Review. She earned a B.A. in English, with distinction, from the University of Virginia. Ms. Maynard is annually recommended as a leading lawyer by Chambers USA, Legal 500 US, and Best Lawyers in America. She is a Fellow in the American Academy of Appellate Lawyers, selected for her distinction as an appellate lawyer. Ms. Maynard serves on the Board of Trustees of the Supreme Court Historical Society. She also is a Master in, and Past President of, the Coke Appellate Inn of Court.

Cynthia Mitchell has practiced intellectual property law for over 25 years, starting as a patent examiner at the USPTO. She currently works for Zimmer Biomet. Formerly she also practiced IP law at Hewlett Packard, Agilent Technologies, National Renewable Energy Laboratory, Avaya. She is currently pursuing an LLM in international business transactions at the University of Denver Sturm College of Law.

Shelley Mixon is in-house patent counsel at Agilent Technologies, Inc. in Santa Clara, CA, a global leader in life sciences, diagnostics, and applied chemical market. Shelley develops and implements IP strategies for business divisions of Agilent Crosslab Group (ACG). She is a former President of the Colorado IP Inn of Court and now serves on the Inn's mentoring committee. Shelley has a bachelor's degree in Biomedical Engineering from Boston University and a J.D. from the University of Texas School of Law.

Honorable Kimberly Moore was appointed by President George W. Bush in 2006. Prior to her appointment, Judge Moore was a Professor of Law from 2004-2006 and Associate Professor of Law from 2000 to 2004 at the George Mason University School of Law. She was an Assistant Professor of Law at the University of Maryland School of Law from 1999 to 2000. She served both as an Assistant Professor of Law from 1997 to 1999 and the Associate Director of the Intellectual Property Law Program from 1998 to 1999 at the Chicago-Kent College of Law. Judge Moore clerked from 1995 to 1997 for the Honorable Glenn L. Archer, Jr., Chief Judge of the United States Court of Appeals for the Federal Circuit, and was an Associate at Kirkland & Ellis from 1994 to 1995. From 1988 to 1992, Judge Moore was employed in electrical engineering with the Naval Surface Warfare Center. Judge Moore received her B.S.E.E. in 1990, M.S. in 1991, both from the Massachusetts Institute of Technology, and her J.D. (cum laude) from the Georgetown University Law Center in 1994. Judge Moore has written and presented widely on patent litigation. She co-authored a legal casebook entitled Patent Litigation and Strategy and served as the Editor of The Federal Circuit Bar Journal from 1998 to 2006.

Scott Piering is the Vice President & Chief Intellectual Property Counsel at Spectrum Brands, Inc. In this capacity, Mr. Piering oversees a wide range of global intellectual property matters, from the identification and acquisition of intellectual property rights to the exploitation and protection of those rights, for Spectrum Brands' five divisions: Global Auto Care, Global Batteries, Hardware and Home Improvement, Personal Care and Home Appliances, and Pet, Home and Garden. Mr. Piering is also directly involved in the management of the enforcement of Spectrum Brands' intellectual property in both retail and online settings, and oversees all anti-counterfeiting efforts. Before joining Spectrum Brands, Mr. Piering was a Senior Intellectual Property Lawyer at Cargill, Inc., where he led the intellectual property function for several of its divisions. Prior to that, Mr. Piering practiced law with several law firms, where he focused on intellectual property, antitrust and trade regulation, litigation, and legal issues before various administrative agencies. Mr. Piering holds a Bachelor's degree from Marquette University and received his J.D. *cum laude* from the University of Wisconsin Law School. Mr. Piering frequently addresses topics related to the intellectual property issues that arise in the corporate context, and managing legal costs. Mr. Piering is admitted to the State Bars of Wisconsin, California, Ohio and Minnesota.

Brian Platt

Evan Rothstein focuses his practice on complex commercial litigation with a specific emphasis on intellectual property. A recognized trial lawyer, he has significant experience handling patent litigation in federal courts around the country and at the Patent Trial and Appeal Board, trademark litigation in federal court and at the Trademark Trial and Appeal Board, copyright cases, and trade secret matters. Evan works with all sizes of companies, foreign and domestic across a broad range of technologies, including those in media and advertising, gaming, travel merchandise, digital signage, software, networking and telecommunications, e-commerce, and industrial equipment.

Chief Judge Leonard Stark was appointed to the United States District Court for the District of Delaware by President Obama in August 2010 and became the District's Chief Judge on July 1, 2014. He had previously served for three years as a U.S. Magistrate Judge on the same Court. From 2002 through 2007, Judge Stark was an Assistant United States Attorney for the District of Delaware, and from 1997 through 2001 he was an Associate in the Delaware office of Skadden, Arps, Slate, Meagher & Flom. He began his career by clerking for the Honorable Walter K. Stapleton of the Court of Appeals for the Third Circuit. Judge Stark graduated from the University of Delaware in 1991 with an Honors Bachelor of Arts in Political Science, a Bachelor of Science with Distinction in Economics, and a Masters of Arts in European History. He then earned a Doctor of Philosophy in Politics from the University of Oxford (Magdalen College) as a Rhodes Scholar in 1993 and a J.D. from Yale Law School in 1996. Judge Stark has served as the Third Circuit's District Judge representative to the Judicial Conference of the United States, the policy-making body for the federal judiciary, and is currently a member of the Judicial Conference's Judicial Resources Committee. He is also an adjunct professor at the University of Pennsylvania Law School.

Derek Stettner

Honorable Kara Stoll was appointed to the United States Court of Appeals for the Federal Circuit by President Barack H. Obama on November 12, 2014, was confirmed unanimously by the United States Senate on July 7, 2015, and assumed her duties on July 17, 2015. Judge Stoll practiced law with the firm of Finnegan, Henderson, Farabow, Garrett and Dunner from 1998 to 2015, and became a partner at the firm in 2006. While in private practice, Judge Stoll specialized in patent litigation with an emphasis on appeals. Judge Stoll was an adjunct professor at George Mason University Law School from 2008 to 2015 and at the Howard University School of Law from 2004 to 2008. From 1997 to 1998, Judge Stoll served as a law clerk to The Honorable Alvin A. Schall of the United States Court of Appeals for the Federal Circuit. Judge Stoll worked as a patent examiner at the United States Patent and Trademark Office from 1991 to 1997. Judge Stoll received a J.D. from the Georgetown University School of Law in 1997, where she received the Leon Robin Patent Award, and a B.S.E.E. from Michigan State University in 1991.

Edward R. Tempesta is a Senior Counsel, Intellectual Property at Mastercard. At Mastercard Mr. Tempesta is responsible for all aspects of IP, including IP litigation, patent prosecution, and IP-related transactions. Before joining Mastercard Mr. Tempesta was an associate at Patterson Belknap Webb & Tyler LLP and Baker Botts LLP in New York, where his practice focused on patent litigation and prosecution in the pharmaceutical, consumer electronics, and industrial processing fields. Mr. Tempesta received a B.S. in Chemical Engineering from Carnegie Mellon University in 1999 and his J.D. *cum laude* from Cornell Law School in 2005.

John Whealan, before joining GW Law in 2008, worked at the U.S. Patent and Trademark Office (USPTO) where he served as deputy general counsel for intellectual property law and solicitor since 2001. Dean Whealan represented the USPTO in all intellectual property litigation in federal court and advised the agency on a variety of policy issues. During his tenure, he argued approximately 30 cases before the Federal Circuit and, with his staff, was responsible for briefing and arguing more than 250 cases. Dean Whealan also assisted the U.S. Solicitor General on virtually every intellectual property case that has been heard by the Supreme Court since 2001. He also served as counsel to the U.S. Senate Committee on the Judiciary for the last year.

Paula Zecchini is a shareholder at Cozen O'Connor and focuses her national practice on complex commercial and intellectual property litigation, with an emphasis on the Internet and technology. She has spent more than a decade litigating trademark infringement, domain disputes, unfair competition, and false advertising claims on behalf of Fortune 500 companies and small businesses. Paula also provides clients with strategic guidance on a wide range of issues related to advertising and brand protection, including compliance with the Telephone Consumer Protection Act, the enforcement of intellectual property rights, and the legal landscape surrounding web accessibility. Paula has successfully defended numerous class actions and currently serves as the co-chair for the Class Action Subcommittee of the American Bar Association's Section of Litigation, Consumer Litigation Committee. Prior to practicing law, Paula served as a Special Operations soldier in the U.S. Army Reserve, graduating first in her class from the John F. Kennedy Special Warfare Center and School.

TABLE OF CONTENTS

SECTION 1

Developments in Copyright Law

Evan M. Rothstein, Arnold & Porter Kaye Scholar LLP, Denver, CO

SECTION 2

Developments in Trademark Registration Practice

Hope Hamilton, Holland & Hart LLP, Boulder, CO

SECTION 3

Developments in Trademark Litigation

David H. Bernstein, Debevoise & Plimpton LLP, New York, NY

SECTION 4

Trade Secrets Law Update

Peter Brody, Ropes & Gray LLP, Washington, DC

SECTION 5

Advertising Law Update

Laura Brett, Director, National Advertising Division, Advertising Self-Regulation Council, Washington, DC

SECTION 6

Right of Publicity Update

Megan K. Bannigan, Debevoise & Plimpton LLP, New York, NY

SECTION 7

Plenary Session - More Fun with Ethics at the Movies

Larry J. Cohen, Ph.D., J.D., Cohen's Counsel, Bethel, VT

SECTION 8

Practical Strategies from Corporate Counsel on the Scope of Intellectual Property Protection

Scott Piering, Vice President and Chief Intellectual Property Counsel, Spectrum Brands, Inc., Middleton, WI

SECTION 9

The ACPA, UDRP and URS: Navigating the Alphabet Soup of Domain Name Dispute Resolution

Paula L. Zecchini, Cozen O'Connor, Seattle, WA

SECTION 10

Developments in European IP Law, and the Expected Impact of Brexit

Nick Aries, Bird & Bird LLP, London, UK

SECTION 11

Bonus Plenary Session - CTE and Mild Traumatic Brain Injury: An Update and a Litigator's Protocol

Larry J. Cohen, Ph.D., J.D., Cohen's Counsel, Bethel, VT

SECTION 12

The Top Ten Patent Issues to Know About the U.S. Patent and Trademark Office

Drew Hirshfeld, Commissioner for Patents, US Patent and Trademark Office, Washington, DC

SECTION 13

Building a Strong Patent Portfolio: Views from In-House

Steve Mackenzie, Senior Counsel, Intellectual Property and Intellectual Property Litigation, Koch Companies Public Sector LLC, Wichita, KS

David McKenzie, Associate General Counsel, IP Legal, WD, a Western Digital Company, San Jose, CA

Cynthia S. Mitchell, Senior Corporate IP Counsel, Zimmer Biomet, Denver, CO

SECTION 14

The Fast-Changing World of Software-Related Patents: Critical Issues You Need to Know

Scott Alter, Michael Best & Friedrich LLP, Denver, CO

Edward R. Tempesta, Vice President – Senior Counsel – Intellectual Property, Mastercard, New York, NY

SECTION 15

Patent Law Update – 2018 in Review

Dennis D. Crouch, Associate Professor of Law, University of Missouri Law School, Columbia, MO

SECTION 16

Beyond the Looking Glass: Getting in Front of the Next Generation of Patent Prosecution Cases

Derek C. Stettner, Michael Best & Friedrich LLP, Waukesha, WI, and Chicago, IL

SECTION 17

The Interplay Between IPRs and Other PTAB Trial Proceedings and Litigation — Strategy and Lessons

Honorable Kara Stoll, Circuit Judge, Court of Appeals for the Federal Circuit, Washington, DC

Erika Arner, Finnegan, Henderson, Farabow, Garrett & Dunner LLP, Washington, DC

SECTION 18

Corporate Counsel Panel: What's Keeping Corporate Counsel Awake at Night

Monica Adjemian, Attorney, Microsoft Corporate, External and Legal Affairs, Seattle, WA

Toni Y. Hickey, Chief Intellectual Property Counsel, Cummins, Inc., Indianapolis, IN

Heath Hogle, Chief Patent Counsel, Dolby, San Francisco, CA

Shelley Mixon, Agilent Technologies, Inc., Colorado Springs, CO

Brian Platt, Director of IP Litigation, Nagra, Wenatchee, WA

SECTION 19

A Dialogue Between Bench and Bar

Honorable Kimberly Ann Moore, Circuit Judge, Court of Appeals for the Federal Circuit, Washington, DC

Honorable Kara Stoll, Circuit Judge, Court of Appeals for the Federal Circuit, Washington, DC

Honorable Leonard P. Stark, Chief Judge, United States District Court, District of Delaware, Wilmington, DE

Ian Gershengorn, Jenner & Block, Former Acting Solicitor General and Deputy Solicitor, Washington, DC

John M. Whealan, Intellectual Property Advisory Board Associate Dean for Intellectual Property Law Studies, GW | Law, The George Washington University, Washington, DC

Deanne E. Maynard, Morrison Foerster, Washington, DC

SECTION 20

Cyber-Rights and Cyber-Wrongs: Legal Ethics in a Digital Age

Sherman W. Kahn, Mauriel Kapouytian Woods LLP, New York, NY

Joseph V. DeMarco, DeVore and DeMarco LLP, New York, NY

SECTION 1

Developments in Copyright Law



Presented by

Evan M. Rothstein
Arnold & Porter Kaye Scholar LLP
Denver, CO

Year in Review: 2018 Copyright Cases

Flo & Eddie, Inc. v. Sirius XM Radio, Inc., 229 So. 3d 305 (Fla. 2017)

Case Decided: October 26, 2017

- Sirius XM Radio broadcast certain songs by The Turtles to subscribers located in Florida.
- Sirius XM did not secure a license to broadcast the songs, nor did it pay royalties to Flo & Eddie (the founding members of the Turtles).
- Flo & Eddie sued for copyright infringement, arguing that Sirius XM's broadcasts constituted unauthorized public performances of the recordings.
- The suit only involved recordings by The Turtles made prior to 1972. Pre-1972 recordings are in a legal gray area, as they are protected by state law rather than the federal copyright system that protects songs recorded after 1972.
- The Florida Supreme Court found that Flo & Eddie do not have the exclusive right to the performance of their sound recordings under Florida law.
- Both Florida's legislature and Congress have declined to recognize a common law right of public performance for pre-1972 recordings.
- Thus, the court found that Flo & Eddie have no right to collect royalties from their pre-1972 recordings.
- Conclusion: This suit is the latest in a series of cases across the country attempting to get recognition for performance rights that would require traditional radio stations and digital services (e.g. Pandora) to pay hundreds of millions of dollars in royalty fees for pre-1972 songs.

Williams v. Gaye, 895 F.3d 1106 (9th Cir. 2018)

Case Decided: March 21, 2018

- Marvin Gaye's estate brought suit against Pharrell Williams and Robin Thicke, claiming that their song "Blurred Lines"—the best-selling song in the world in 2013—infringed the copyright to Marvin Gaye's "Got to Give it Up."
- Thicke had previously admitted in an interview that "Got to Give it Up" was one of his favorite songs, and that he told Williams they should write a song with the same "groove"
- This dispute is similar to a number of recent copyright disputes over the likeness between songs by different artists.
- For instance, Sam Smith settled a copyright dispute with Tom Petty over the likeness between Smith's "Stay with Me" and Petty's "I Won't Back Down" (<https://www.youtube.com/watch?v=YflFw9T77FQ>).
- The district court found that "Blurred Lines" does infringe the copyright to "Got to Give it Up" (<https://www.youtube.com/watch?v=ziz9HW2ZmmY>).
- This decision prompted a significant amount of outrage, with over 200 prominent musical artists signing an amicus brief urging the appeals court to overturn the district court's decision.
- The musicians wrote that "[t]he verdict in this case threatens to punish songwriters for creating new music that is inspired by prior works. All music shares inspiration from prior musical works, especially within a particular musical genre."
- However, the Ninth Circuit upheld the district court's decision. The court also upheld damages of \$5.3 million.

- The court did not resolve the question of whether the scope of Gaye’s copyright is limited to the sheet music, or if it extends to the commercial sound recording.
- Conclusions:
 - Critics, including the dissenting judge, believe that this case has gone too far by allowing Gaye’s estate to copyright a general “musical style,” rather than specific expression.
 - The ruling has widely been recognized as a departure from previous thinking on how copyright law applies to music.

Cortés-Ramos v. Sony Corp., 889 F.3d 24 (1st Cir. 2018)

Case Decided: May 4, 2018

- Cortés-Ramos sued Ricky Martin, Sony and its affiliates in 2014 alleging that he was not compensated for Martin’s use of his song in creating “Vida.”
- The district court dismissed the suit with prejudice because the claims were subject to a mandatory arbitration agreement Cortés-Ramos signed when he entered a songwriting contest co-sponsored by Sony.
- Sony subsequently awarded attorney’s fees as the “prevailing party” pursuant to § 505 of the Copyright Act.
- First Circuit reversed district court’s order granting attorney’s fees to Sony.
 - Sony does not qualify as a “prevailing party” under the Copyright Act because compelling arbitration did not materially alter the parties’ legal relationship.
 - “[T]he touchstone of the prevailing party inquiry . . . [is] the material alteration of the legal relationship of the parties *in a manner which Congress sought to promote in the fee statute.*”
 - Cortés-Ramos’s claims were not “extinguished, but [] merely left to the arbitrator” and the Copyright Act “reflects no congressional policy favoring or disfavoring arbitration of claims.”
- Conclusion: compelling arbitration does not result in prevailing party for purposes of awarding attorney’s fees under the Copyright Act.

Goldman v. Breitbart News Network, LLC., 302 F. Supp. 3d 585 (S.D.N.Y. 2018)

Case Decided: February 15, 2018

- Justin Goldman photographed Tom Brady with Boston Celtics manager Danny Ainge and published the photo on Snapchat. The photo went viral and was copied and republished (without permission) on Twitter.
- Breitbart News and other news outlets featured Goldman’s copyrighted photo by embedding these tweets within news articles. The articles claimed that Tom Brady was helping the Boston Celtics to recruit basketball player Kevin Durant.
- Goldman sued the news outlets for copyright infringement.
- The Southern District granted partial summary judgment to the plaintiff and denied the defendant’s motion for summary judgment.
- In July 2018, the Second Circuit denied a Petition for leave to appeal an interlocutory order, finding that an immediate appeal is unwarranted.
- Takeaway: embedded images (images hosted on a third-party server) can constitute copyright infringement.

- The Copyright Act of 1976 gives a copyright owner “display rights:” “the right to transmit or otherwise communicate . . . a display of the work . . . To the public, by means of any device or process.”
 - The court reviewed the legislative history and determined that drafters of the 1976 Amendments “intended copyright protection to broadly encompass new, and not yet understood technologies.”
- The Copyright Act does not require physical possession of an image in order to infringe the owner’s display right.
 - Each defendant actively embedded code from Twitter into their websites to display the image seamlessly on their webpages.
 - “[L]iability should not hinge on invisible, technical processes imperceptible to the viewer.”

Naruto v. Slater, 888 F.3d 418 (9th Cir. 2018)

Case Decided: April 23, 2018

- In 2011, Naruto, a crested macaque monkey in Indonesia, took selfies on a wildlife photographer’s unattended camera.
 - These selfies were ultimately published in the book *Wildlife Personalities*.
- PETA filed suit on behalf of Naruto against the photographer and book publishers, claiming that the defendants infringed on Naruto’s copyright on the selfies by “falsely claiming to be the photographs’ authors and by selling copies of the images” for profit, and that the profits should go to Naruto.
- Defendants moved to dismiss the case, writing: “A monkey, an animal rights organization and a primatologist walk into federal court to sue for infringement of the monkey’s claimed copyright. What seems like the setup for a punchline is really happening. It should not be happening.
- The case settled in 2017 but the Ninth Circuit weighed in anyway, affirming the district court’s dismissal of the action and finding that Naruto lacked standing.
- Because the Copyright Act does not expressly authorize animals to file copyright infringement suits, Naruto lacked statutory standing (but he did have Article III standing as the complaint fairly stated a “case or controversy” involving a redressable harm).
- The court primarily used its opinion as an opportunity to criticize PETA, stating that PETA “employ[ed] Naruto as an unwitting pawn in its ideological goals” (by obtaining a settlement that did not directly benefit Naruto but involved donating proceeds to charities working to protect monkeys).
- Conclusions:
 - Non-human animals may only sue under a federal statute if the statute itself explicitly authorizes it.
 - Non-human animals have constitutional standing if they fairly allege a case or controversy.



Oracle America, Inc. v. Google LLC, 886 F.3d 1179 (Fed. Cir. 2018)

Case Decided: March 27, 2018

- Oracle initially filed suit in 2010, alleging that Google’s unauthorized use of several thousand lines of Oracle’s Java programming code infringed on Oracle’s copyright. The code is used in application programming interfaces (APIs) (instruction sets that enable one computer program to share data with another).
- Google’s Android uses Oracle’s copyrighted material in 11,000 of its 13 million lines of software code.
- Oracle initially sought \$9 billion from Google. Google estimates it has made \$21 billion in profits from Android since they began production in 2007.
- Google argues fair use, claiming the use of the copyright was relatively small, as well as transformative, because Java had not been previously been tweaked for use in mobile devices.
- Jury below made two findings: 1) the APIs were copyrightable (sufficiently original, expressive and fixed); and 2) Google’s use of the copyright-protected APIs was excusable fair use.
- Federal Circuit reviewed the four factors in the fair use analysis and found that, on balance, they showed Google’s use was not fair use:
 - 1) Purpose and character of use - Court found that the highly commercial and non-transformative nature of the use weighed this factor in Oracle’s favor. They also found the use to be non-transformative, because the APIs served identical functions and purpose in Java and Android.
 - 2) Nature of copyrighted work - Court found that a reasonable jury could have concluded that functional considerations were substantial and important (weighing in Google’s favor), but also noted that this factor is not very significant in the balancing.
 - 3) Amount and substantiality of portion used - Court found that no reasonable jury could find that the copied material was qualitatively insignificant. Moreover, Google conceded that they could have written the interface differently but it chose not to.
 - 4) Effect upon potential market - Court found evidence of actual and potential harm for the market of the original product and its derivatives.
- Conclusions:
 - Google is pushing for greater openness and latitude in copyright. The Federal Circuit’s decision endorses a more strict “license as you go” model. This approach may have an impact on open-source software development. Some argue that it reduces the incentive to produce.
 - The Court’s decision arguably means that virtually no use of a functional work could be transformative, because copied elements would invariably perform the same function in the new work. There is concern that this view would constrain legitimate competition.
 - Converse of this is simple: get a license.
 - Google argues that the Federal Circuit’s opinion concludes that “a firmly established, widely practiced method of designing computer software violates copyright law.” They stated that “had the panel’s decision been the law at the inception of the Internet age, early computer companies could have blocked vast amounts of technological development by claiming 95-year copyright monopolies over the basic building blocks of computer design and programming.”

- Even a relatively small amount of use (here was only 0.08% of Android’s software code) can have massive legal implications.

Fox News Network, LLC v. Tveyes, Inc., 883 F.3d 169 (2d Cir. 2018)

Case Decided: February 27, 2018

- TVEyes is “a media monitoring company that offers a platform enabling users to search, view, distribute, analyze and archive media content available on television, radio, print and social media.” It collects recordings of broadcasts across more than 1,400 television and radio stations. Subscribers are able to search these recordings by using key words or phrases. Once they have identified videos containing relevant information, they are able to watch a clip of the program that is up to 10 minutes in length.
- Fox accused TVEyes of profiting off of its broadcasting without a license. TVEyes claimed fair and transformative use.
- Second Circuit reversed the S.D.N.Y.’s finding of fair use and instead held that the recording and retrieval services offered by TVEyes infringed on Fox’s copyright.
 - Court found that changing the TV programs to video clips was not sufficiently transformative to excuse the infringement under the first fair use factor. TVEye’s clients used their service for the same purpose that Fox’s viewers used those broadcasts.
 - The third factor (nature of copyrighted work) favored Fox. Given the short length of most news segments, the 10 minute clips were enough to negate the need to watch Fox news (compare with *Google Books* case where only a snippet of the book was available).
 - The court also found that the fourth factor clearly favored Fox, as their market was usurped and this was a derivative use.
 - Court held that TVEyes was unlawfully profiting of the work of Fox by distributing that work commercially and isolating all that a viewer wished to use, without any payment or license to Fox.
- The decision barred only TVEyes’ feature that allowed clients to watch clips. The company is not infringing by compiling a text-searchable database of television and radio broadcasts.
- Conclusions:
 - Transformative use can be seen as a parameter within the analysis of the first fair use factor (comparing the purpose and character of the new use with the original use), rather than as its own analysis. The strength of the first factor in this case was undercut by the commercial use.
 - Although the work was moderately transformative, the effect on Fox’s prospective revenue was too great.

Cohen v. G & M Realty L.P., 320 F. Supp.3d 421 (E.D.N.Y. 2018)

Case Decided: February 12, 2018



- 5Pointz Aerosol Art Center was an outdoor exhibition space in New York City that operated as a graffiti “museum” for twenty years - attracting visitors, artists, photographers, filmmakers, etc. The owner of the building, Gerald Wolkoff, gave the initial permission to the artists to paint on the building. Wolkoff made clear from the outset that 5Pointz would not be permanent.
- Since 1993, around 1,500 artists contributed to the constantly evolving site, often painting over one another’s work.
- As the surrounding neighborhood gentrified and housing prices increased, Wolkoff whitewashed the 5Pointz Aerosol Art Center before and after whitewashing building in the middle of the night. The building was later torn down to make way for new condominiums.
- 21 Artists filed suit, alleging that their work was protected under copyright provisions of the Visual Artists Rights Act of 1990 (VARA), which grants artists the right to protect their work from distortion, mutilation or modification. This includes, in some cases, protecting artists against the destruction of their work that is incorporated into a building.
 - The artists were not given advance notice of the whitewashing and were unable to remove or document their work. Under the statute, Wolkoff could have given 90 days’ notice to allow for attempted salvage of the works.
- Jury found in favor of the artists and found the graffiti to be of “recognized stature,” entitling the artists to damages under VARA.
- Court awarded maximum statutory damages (\$6.75 million total) under VARA for each of the 45 works of art it found were wrongfully and willful destroyed.
- Conclusions:
 - Case recognizes aerosol art (graffiti) are as a fine art and subject to VARA.
 - Even as owners of property, developers do not have the unfettered ability to do as they wish with their own property. They are subject to the rights of the artist to preserve and protect their work.
 - Just because art is public, temporary or free does not make it disposable.
 - If a building owner is in a position where it must remove art protected by VARA, a written VARA waiver should be obtained. If no waiver is obtained, the owner should proceed cautiously and in good faith in the destruction or removal of the art.
 - Bad faith mattered to the Court here. Judge Block wrote: “If not for Wolkoff’s insolence, these damages would not have been assessed. If he did not destroy 5Pointz until he received his permits and demolished it 10 months later, the Court would not have found that he had acted willfully.”

BMG Rights Management LLC v. Cox Communications, Inc., 881 F.3d 293 (4th Cir. 2018)

Case Decided: February 1, 2018

- BMG Rights Management, a music publisher, brought suit against Cox, an internet service provider, alleging that Cox allowed its users to pirate the company’s music.
 - BMG argued that Cox ignored thousands of notices of infringement.
- The Digital Millennium Copyright Act’s safe harbor provisions shields internet service providers from potential liability linked to illegal behavior by their users. However, in order for these provisions to kick in, providers must reasonably implement a policy to terminate repeat infringers.

- Fourth Circuit affirmed the trial court finding that Cox could not be afforded the copyright immunity because, while they “formally adopted a repeat infringer ‘policy’ [...] [Cox] made every effort to avoid reasonably implementing that policy.” The Court went so far as to state that “Cox very clearly determined *not* to terminate subscribers who in fact repeatedly violated the policy.”
- Fourth Circuit overturned \$25 million infringement verdict, finding that the trial judge had improperly instructed jurors that Cox could be found liable merely if it “should have known” that subscribers were pirating music. The Court said this instruction reflects a negligence standard which is too low.
- BMG and Cox reached a settlement on August 24.
- Conclusions:
 - Reasonable implementation of a policy requires more than a formal implementation. It also requires meaningful enforcement.
 - The Court rejected Cox’s reading of the “repeat infringer” rule as only requiring providers to terminate users who have been found liable of infringement. Repeat accusations are sufficient to require termination of these users.

Davidson v. United States, 138 Fed. Ct. 159 (Fed. Cl. 2018)

Case Decided: June 29, 2018

- The United States Postal Service (USPS) redesigned their “Forever” stamps using a photo of what they believed was the Statue of Liberty that they found on Getty Images. They paid \$1,500 to license the photo. However, it was later discovered that the photo was actually taken of a replica Statue of Liberty located at the New York, New York Hotel & Casino in Las Vegas.
- Robert Davidson, the sculptor of the Las Vegas replica statue, sued USPS for copyright infringement.
- Between 2010 and 2014, USPS produced and sold 4.9 billion Forever stamps featuring Davidson’s statue, collecting over \$70 million in profit.
- The Court found in favor of Davidson and awarded him \$3.5 million in damages (the amount was calculated as a 5% royalty on the USPS’s profits on the stamp).
 - Davidson was able to show creativity and a nontrivial variation from the original statue. The Court was persuaded by his testimony that he sought to give his sculpture fresher and more feminine features than the original, which he described as “harsher” and “more masculine.” The court noted the softened jaw line, rounded face and modified eyes and lips of Davidson’s statue.
- Although USPS had paid a licensing fee, the photo itself was an infringing work as it was posted on Getty Images without Davidson’s permission. Continued distribution by USPS therefore constituted an additional infringement.



The original Statue of Liberty (left) vs. Davidson’s replica (right)

- Conclusions:
 - Even something that, to most casual viewers, appears to be a replica of a famous work of art, can be copyrightable. What matters is the showing of a “new and original expression of some previous work or idea.” To render his work copyrightable, Davidson needed only to show a “modicum of creativity.”

Graham v. Prince et al. (Case No. 1:15-CV-10160, S.D.N.Y.)

Currently ongoing (Motion for Summary Judgment filed by Prince on October 5, 2018)

- Controversial “appropriation artist” Richard Prince, who is no stranger to copyright suits (*Cariou v. Prince*, 714 F.3d 694 (2d. Cir. 2013)) is being sued for his use of various Instagram photos in an installation called “New Portraits” at the Gagosian Gallery. The installation was comprised of screenshotted Instagram photos printed on large canvases, with Prince adding his own Instagram-style comment below the photo.
- Photographer Donald Graham brought suit against Prince and the Gagosian for copyright infringement. Graham’s photo “Rastafarian Smoking a Joint” was featured in the installation via a print from another user’s Instagram account.



Graham’s original photo (left) was posted by the Instagram user rastajay92. Prince then took this Instagram photo, added his own comment to the bottom and displayed it at the Gagosian with a series of similar prints (right).

- Graham’s lawsuit is one of four others filed by photographers whose images were used in the “New Portraits” installation.
- Prince’s motion to dismiss was denied in July 2017. S.D.N.Y Judge Stein challenged Prince’s argument that his work was transformative.
 - “Prince’s ‘Untitled’ does not make any substantial aesthetic alterations [...] The primary image in both works is the photograph itself. Prince has not materially altered the composition, presentation, scale, color palette and media originally used by Graham.”
- In October 2018, Prince filed a motion for summary judgment, arguing fair use.
 - In a declaration in support of the motion, Prince refers to his iPhone as a paintbrush and explains that he sought “to reimagine traditional portraiture and bring to canvas and art gallery a physical representation of the virtual world of social media.” He argues that this intent would not have been properly conveyed had he altered the photos.

- Prince argues that he did not usurp Graham’s market because their work appeals to different buyers. He also claims that Graham benefited from his appropriation, noting that his photograph has only increased in value since being used by Prince. Prince sold some of the pieces from his installation for up to \$100,000.
- Prince argues that he “transformed the photograph from a documentary photographic portrait to commentary on the nature of social media.”
- Issues:
 - How does the fair use doctrine relate to Instagram? What role does copyright law play in social media?
 - What role does the brand of the artist play in the fair use factors? Does the doctrine give too much leeway to well-known artists who appropriate works of their relatively unknown peers? In these cases, will the fourth fair use factor always point in favor of the artist who is appropriating because the value of the unknown work usually increases or because there is no real market overlap?
 - Can relate to appropriation of images that happens every day through memes (where you have a similar exercise of posting someone else’s image and simply adding words).

Andy Warhol Foundation v. Lynn Goldsmith (Case No. 1:17-cv-02542, S.D.N.Y.)

Currently ongoing (Motion for Summary Judgment filed October 12, 2018)



Portrait of Prince by Warhol (left) compared with Goldsmith’s photograph (right).

- Goldsmith publicly asserted that Warhol infringed on her copyrighted photo of Prince, taken in 1981. Warhol created a series of photos of Prince in 1984, using publicity photos of Prince as “inspiration.”
- The Warhol Foundation preemptively filed suit, seeking a declaration of non-infringement and fair use, to “protect the legacy of Andy Warhol.” Moreover, they allege that Goldsmith attempted to “shake down the foundation,” demanding a “substantial” sum of money.
- The Warhol Foundation claims the

portraits are transformative or otherwise protected by fair use. They point to aesthetic differences between the photograph and Warhol’s portrait (e.g. Prince having heavier eye makeup in the Warhol prints and his hair appearing to be a more solid block of color).

- While the Foundation admits Warhol “often used photographs taken by others as inspiration” for his appropriation portraiture, they describe his portraits as “entirely new creations.”
- They claim Warhol’s work “comments on consumer culture and explores the relationship between celebrity culture and advertising.”
- As to the fourth fair use factor, they argue that Warhol did not usurp Goldsmith’s market because she had not licensed the photo, and she and Warhol did not share the same audience (art collectors/commercial markets).

- Goldsmith argues that the Warhol series copies her photograph, contains derivative works and is not transformative or otherwise protected fair use.
 - She notes that the aesthetic changes in Warhol’s portrait are “relatively minimal” and that the series retains the essence, composition and key elements of her photograph.
 - Goldsmith contends that her and Warhol share licensing markets (ex: magazines), that her photographs have been showcased in museums, and that a prominent collector owns one of her Prince photographs as well as Warhol’s works.
- The Warhol Foundation also asserts that Goldsmith’s claims are barred by the statute of limitations (since Warhol’s portrait appeared in Vanity Fair in 1984 and had been widely disseminated in museums, books and auctions by the 1990s). Goldsmith claims she was not made aware of the photo until 2016, when she saw images of Warhol’s portrait on Instagram following Prince’s death.
- Issues: when is appropriation art fair use and when is it an infringement?

Michael Skidmore v. Led Zeppelin et al., 905 F.3d 1116 (9th Cir. 2018)

Case Decided: September 28, 2018

- Owner of copyright for song “Taurus” by the band Spirit brought action against Led Zeppelin and others, alleging “Stairway to Heaven” infringed on its copyright.
 - Comparison:
 - https://www.youtube.com/watch?v=ye7hCIWwhGE&list=RDye7hCIWwhGE&start_radio=1&t=0
- Skidmore’s expert testified that there was substantial similarity between the two songs based on the combination of five elements -- some of which were protectable and some of which were in the public domain.
- At trial, jurors could only listen to renditions of the sheet music for Taurus, not the original recorded version performed by Spirit.
- District Judge instructed the jury that common musical elements, such as “descending chromatic scales, arpeggios, or short sequences of three notes,” were not protected by copyright.
- Jury below returned a verdict in favor of Led Zeppelin, finding the protectable elements in the two songs dissimilar for the purposes of copyright infringement.
- The Ninth Circuit ordered a new trial, finding that several of the district court’s jury instructions were erroneous and prejudicial.
 - District Judge failed to advise jurors that, while individual elements of a song may not qualify for copyright protection, a combination of those elements may qualify if the arrangement is sufficiently creative and original.
 - The Circuit also held that jurors should have been permitted to hear the original recording of Taurus, in order to fairly compare the two songs.
- Takeaways:
 - Selection and arrangement of otherwise unprotectable musical elements are protectable.
 - The original part of the work need not be new or novel. The Ninth Circuit emphasized that there is a low bar for originality in copyright.
 - Led Zeppelin has petitioned for a rehearing en banc, saying the Court’s ruling improperly extends copyright protections to material that should be in the public domain and

therefore upsets “the delicate balance between protecting authors of original material, and the freedom to use public domain elements.”

- The Recording Industry Association of America has filed an amicus brief supporting the petition, arguing that “the panel opinion broadly overprotects.” While they agree that “composers’ intellectual property must be protected,” they caveat that “new songs incorporating new artistic expression influenced by unprotected, pre-existing thematic ideas must also be allowed.”

Fourth Estate Public Benefit Corp. v. Wall-Street.com, LLC, 856 F.3d 1338 (11th Cir. 2017), cert. granted, No. 17-571 (US June 28, 2018)

Supreme Court granted writ of certiorari petition on June 28, 2018

- Fourth Estate licensed journal articles to Wall-Street. Wall-Street later cancelled the agreement but did not remove Fourth Estate’s content (as was required in the agreement). Fourth Estate filed suit for copyright infringement.
- Wall-Street moved to dismiss because the Copyright Office had not yet approved Fourth Estate’s application for registration, barring them from bringing suit under § 411(a).
 - District court granted dismissal and Eleventh Circuit affirmed, holding that filing an application does not amount to registration under §411(a).
- Supreme Court to consider question of whether a copyright owner can commence an infringement lawsuit as of the date of application for registration, or as of the date when the US Copyright Office has approved or denied the application.
 - Circuits are split between two approaches under 17 U.S.C. § 411(a):
 - Application approach - can bring lawsuit “once the copyright [owner] delivers the required application, deposit and fee to the Copyright Office.”
 - Courts that rely on this approach have relied on text of 17 U.S.C. § 410(d) (stating that the effective date of a copyright registration is the day on which the application, deposit and fee were received by the Copyright Office).
 - Registration approach - can bring lawsuit only once “the Copyright Office acts on that application.”
 - Courts that rely on this approach look at the plain text of § 411(a).
- Issues:
 - Clarification on the preconditions on copyright infringement actions imposed by 17 U.S.C. § 411(a). This may impact current suits that were filed when copyright owners had pending applications for registration.

Donald Trump’s Copyright Woes

- The President has a long history of popular musicians rejecting the use of their music at his rallies. In the last month alone, four musicians have publicly demanded Trump discontinue the use of their songs while campaigning:
 - Prince’s estate issued a statement on October 13, warning Trump to cease using the song “Purple Rain” after it played at one of his pre-midterm election rallies.
 - After learning that Trump played his song “Happy” at an Indiana rally just hours after the Tree of Life massacre, Pharrell Williams served Trump an impassioned cease-and-desist letter, demanding that the President stop playing “Happy” at his rallies and criticizing him for using the song following the atrocity.

- On November 4, Rihanna took to Twitter after learning that her song “Please Don’t Stop the Music” was played by Trump at a rally in Tennessee, tweeting: “Not for much longer ... me nor my people would ever be at or around one of those tragic rallies.”
- After finding out that Trump played “Sweet Child ‘o Mine” at a rally in West Virginia on November 2, Axel Rose took to Twitter to publicize that he and Guns N’ Roses formally denied Trump permission to use their music.

SECTION 2

Developments in Trademark Registration Practice



Presented by

Hope Hamilton
Holland & Hart LLP
Boulder, CO

National CLE Conference®

Developments in Trademark Registration Practice



Hope Hamilton

Holland & Hart LLP

Boulder, Colorado

<https://www.hollandhart.com/hihamilton>

National CLE Conference

January 2-6, 2019

Aspen, Colorado

(Materials submitted October 31, 2018)

I. TRADEMARK POLICY CHANGE DEVELOPMENTS AND PILOT PROGRAMS

A. Mandatory Electronic Filings

- The USPTO has published a proposed rulemaking to amend the Rules of Practice to mandate electronic filing of all trademark applications and submissions associated with trademark applications and registrations.
- The period for comments ended July 30, 2018, and it is estimated that implementation may go into effect early 2019.

B. Requirement for U.S. Counsel for Foreign Applicants and Registrants

- In response to a recent flood of questionable foreign applications (including a substantial number from China), the USPTO is considering a policy change requiring foreign trademark applicants and registrants to hire U.S. counsel.
- Goals include (1) streamlining the application process by having experienced practitioners involved from the inception, and (2) reducing fraudulent or void applications, which have become a strain on Trademark Examiners, as well as the Trademark Trial and Appeal Board (TTAB).
- A Notice of Proposed Rulemaking will publish November 1, 2018.

C. Note About Domestic Representatives

- Some jurisdictions, like the EU and Japan, require that an applicant appoint a representative after filing an application. The USPTO does not have this requirement.
- It is important to note that a Domestic Representative is not the same as an Attorney of Record, and this has become increasingly important since the TBMP Rules were updated to require that the USPTO serve oppositions/cancellations.
 - *See* TBMP § 309.02(c)(2) (“Board will endeavor to forward a courtesy copy of the notice to the international registration holder’s designated representative which will include a web link or web address to access the electronic proceeding record.”).
- Foreign trademark owners should strongly consider appointing a Domestic Representative for service/notice of cancellations and other post-registration notifications.

D. Specimen Protest Pilot Program

- The USPTO will re-examine an application in response to a specimen protest that offers objective evidence of a fraudulent specimen. Submission should be:
 - made via email to TMSpecimenProtest@uspto.gov
 - include Serial Number of application being protested in email Subject Line
 - include in body of email either:
 - Objective evidence of third party use of the identical image without the mark in question, such as the URL and screenshot from an active website or a digital copy of a photograph from a print advertisement and the publication in which it was featured; **OR**
 - The prior registration numbers and/or serial numbers of applications in which identical images of objects, mock-ups of websites, etc., all bearing different marks have been submitted to the USPTO.
- Outcome of protest must be tracked via status of application on TSDR.

E. Proof of Use Audit Program

- Launched November 1, 2017 to “assess and promote the accuracy of the trademark register.” Audits are conducted to determine if a mark is in use with all services identified in a registration.
- Selection for the audit is random, and approximately 2,000 registrations have been audited so far. Section 44(e) and 66(a) Registrants comprise nearly 30% of these audits.
- A registrant may be audited if it makes a post-registration filing (e.g., declaration of use or renewal) AND the registration includes (1) at least one Class with four or more goods/services, or (2) at least two Classes with two or more goods/services.
- If audited, registrants must:
 - Respond within six months
 - Submit acceptable specimens for *each* good or service in the registration

- Acceptable specimens must show use within the relevant period for filing the Affidavit of Use (e.g., use that commenced after the 6-month audit response period begins is not acceptable).
- Practice Tip: Carefully review registrations at maintenance/renewal and delete goods/services for which there is no use or no specimen.

F. Unauthorized Changes To Active Trademark Records

- The USPTO announced that there has been a recent trend in unauthorized changes to active trademark applications and registrations, which the USPTO says may be part of a scheme to register the marks of others on third-party “brand registries.”
- To combat this, the USPTO has implemented an automated email message alert when a change is made to the primary correspondence email address.
- Practice Tip: If you receive one of these emails, do not ignore it. Verify that the change was authorized, and if it was not, report it to the USPTO and take steps to correct it. Additional information is available here: <https://www.uspto.gov/trademark/trademark-updates-and-announcements/unauthorized-changes-your-file>

II. PRECEDENTIAL 2018 TRADEMARK TRIAL AND APPEAL BOARD CASES RELATED TO TRADEMARK REGISTRATION PRACTICE

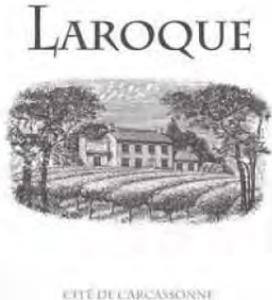
A. Scandalous & Disparaging Marks – Section 2(a)

The big news from 2017 was the Supreme Court’s decision in *Matal v. Tam*, 137 S. Ct. 1744 (2017), finding that the bar against “disparaging” marks was unconstitutional because it constituted “viewpoint discrimination.”

We are now watching for possible Supreme Court action in the case of *Iancu v. Brunetti* involving the mark FUCT for clothing. The USPTO refused registration on the grounds that the mark was vulgar and obscene and therefore barred by Section 2(a), which prohibits registration of “scandalous” marks. The applicant appealed to the TTAB (which affirmed the refusal), then to the Federal Circuit, which cited *Matal v. Tam* in holding that the bar in Section 2(a) against registering “scandalous” marks is unconstitutional under the First Amendment. *In re Brunetti*, 877 F.3d 1330 (Fed. Cir. 2017).

On September 7, 2018, the USPTO submitted a Petition for Writ of Certiorari (Case No. 18-302), arguing that determination of a scandalous mark is viewpoint-neutral, and that the First Amendment does not prohibit Congress from making vulgar terms and graphic sexual images ineligible for federal trademark registration. The applicant’s response is due November 8, 2018.

B. Likelihood of Confusion – Section 2(d) - Summary of Precedential Decisions

Applicant/Registrant Mark	Cited Mark / Adverse Party	Outcome
<p>populace</p> <p>Class 9: Computer application software for mobile phones and desktop computers, namely, software for visualizing the popularity of places in real time, that uses an underlying map capability for navigation, sold as ‘business to consumer’ (B2C) software, and not as ‘business to business’ (B2B) software</p>	 <p>Class 9: Downloadable mobile applications for mobile phones and mobile electronic devices, primarily software for travel and destination marketing organizations and travel marketing professionals</p>	<p>Refusal to Register Affirmed</p> <p><i>In re Solid State Design, Inc.</i>, 125 U.S.P.Q.2d 1409 (TTAB Jan. 3, 2018)</p> <ul style="list-style-type: none"> - POPULACE is dominant - Board must presume same trade channels and consumers.
<p>IPAD</p> <p>Classes 35, 38, 39, 42: Various, including computerized database and file management; data processing services; providing business and commercial information over computer networks and global communication networks</p>	 <p>providing temporary use of a web-based software application for mobile-access database management whereby users can store and access their personal information</p>	<p>Opposition Dismissed in Favor of Applicant</p> <p><i>RxD Media, LLC v. IP Application Development LLC</i>, 125 U.S.P.Q.2d 1801 (TTAB Feb. 22, 2018)</p> <ul style="list-style-type: none"> - Opposer failed to prove use of IPAD as standalone mark - IPAD also merely descriptive, and Opposer failed to prove acquired distinctiveness as of Applicant’s constructive priority dates. <p>On appeal to in the EDVA, 1:18-cv-00486-LO-TCB</p>
 <p>Cité de Carcassonne disclaimed</p> <p>Class 33: Wine of French origin protected by appellation of the origin Cité de Carcassonne</p>	<p>CHATEAU LAROQUE</p> <p>Class 33: Wines having the controlled appellation Saint-Emilion Grand Cru</p>	<p>Refusal to Register Affirmed</p> <p><i>In re Aquitaine Wine USA, LLC</i>, 126 U.S.P.Q.2d 1181 (TTAB Apr. 2, 2018)</p> <ul style="list-style-type: none"> - Marks share dominant term LAROQUE - Words are accorded greater weight in design marks - Depiction in design connotes a chateau or estate

Applicant/Registrant Mark	Cited Mark / Adverse Party	Outcome
<p>KEMI OYL</p> <p>OYL disclaimed</p> <p>Class 3: cosmetics; eyebrow cosmetics; sun-tanning preparations; shampoo, conditioners, hair dye, soap for body care; skin moisturizer; cosmetic creams for skin care; lotions for face and body care; skin lighteners; hair lighteners; powdered hair bleach</p>	<p>KEMI OYL</p> <p>Alleged common law rights for variety of hair and skin care products</p>	<p>Petition for Cancellation Granted in Favor of Petitioner</p> <p><i>Kemi Organics, LLC v. Rakesh Gupta</i>, 126 U.S.P.Q.2d 1601 (TTAB May 15, 2018)</p> <ul style="list-style-type: none"> - ACR program used and the parties stipulated that confusion was likely - Petitioner established by preponderance of evidence priority of use - Three-years delay in filing petition did not create laches bar¹
 <p>Class 43: restaurant and bar services</p>	<p>5IVESTEAK</p> <p>Colors disclaimed</p> <p>Class 43: restaurant and bar services</p>	<p>Refusal to Register Affirmed</p> <p><i>In re Inn at St. John's LLC</i>, 126 U.S.P.Q.2d 1742 (TTAB June 6, 2018)</p> <ul style="list-style-type: none"> - Evidence of third-party registrations, without evidence of use, afforded limited probative value - Applicant owned an existing registration for stylized 5IVE RESTAURANT mark (13th Factor), but STEAK/STEAKHOUSE overlap compelled refusal <p>On appeal to Federal Circuit, No. 18-2236</p>
<p>I LOVE YOU</p>  <p>Class 14: Bracelets</p>	<p>ILUV U</p> <p>Class 14: jewelry, namely, necklaces, bracelets, rings and charms; pendants; earrings</p>	<p>Refusal to Register Affirmed</p> <p><i>In re Peace Love World Live, LLC</i>, 127 U.S.P.Q.2d 1400 (TTAB July 23, 2018)</p> <ul style="list-style-type: none"> - Applicant argued mark was weak and coexisting with many other I LOVE YOU formative marks for jewelry – but Board found cited mark to be too similar - Also refused because it fails to function as a mark, merely ornamental, merely informational

¹ Compare *TPI Holdings, Inc. v. TrailerTrader.com, LLC*, 126 U.S.P.Q.2d 1409 (TTAB Apr. 24, 2018) (precedential), concluding that Petitioner's likelihood of confusion claim was barred by laches after delay of more than four years.

Applicant/Registrant Mark	Cited Mark / Adverse Party	Outcome
<p>#WILLPOWER</p> <p>Class 25: Various clothing items, including headwear, jackets, pants, shirts, footwear</p>	 <p>Class 25: Hats; Jackets; Pants; Shirts; Shoes</p>	<p>Refusal to Register Affirmed</p> <p><i>In re i.am.symbolic, llc</i>, 127 U.S.P.Q.2d 1627 (TTAB Aug. 16, 2018)</p> <ul style="list-style-type: none"> - Analysis of similarity based on average customer, who retains a general rather than specific impression of marks - Both marks share dominant term WILLPOWER - Dismissed differences based on side-by-side comparison or consumers familiar with persona - # symbol or word HASHTAG generally afford little to no source-indicating distinctiveness - Evidence of five other coexisting uses of WILLPOWER only somewhat probative, declined to find mark weak <p>Appealed to Federal Circuit, No. 19-1077</p>
<p>I'M SMOKING HOT</p> <p>Class 3: Various cosmetics and personal care products</p>	<p>SMOKIN' HOT SHOW TIME</p> <p>Class 3: cosmetics, mascara</p>	<p>Refusal Reversed</p> <p><i>In re FabFitFun, Inc.</i>, 127 U.S.P.Q.2d 1670 (TTAB Aug. 23, 2018)</p> <ul style="list-style-type: none"> - SMOKIN' HOT/SMOKING HOT both conceptually weak and diluted for beauty products - Board gave weight to additional terms in marks (I'M / SHOW TIME) to find differences in appearance, sound, and connotation
<p>AMERICAN CONSTELLATION</p> <p>Class 39: Cruise ship services; transportation of passengers by ship; arranging and conducting cruises for others</p>	<p>CONSTELLATION CELEBRITY CONSTELLATION</p> <p>Class 39: Cruise ship services, arranging and conducting cruises for others, and transportation of passengers by ship</p>	<p>Refusal Reversed</p> <p><i>In re American Cruise Lines, Inc.</i>, 128 U.S.P.Q.2d 1157 (TTAB Oct. 3, 2018)</p> <ul style="list-style-type: none"> - TTAB gives "great weight" to consent agreements.

C. Section 2(e) Descriptiveness & Functionality / Section 2(f) - Acquired Distinctiveness

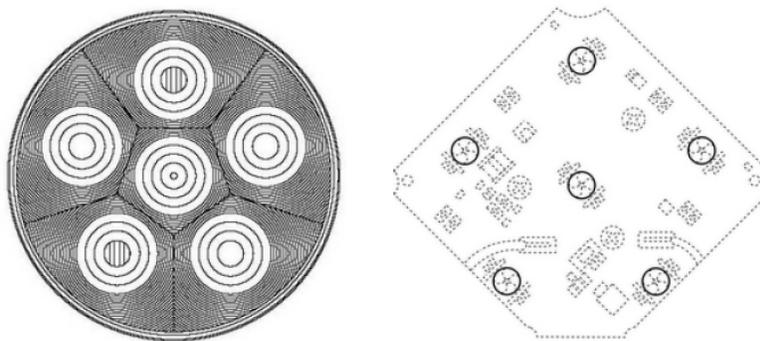
1. *In re S. Malhotra & Co. AG*, 128 U.S.P.Q.2d 1100 (TTAB Sept. 27, 2018), affirming refusal to register on merely descriptiveness grounds.

GÁMOS ΓΑΜΟΣ

Applicant sought to register the above marks (word and design). The English translation and transliteration of the design both mean “wedding, matrimony or marriage.” The application covered “precious metals and their alloys and goods made of these materials or coated therewith included in this class, namely jewelry and watches” in Class 14.

Applying the doctrine of foreign equivalence, the examining attorney refused registration on grounds that the marks were merely descriptive of the goods. The Board agreed, noting that “[a] term need not immediately convey an idea of each and every specific feature of the applicant’s goods or services in order to be considered merely descriptive; it is enough that the term describes one significant attribute, function or property of the goods or services.” Because wedding, matrimony, and marriage have descriptive significance for jewelry, the Board found the marks to be merely descriptive and unregistrable in the absence of acquired distinctiveness.

2. *Grote Industries v. Truck-Lite Co.*, 126 U.S.P.Q.2d 1197 (TTAB Mar. 30, 2018). Opposition to registration and cancellation sustained in favor of opposer/petitioner. On appeal for *de novo* review in the Western District of New York, No. 1:18-cv-00599.



Truck Lite opposed and sought to cancel Grote Industries’ applications and registration for two Penta-Star designs for vehicle lights on grounds that both are functional and lack acquired distinctiveness.

Functionality: The Board found “that (1) no patent specifically discloses the benefits of the Penta-Star Pattern; (2) the relevant advertising does not suggest a benefit arising from the pattern per se; (3) there appear to be alternative designs that satisfy federal regulations; and (4) there is no clear benefit as to either cost or ease of manufacture attributable to the pattern.”

Acquired Distinctiveness: The Board found that the record “contains insufficient probative evidence that the primary significance” of the product configuration design is to serve as a source identifier in the minds of consumers. Evidence of strong sales of a product is not, by itself, probative of purchaser recognition of a configuration as an indication of source. Witness testimony of a company executive stating that consumers recognize the lamp as source-identifying was insufficient. And purported “look for” advertising (which can be useful to demonstrate consumer recognition) did not mention the configuration as a source identifying feature.

3. *In re Serial Podcast, LLC*, 126 U.S.P.Q.2d 1061 (TTAB Mar. 26, 2018), it’s complicated.



Applicant filed three applications to register SERIAL, one standard word mark and two Composite Logo mark applications (above), all for “entertainment in the nature of an ongoing audio program featuring investigative reporting, interviewing, and documentary storytelling.”

The examining attorney refused registration on grounds that SERIAL was generic or, if not generic, merely descriptive and that the Applicant failed to show that the mark had acquired distinctiveness under Section 2(f).

Generic: Generic terms are not registrable because they are incapable of serving as a source identifier. Applicant’s SERIAL mark is used to promote an “ongoing audio program.” After considering substantial evidence showing use of the term “serial” as a noun or adjective for similar third-party programs, the Board held that the word SERIAL is generic for Applicant’s identified services. In so doing, the Board cautioning: “[M]erchants act at their peril in attempting, by advertising, to convert common descriptive names, which belong to the public, to their own exclusive use.” (Quoting *In re Pennington Seed Inc.*, 466 F.3d 1053 (Fed. Cir. 2006).)²

Acquired Distinctiveness: Relying on the same evidence of third-party uses of SERIAL, the Board also found that the standard character mark had not acquired distinctiveness as a source identifier for Applicant: “[C]ommercial success of a product or service does not

² For another precedential decision on genericness, see *In re Mecca Grade Growers, LLC*, 125 U.S.P.Q.2d 1950 (TTAB Mar. 12, 2018), in which the Board affirmed a refusal to register MECHANICALLY FLOOR-MALTED for “malt for brewing and distilling” in Class 31 and for “processing of agricultural grain” in Class 40.

necessarily mean that the consuming public perceives the mark used in connection with such products or services as primarily a source-indicator.”

Composite Marks: “A composite mark may be registrable even when its word portion, taken alone, is not.” Even though Applicant’s composite marks contain a generic or descriptive term, SERIAL, and the design elements (typeface set on a common geometric shape akin to a tile in a board game) were not inherently distinctive, the Board found that the Applicant met its high burden of proving that its logos had acquired distinctiveness. Particularly compelling was evidence of *Saturday Night Live* and *Sesame Street* parodies featuring the composite marks, as well as unauthorized merchandise and other uses seeking to capitalize on consumer recognition of the SERIAL composite marks.

Decision: The Board affirmed refusal of the SERIAL word mark on grounds of genericness and descriptiveness. The Board reversed the genericness refusal as to the Composite Logos and agreed to set aside the mere descriptiveness refusal if Applicant disclaimed the word SERIAL. (Applicant disclaimed SERIAL, and both logo marks have now registered.)

4. *In re American Furniture Warehouse CO*, 126 U.S.P.Q.2d 1400 (TTAB Apr. 12, 2018), affirmed refusal to register in absence of disclaimer.



The examining attorney refused registration to the above mark in the absence of a disclaimer of the wording “AMERICAN FURNITURE WAREHOUSE,” on grounds that AMERICAN is geographically descriptive, and FURNITURE WAREHOUSE is generic, so that the whole phrase was primarily geographically descriptive, and that FURNITURE (bottom line) was generic. The application covered “retail furniture store” in Class 35.

Notably, Applicant owned several other registrations without disclaimers and with claims of acquired distinctiveness-in-part as to AMERICAN FURNITURE WAREHOUSE. These prior registrations ended up serving as a double-edged sword. On the one hand, they undermined Applicant’s position because (1) the prior Section 2(f) claims were deemed a “concession” that the wording itself is not inherently distinctive for those services, and (2) they served as evidence that the design was not a unitary mark, with all parts being deemed inseparable. On the other hand, the Board accepted the prior registrations as sufficient evidence of acquired distinctiveness-in-part of AMERICAN FURNITURE WAREHOUSE.

The Board therefore refused the requirement that the entire term AMERICAN FURNITURE WAREHOUSE be disclaimed and instead held that the application could proceed to registration if Applicant submits a disclaimer of the generic portion, FURNITURE

WAREHOUSE, and second reference to FURNITURE on the bottom line. (Applicant submitted both disclaimers, and the mark is now registered.)

D. Color Mark or Product Packaging



In re Forney Industries, Inc., 127 U.S.P.Q.2d 1787 (TTAB September 10, 2018) (precedential), refusal to register affirmed. On appeal to the Federal Circuit, No. 19-1073.

Applicant sought to register the above mark, with the colors black, yellow, and red claimed as features of the mark. The examining attorney refused registration on grounds that the mark is not inherently distinctive, and further, that a color mark consisting of multiple colors can *never* be inherently distinctive.

Among the issues on appeal to the Board was whether this was an application for a “color mark” or for a “symbol” comprised of a “distinctive design” that incorporates colors. The Board held that it constituted a “color mark”, noting in particular that the description of the mark stating that the dotted lines surrounding the color “merely depict placement of the mark on the packaging” and are not part of the shape of the mark.

The Board held that “a color mark consisting of multiple colors” is still a color mark and therefore “is not capable of being inherently distinctive.” A multiple color mark is eligible for registration on the Principal Register only upon showing proof of acquired distinctiveness. (The applicant did not request registration under Section 2(f).)

E. Faulty Specimens

There were two precedential decisions reversing refusals to register based on faulty specimens. In both cases, the Applicant’s clarification regarding consumer interaction with the marks was critical.

1. *In re Pitney Bowes, Inc.*, 125 U.S.P.Q.2d 1417 (TTAB Jan. 10, 2018), Board reversed examining attorney’s refusal to accept specimen of a website printout advertising applicant’s mailing and shipping services. The examining attorney argued that the specimens showed use of the mark with a software product, but not with the Class 39 services applied for. Although the Board agreed that the specimen was unclear, it held that the applicant’s explanation of the specimen and how it provides services resolved the ambiguity.

2. ***In re Minerva Associates, Inc.***, 125 U.S.P.Q.2d 1634 (TTAB Feb. 12, 2018), Board reversed examining attorney’s refusal to accept specimens of login and search screens showing Applicant’s downloadable software when in use, noting that an acceptable specimen for software (Class 9) can include “a photograph or printout of a display screen projecting the identifying trademark for a computer program.” The examiner was skeptical that the mark was visible to consumers, but the Applicant’s explanation of how consumers interfaced with the software convinced the Board otherwise.

F. Procedure & Evidence

1. **Internet Evidence:** Four precedential opinions this year related to Internet evidence.
 - a) **Internet printouts must include a date and source/URL, and this rule applies equally to examining attorneys and parties.** *See In re Mueller Sports Medicine, Inc.*, 126 U.S.P.Q.2d 1584 (TTAB May 16, 2018); *In re Canine Caviar Pet Food, Inc.*, 126 U.S.P.Q.2d 1590 (TTAB May 17, 2018); *In re I-Coat Company, LLC*, 126 U.S.P.Q.2d 1730 (TTAB June 7, 2018).
 - b) **Evidence of a cached website that is no longer active is not probative.** *In re Canine Caviar Pet Food, Inc.*, 126 U.S.P.Q.2d 1590 (TTAB May 17, 2018).
 - c) **Because Internet evidence is hearsay, it is admissible only for what it shows on its face, not for the proof of the matter asserted. Assertions appearing in printouts are not admissible without accompanying and corroborating testimony.** *WeaponX Performance Products Ltd. v. Weapon X Motorsports, Inc.*, 126 U.S.P.Q.2d 1034 (TTAB Mar. 14, 2018).
2. **Motions:** Be reasonable, cooperate, and don’t bother moving unless there is substantial prejudice that cannot be remedied through other means.
 - a) ***KID-Systeme GmbH v. Turk Hava Yollari Teknik Anonim Sirket***, 125 U.S.P.Q.2d 1415 (TTAB Jan. 12, 2018), granting motion to reopen time for filing summary judgment to accommodate recent rule changes.
 - b) ***Monster Energy Company v. Martin***, 125 U.S.P.Q.2d 1774 (TTAB Feb. 26, 2018), denying motion to strike timely filed expert disclosure which was inadvertently filed under different proceeding number, but properly served providing notice to respondent.
 - c) ***Kate Space LLC v. Thatch, LLC***, 126 U.S.P.Q.2d 1098 (TTAB Mar. 22, 2018), denying motion to strike pretrial disclosures and to exclude testimony declarations because (1) disclosure of authenticating

witness in pretrial disclosures was timely, and (2) the disclosure of two new testimony witnesses in pre-trial disclosures was justified and harmless given that both would testify recording documents and discovery already taken regarding third-party use.

d) *One Jeanswear Group Inc. v. YogaGlo, Inc.*, 127 U.S.P.Q.2d 1787 (TTAB Sept. 7, 2018), granting motion to compel discovery responses and rejecting objection to interrogatories on grounds that the subparts exceeded the limit of 75.

e) *Trans-High Corp. v. JFC Tobacco Corp.*, 127 U.S.P.Q.2d 1175 (TTAB July 2, 2018), granting unconsented motion to extend discovery after opposer objected to timeliness of discovery and did not provide a definitive response to applicant's request for consent to extend discovery. Notably, this was the opposer's first request to extend time, and it followed after hurricanes devastated Puerto Rico, where opposer is located.

3. Intersection with Federal Court

a) *In re FCA US LLC*, 126 U.S.P.Q.2d 1214 (TTAB Apr. 10, 2018), affirming Section 2(d) refusal to register and declining to give estoppel effect to court ruling in a trademark infringement and unfair competition dispute between the same parties. Because the Board noted that the marks and goods at issue in the court case were different, it declined to extend *B&B Hardware* to require the Board be bound by district court litigation to which the USPTO is not a party. The decision is on appeal to the Federal Circuit, No. 18-2069.

b) *Piano Wellness, LLC v. Williams*, 126 U.S.P.Q.2d 1739 (TTAB May 31, 2018), Board held that a U.S. district court exceeded its authority to rectify the register under Section 37 (which is limited to registrations) by directing "the Commissioner of Trademarks to transfer" a pending application. The Board outlined three alternatives to effect the desired outcome: (1) the district court may order that the parties take steps to effectuate a transfer of the application, (2) the parties may move the Board to amend ownership of the application, or (3) the parties may move the Board to sustain the opposition, which would cause the application to become abandoned (consistent with the court's permanent injunction).

SECTION 3

Developments in Trademark Litigation



Presented by

David H. Bernstein
Debevoise & Plimpton LLP
New York, NY

Thirty-Sixth Annual National CLE Conference

Trademark Litigation Year in Review

David H. Bernstein¹
Debevoise & Plimpton LLP
New York, New York

January 2, 2019
Snowmass, Colorado

¹ David H. Bernstein is chair of the Intellectual Property Litigation Group at Debevoise & Plimpton LLP in New York, and an adjunct professor of law at New York University Law School and George Washington University Law School, where he teaches Advanced Trademark Law. He received an A.B. *magna cum laude* from Princeton University's Woodrow Wilson School of Public and International Affairs in 1985, an M.Sc. from the London School of Economics and Political Science in 1986, and his J.D. from Yale Law School in 1989. Mr. Bernstein has served as Counsel and Director of INTA, and has chaired its International Amicus, Emerging Issues, and Programs Committees, and has co-chaired its Annual Meeting.

Kate Saba, Josh Shirley, and Matt Mutino, associates with Debevoise & Plimpton LLP, assisted with the preparation of this outline, which is current as of November, 2019.

This paper highlights noteworthy trademark decisions during the past year.

I. LICENSING

In *In re Tempnology, LLC*, 879 F.3d 389 (1st Cir. 2018), the First Circuit held that a debtor-licensor in bankruptcy may reject a trademark license agreement, and that the effect of that rejection is to permanently terminate the licensee’s right to use the licensed trademark. The Supreme Court has granted certiorari (*Mission Prod. Holdings, Inc. v. Tempnology, LLC*, No. 17-1657, 2018 WL 2939184 (U.S. Oct. 26, 2018)) to resolve a circuit split on this issue.

Tempnology, the debtor-licensor, made athletic products (*e.g.*, towels, socks, headbands, and other accessories) designed to remain at low temperatures even when used during exercise, and marketed them under the “Coolcore” and “Dr. Cool” brands. In 2012, Tempnology entered into a marketing and distribution agreement with Mission Products Holdings (“Mission”). As part of that deal, Tempnology granted Mission a limited license to use Tempnology’s trademarks and logo.² Several years later, Tempnology filed for bankruptcy.

Under § 365(a) of the Bankruptcy Code,³ a bankruptcy debtor may secure court approval to “reject” any executory contract of the debtor, meaning that the other party to the contract is left with a damages claim for breach, but not the ability to compel further performance. Citing § 365(a), Tempnology moved to reject its agreement with Mission, alleging that the agreement “suffocated [its] ability to market and distribute its products” and “essentially starv[ed]” Tempnology of income. Mission objected, arguing that, post-rejection, it was allowed to maintain its trademark rights under the license. The Bankruptcy Court found in Tempnology’s favor,⁴ but the Bankruptcy Appellate Panel of the First Circuit reversed.⁵

The First Circuit began by explaining the circuit split on this issue. In 1985, the Fourth Circuit’s *Lubrizol* decision held that a debtor may indeed reject an intellectual property license, and that the effect of such rejection was a termination of the license.⁶ Three years later, Congress responded by adding what is now § 365(n) of the Bankruptcy

² The agreement also concerned patent and distribution rights; the First Circuit’s discussion of those issues is not summarized here.

³ 11 U.S.C. § 365(a).

⁴ *In re Tempnology, LLC*, 541 B.R. 1, 7 (Bankr. D.N.H. 2015).

⁵ *In re Tempnology LLC*, 559 B.R. 809, 822 (B.A.P. 1st Cir. 2016).

⁶ *Lubrizol Enters., Inc. v. Richmond Metal Finishers, Inc.*, 756 F.2d 1043 (4th Cir. 1985).

Code. Section 365(n) provides an exception to the broad rejection power of § 365(a): when the rejected contract is one “under which the debtor is a licensor of a right to intellectual property,” the licensee may elect to “retain its rights . . . to such intellectual property,” thereby continuing the debtor’s duty to license the intellectual property. Yet, the Code’s definition of “intellectual property” (§ 101(35A)) conspicuously does not include trademark rights. In 2012, the Seventh Circuit’s *Sunbeam* decision expressly declined to follow *Lubrizol*, thus creating a circuit split.⁷ The Seventh Circuit held that rejection is better seen as a *breach* of the agreement, rather than a *termination*. Rejection relieves the debtor-licensor of its obligations under the agreement, but it does not terminate either the licensee’s right to continue using the licensed mark or its obligation to continue to comply with the license. Lower courts are also split on this issue.⁸

In a 2–1 decision, the First Circuit endorsed the *Lubrizol* rule, holding that Tempnology’s rejection of the license terminated Mission’s right to use the trademarks.⁹ The court found that the *Sunbeam* rule would subject debtor-licensors to a “residual enforcement burden.” In most trademark licenses, the licensor is obliged to monitor and exercise control over the quality of the goods sold under the trademark. Failure to do so results in a “naked license,” which can result in abandonment of the mark. Hence, if the license is not terminated, the debtor-licensor is forced to either continue its quality-control obligations, or potentially lose its trademark rights. The court found that this choice is at odds with the § 365(a) rejection power, and the bankruptcy concept of a “fresh start” for the debtor.

⁷ *Sunbeam Prod., Inc. v. Chicago Am. Mfg., LLC*, 686 F.3d 372, 378 (7th Cir. 2012). This holding was in accord with a Third Circuit concurrence: *In re Exide Techs.*, 607 F.3d 957, 964–68 (3d Cir. 2010) (Ambro, J., concurring).

⁸ Following the *Lubrizol* rule: *In re HQ Global Holdings, Inc.*, 290 B.R. 507, 512–13 (Bankr. D. Del. 2003); *In re Blackstone Potato Chip Co.*, 109 B.R. 557, 560–61 (Bankr. D.R.I. 1990); *In re Centura Software Corp.*, 281 B.R. 660, 673 (Bankr. N.D. Cal. 2002).

Following *Sunbeam*: *Banning Lewis Ranch Co. v. City of Colo. Springs (In re Banning Lewis Ranch Co.)*, 532 B.R. 335, 345 (Bankr. D. Co. 2015); *In re Crumbs Bake Shop, Inc.*, 522 B.R. 766, 770 (Bankr. D.N.J. 2014); *In re Sima Int’l, Inc.*, Case No. 17-21761, 2018 WL 2293705, at *8 (Bankr. D. Conn. May 17, 2018).

⁹ Judge Torruella dissented in part, stating that he would follow the Seventh Circuit’s *Sunbeam* decision on this issue. *In re Tempnology, LLC*, 879 F.3d 389, 405 (1st Cir. 2018).

As noted above, the Supreme Court has granted certiorari to resolve this circuit split. INTA submitted an *amicus* brief advocating that the Court reverse the First Circuit and adopt the *Sunbeam* approach.¹⁰

II. COMMON LAW RIGHTS

In *Commodores Entertainment Corp. v. McClary*, 879 F.3d 1114 (11th Cir. 2018), *cert. denied*, No. 18-47, 2018 WL 3349494 (U.S. Oct. 1, 2018), the Eleventh Circuit affirmed the district court’s grant of judgment as a matter of law to plaintiff, owner of several trademarks relating to the name and logo of the notable music group The Commodores, against defendant, a former member of the band who sought to continue to perform under that name.

“This is how the story goes”: In the 1970s William King, Ronald LaPread, Thomas McClary, Walter Orange, Lionel Richie and Milan Williams formed The Commodores, a band that signed with Motown Records and was known for its funk/soul musical style. In 1978, the original members of The Commodores, along with their manager formed a general partnership; the General Partnership Agreement addressed the use of “The Commodores” name, and provided that, “[u]pon the death or withdrawal of less than a majority of the Partners, the remaining majority of the Partners shall continue to have the right to use the name THE COMMODORES for any purpose.” The partners also incorporated Commodores Entertainment Corporation (“CEC”), and later amended the partnership agreement to give CEC “all rights in and to,” *inter alia*, “The Commodores” name and any associated marks. CEC then entered into a series of agreements with Motown Record Corporation that specifically provided that, upon withdrawal from the band, individual members did not have the right to use “The Commodores” name.

Over time, most of original Commodores departed—including Lionel Ritchie in 1982 and Thomas McClary (the defendant) in 1984—leaving King and Orange the only remaining original members. King and Orange transferred their common-law trademark rights to CEC, which in turn registered four marks with the USPTO for the word mark “THE COMMODORES” and the word mark “COMMODORES” with a design.

After leaving the group, the defendant, McClary, continued to perform under variations of “The Commodores,” including “The 2014 Commodores,” and “The Commodores Featuring Thomas McClary” (the “Infringing Uses”). CEC sued, claiming

¹⁰ Amicus Curiae Brief of the International Trademark Association in Support of Petitioner, *Mission Prod. Holdings, Inc. v. Tempnology, LLC*, No. 17-1657 (U.S. Oct. 26, 2018), <https://www.inta.org/Advocacy/Documents/2018/17%201657%20Mission%20Product%20Holdings%20Inc%20v%20Tempnology%20LLC.pdf>.

inter alia, trademark infringement. In 2014, the district court granted CEC a preliminary injunction barring McClary from using The Commodores marks “in a manner other than fair use.” 2014 WL 5285980 (M.D. Fla. Oct. 15, 2014). The Eleventh Circuit affirmed. 648 Fed. Appx. 771 (11th Cir. 2016). In 2018, after a two-week trial, the district court granted CEC’s motion for judgment as a matter of law, ruling that CEC owns rights to the marks at issue and that McClary does not. The court thereafter converted the preliminary injunction into a permanent injunction.¹¹

On an interlocutory appeal of the JMOL, the Eleventh Circuit framed the “essential question” as: “What happens to the ownership of a trademark in the name of a performing group when the group’s membership has evolved with time?”

Common-law trademark rights, the court began, are acquired through priority of appropriation, which entails adoption of a mark and use in a manner sufficiently public that “an appropriate segment of the public mind” identifies the goods or services “as those of the adopter of the mark.” Here, the band members, acting as a group, appropriated the “The Commodores” name. Consequently, common-law rights remained in, and could not be divided from, the group, which continued to control what the band did in connection with the marks by deciding, *e.g.*, where and when the group would perform, what songs the group would sing, and what costumes the group would wear. Therefore, when McClary left the band, he left behind his common-law rights to “The Commodores” trademarks.

The Court rejected McClary’s argument that his continued collection of royalties was evidence that he possessed rights in the marks; if anything, collection of royalties only for songs from when McClary was in the band showed that he lacked continuing trademark rights after leaving the band. Moreover, CEC’s various contractual agreements contemplating joint, but not several, ownership supported the holding that the group retained all rights to the marks.

The court’s holding suggests that original band members who stay with the band hold the band’s trademark rights, to the exclusion of departing members, particularly in the presence of contracts providing joint ownership. However, the court left room for fair use of bands’ trademarks. The court noted that, although McClary could not use the group’s name to identify himself in United States commerce or abroad, he could make fair use of the band’s name in order to refer historically to his tenure as an original band

¹¹ The district court also denied McClary’s motion to dismiss for failure to join an indispensable party, Ronald LaPread, an original member of The Commodores. The Eleventh Circuit declined to exercise pendant jurisdiction to review this denial on that grounds that it was neither a final decision of a lower court nor an issue “inextricably intertwined” with the permanent injunction.

member. (“An individual can continue to be a Commodore – a member of the original group –without having the legal right to call himself ‘The Commodores.’”).

The court’s discussion of injunctive relief is discussed in Section XI, *infra*.

III. FRAUD ON THE PTO

In *OTR Wheel Engineering, Inc. v. West Worldwide Services, Inc.*, 897 F.3d 1008 (9th Cir. 2018), the Ninth Circuit affirmed a district court judgment finding that plaintiff, OTR Wheel Engineering, had not committed fraud on the United States Patent and Trademark Office. Nevertheless, the court also affirmed a separate district court judgment that the trademark was invalid.

Plaintiff, OTR, and defendant, West, both sell tires for industrial use. One of OTR’s tire models is called “the Outrigger.” OTR obtained a registered trademark on the Outrigger name and a registered trade dress in its tire tread design. West wanted to sell tires to one of OTR’s existing customers. To do so, West approached OTR’s Chinese manufacturer and requested a set of tires the same size as the Outrigger. When the manufacturer advised that it would take a long time to make a mold for West’s tires, West asked the manufacturer to just use OTR’s Outrigger molds and take out the nameplate, so that “nobody will know.” The manufacturer agreed and West successfully poached OTR’s customer.

OTR sued, bringing numerous Lanham Act and state law claims. A jury found West liable for reverse passing off and some of the state law claims, with actual damages in the amount of \$967,015. (The portions of this decision discussing reverse passing off are discussed in Section XIII, *infra*.) On the other hand, the jury also found that OTR had obtained its Outrigger trade dress registration through fraud on the PTO and, thus, that the registration should be cancelled. The district court set aside this finding as a matter of law, ruling that there was not substantial evidence to support the verdict.

The circuit court affirmed. A claim for cancellation based on fraud requires five elements: “1) a false representation regarding a material fact; 2) the registrant’s knowledge or belief that the representation is false; 3) the registrant’s intent to induce reliance upon the misrepresentation; 4) actual, reasonable reliance on the misrepresentation; and 5) damages proximately caused by that reliance.” The court held that these elements must be established by clear and convincing evidence and that West did not meet this burden. West presented two pieces of evidence of fraud. One was an email from a consultant suggesting that the Outrigger tread was functional; West alleged that OTR had fraudulently withheld this email from the PTO. The court held that this omission was immaterial, since OTR had elsewhere disclosed the functionality issue to its PTO examiner. The second piece of evidence was a declaration written by an OTR manager to the PTO claiming that OTR’s tread design “is immediately identifiable.” West alleged that this was a false statement of fact. The court held that even if this was

actually false, it was not material because West could not show that the PTO examiner had reasonably relied on this declaration in reaching its decision.

Despite this holding, however, the circuit court affirmed a separate judgment that OTR's trade dress was invalid. The trial court jury instructions had asked the jury to reach separate findings on trademark infringement (Question 1) and cancellation due to fraud on the PTO (Question 2). The above analysis, overturning the jury's findings on fraud, pertained only to the verdict on Question 2. Separately, with respect to Question 1, the jury found that OTR's trade dress was invalid. Here, unlike the fraud issue, the district court sustained the verdict. OTR moved for a new trial on this issue, arguing that the jury found the trade dress invalid based on its erroneous holding that the registration was fraudulently obtained. The district court denied that motion.

Once again, the circuit court affirmed. Cancellation and invalidity are separate inquiries. If a trademark registration is cancelled, for fraud or any other reason, the underlying unregistered trademark is not necessarily invalid. Indeed, a claim for infringement may still be pursued based on the unregistered mark. (In such cases, the burden simply shifts back to plaintiff to establish distinctiveness and non-functionality.) Because cancellation and invalidity are separate issues, any argument that the jury's finding on invalidity relied on its finding of fraud on the PTO, was pure speculation.

IV. TRADEMARK USE

In *Viacom Int'l v. IJR Capital Investments, L.L.C.*, **891 F.3d 178 (5th Cir. 2018)**, the Fifth Circuit affirmed the district court's grant of summary judgment to plaintiff, Viacom, holding that Viacom had a valid common law trademark in "The Krusty Krab," a fictional restaurant portrayed in the popular *SpongeBob SquarePants* animated television series.

Viacom is the parent of Nickelodeon, which has aired *SpongeBob SquarePants* since 1999. The series has been the most-watched animated television series in the U.S. for 15 consecutive years, and has spawned two successful feature films, a Broadway musical, a mobile app, and a wide array of licensed merchandise. The Krusty Krab, the fast food restaurant that employs SpongeBob, is featured as a setting in most episodes of the show and is an element in many of the works and merchandise derived from the show's universe. However, Viacom had never registered The Krusty Krab as a trademark.

Defendant IJR sought to open actual seafood restaurants named The Krusty Krab. Before IJR opened any restaurants, Viacom sued and the district court granted summary judgment on trademark infringement and unfair competition.¹²

The Fifth Circuit began by holding that, as a threshold matter, “specific elements from within a television show—as opposed to the title of the show itself” were eligible to receive trademark protection, noting that “other courts have unequivocally extended this protection to fictional elements of entertainment franchises.”

Next, the court considered whether Viacom had used The Krusty Krab “as a source indicator,” a prerequisite for trademark protection. The fact that the restaurant was an element in a successful television series was not enough. Rather, “the salient question” is whether the mark, “as used, will be recognized in itself as an indication of origin for the particular product or service” and “creates a separate and distinct commercial impression.” Hence, “the focus is on the role that the element plays within the show and not the overall success or recognition of the show itself . . . [w]hen an element only occasionally appears in a successful television series, the indication-of-origin requirement may not be met.”

The court held that The Krusty Krab satisfied this analysis: the “appears in over 80% of episodes,” “plays a prominent role” in other *SpongeBob* works (*e.g.*, the films and video games), and is consistently used on licensed merchandise. It did not matter that the “The Krusty Krab” typically appears alongside the primary “SpongeBob SquarePants” trademark, because the name creates its own “distinct commercial impression signifying to consumers that products like Krusty Krab playsets or aquarium ornaments originate from the famous fictional restaurant that employs their beloved sea sponge character.” Additionally, the fact that Viacom had used the mark in “varying styles, fonts, and sizes on the licensed products” did not undermine Viacom’s showing of trademark use, as long as the mark was consistently used as an indicator of source.

Having established that Viacom had, indeed, used The Krusty Krab as a source-indicator, the court moved on to the issues of whether the mark had acquired distinctiveness through secondary meaning and whether IJR’s use of the mark created a likelihood of confusion. Those issues are discussed in Sections V and VI, *infra*, respectively.

V. DISTINCTIVENESS & SECONDARY MEANING

In *Royal Crown Co., Inc. v. Coca-Cola Co.*, 892 F.3d 1358, 1362 (Fed. Cir. 2018), the Federal Circuit considered whether the term ZERO, incorporated in numerous

¹² *Viacom Int’l Inc. v. IJR Capital Investments, LLC*, 242 F. Supp. 3d 563 (S.D. Tex. 2017).

trademarks registered by The Coca-Cola Company (*e.g.*, Coke Zero), was generic for soft drinks or energy drinks that contain no calories. The court vacated a Trademark Trial and Appeal Board decision which had ruled that the mark was *not* generic, and remanded for further consideration on that issue and on whether the mark had acquired secondary meaning.¹³

The applicant in this matter was The Coca-Cola Company (“Coca-Cola”), which had, between 2003 and 2008, filed seventeen applications for marks incorporating the term ZERO, including COKE ZERO, SPRITE ZERO, and FANTA ZERO. The opposers, Royal Crown Company (“RC”) and Dr. Pepper/Seven Up, Inc., asserted that ZERO is either generic for zero-calorie soft drinks or descriptive without acquired distinctiveness and thus cannot be registered without a disclaimer of Coca-Cola’s exclusive right in that term. Additionally, Coca-Cola opposed registration by RC of two marks incorporating ZERO on the grounds they were likely to cause confusion with Coca-Cola’s own marks. TTAB concluded that that the term ZERO was descriptive, not generic, and that Coca-Cola had met its burden to establish that acquired distinctiveness in ZERO when used as part of a mark for soft drinks (*e.g.*, Coke Zero) and sports drinks (*e.g.*, Powerade Zero), although not for energy drinks.

On appeal, the Federal Circuit explained that determination of a term’s genericness involves a two-step inquiry: (i) “what is the genus of goods or services at issue?”, and (ii) “is the term . . . understood by the relevant public primarily to refer to that genus of goods or services?” Additionally, “a term can be generic for a genus of goods or services if the relevant public understands the term to refer to a *key aspect* of that genus.” Hence, in this case, if RC could show that the public understands ZERO, used in combination with a designated beverage name, to mean a sub-group or type of soft drinks that carries “specific characteristics,” that would be sufficient to render the term generic. In other words, TTAB must consider whether ZERO “refers to a key aspect of at least a sub-group or type of the claimed beverage goods,” and must consider that “zero calorie beverages” is clearly such a “sub-group.” Finding that TTAB had not engaged in this analysis, the court vacated and remanded.

The court also took issue with TTAB’s review of the evidentiary record on genericness. First, TTAB wrongly suggested that RC was required to provide *direct* evidence of consumer perception to support its genericness challenge, “whether from a survey, dictionary, or otherwise.” Rather, evidence of the public’s perception may be obtained from “any competent source,” including, in this case, RC’s “evidence of competitive use, evidence that other companies use ZERO in combination with their own soft drink marks, third-party registrations and applications for such combined marks, and evidence of third-party and TCCC descriptive uses of ‘zero’ and ‘0’ on various packaging

¹³ *Royal Crown Co. v. Coca-Cola Co.*, Opposition No. 91178927 (Parent), 2016 WL 9227936 (T.T.A.B. May 23, 2016).

and marketing materials.” Second, TTAB incorrectly found that Coca-Cola’s “billions of dollars in sales” of ZERO products, and its associated advertising expenditures, were relevant to the genericness inquiry. The court held that while sales and advertising figures “may be probative of acquired distinctiveness” of a *non-generic term*, such evidence does not demonstrate that a term is not generic.

Apart from genericness, the court also vacated TTAB’s conclusion that ZERO had acquired distinctiveness through secondary meaning. First, TTAB failed to adequately consider a “sliding-scale” approach to proof of secondary meaning, wherein “a more descriptive term requires more evidence of secondary meaning.” The court instructed TTAB, on remand, to “make an express finding regarding the degree of the mark’s descriptiveness on the scale ranging from generic to merely descriptive.” Having done so, TTAB must consider whether the term ZERO, when used in connection with beverages, is “so highly descriptive” that TTAB’s assessment of Coca-Cola’s evidence of acquired distinctiveness must be “exacting.”

The court also criticized Coca-Cola’s secondary meaning survey. First, the survey was conducted more than five years before the close of testimony before the board. Because secondary meaning only “exists at a specific time, in a specific place, among a specific group of people,” and because RC presented evidence of substantial and increased use of ZERO by third parties in the intervening years, the court concluded that the survey was unlikely to be probative of the term’s acquired distinctiveness.

Additionally, the court found the survey’s questions problematic. Respondents were asked whether they “associated” the term ZERO with the products of one or more companies. Yet, the court held, mere *association* does not imply that a consumer “would be confused by seeing a ZERO-branded product under a different label, nor does it address what meaning consumers attach to the term ZERO.” Finally, the court noted that because Coca-Cola had not established that its various ZERO marks were a “family of marks,” the survey was not probative as to those particular marks that consumers failed to mention in the survey.

In *In re Serial Podcast, LLC*, 126 U.S.P.Q.2d 1061 (T.T.A.B. 2018), the TTAB affirmed a refusal to register the word mark SERIAL for “entertainment in the nature of an ongoing audio program featuring investigative reporting, interviews, and documentary storytelling.” However, the TTAB set aside refusals to register two word and design marks depicting SERIAL, finding that the marks had achieved secondary meaning.

An assessment of genericness starts with two questions: (i) “What is the genus of goods or services at issue?” and (ii) “Is the term sought to be registered understood by the relevant public primarily to refer to that genus of goods or services?” Here, the examining attorney and applicant agreed that the genus is provided by the relevant subject application: “entertainment in the nature of an ongoing audio program featuring

investigative reporting, interviews, and documentary storytelling.” The relevant public is “ordinary listeners of audio programs.”

The record contained numerous dictionary definitions of “serial” as either a generic noun (“a story or play appearing in regular installments”) or an adjective (“appearing in successive parts or numbers”). The TTAB noted that the genus “audio program” included not just podcasts, but also radio shows, and that “the serial has long been a staple of the radio waves.” The applicant contended that use of “serial” as a generic *noun*, as in “radio serial,” was antiquated and unrelated to contemporary public understanding. The TTAB was unconvinced, noting, first, ample examples of contemporary use of “serial” as a noun and, second, that “adjectives” can be generic in a trademark sense. The applicant countered that many such contemporary uses dating after the debut of the podcast use “serial” as a reference to the podcast itself, not a generic concept. The TTAB noted, however, that a “mix of generic and non-generic uses” does not preclude a finding of genericness; at best, it amounts to “de facto secondary meaning” in a generic term. And, the fact that a generic term has a secondary meaning to many people is not sufficient to show that the term may be registered as a trademark.

In *dicta*, after reaching its finding of genericness, the TTAB still addressed the issue of whether the applicant had shown secondary meaning. Given that the term “serial” is, at best, “highly descriptive,” an applicant faces a high bar to establish secondary. Hence, despite the applicant’s showing of 12,000 media stories about the podcast, a “spike” in Google searches of “podcast serial” following the program’s debut, and the fact that the podcast had been downloaded 172 million times in the U.S., the TTAB did not find secondary meaning. All of this evidence showed commercial success of the mark, not consumer recognition.

On the other hand, the TTAB found that the applicant’s logo marks did achieve secondary meaning. The logos, consisting of narrow white letters on a background of a series of black rectangles, are minimally stylized, but that is sufficient to make them descriptive, not generic. Moreover, there was ample evidence of the logos’ appearance throughout media and pop culture in clearly source-indicative contexts, including use in SNL and Sesame Street parody sketches, unauthorized merchandise t-shirts, and, according to a newspaper article, on the bulletin boards of schools around the country that adopted the podcast for lesson plans.

In *Converse, Inc. v. Int’l Trade Comm’n*, --- F.3d ----, No. 2016-2497, 2018 WL 5536405 (Fed. Cir. Oct. 30, 2018), the Federal Circuit reversed a determination of the U.S. International Trade Commission, which had found that certain of Converse’s trademarks in design elements of the Chuck Taylor All-Star sneaker were invalid for lack of secondary meaning.

Converse had been marketing sneakers with these design elements since the early twentieth century, and, in 2013, it registered them in a trade dress mark. Shortly

thereafter, Converse filed a complaint with the ITC under Section 337 of the Tariff Act (19 U.S.C. § 1337), which provides a remedy for, among other things, “the importation into the United States . . . or the sale within the United States after importation . . . of articles that infringe a valid and enforceable United States trademark registered under the Trademark Act of 1946.” The complaint alleged that a large number of defendants¹⁴ (including Wal-Mart and Skechers) had violated § 337 by importing shoes that infringed Converse’s trademarks. After an investigation, the ITC issued a final determination finding that Converse’s registered trade dress mark was invalid because Converse had not established secondary meaning.¹⁵

The Federal Circuit began its analysis by establishing the relevant date for assessing secondary meaning. Since product-design trade dress can never be inherently distinctive, it is protectable only upon a showing of secondary meaning. Additionally, to establish infringement, a plaintiff must establish that its trade dress had acquired secondary meaning *before* the first infringing use by each alleged infringer. The court held that, if a mark is infringed *after* it is registered, the markholder is entitled to a presumption that the mark is valid, which shifts the burdens of persuasion and production to the challenger. But, this presumption only operates *prospectively* from the date of registration.

This presented a problem for Converse: many of the defendants had first infringed Converse’s trade dress years before Converse registered the mark in 2013. The court held that “Converse’s registration confers a presumption of secondary meaning beginning only as of the date of registration and confers no presumption of secondary meaning before the date of registration.” Hence, for those defendants who first infringed prior to 2013, Converse would need to establish that its mark had acquired secondary meaning before the first infringing use of each such respondent without the benefit of any presumption.

Once the date was established, the court moved to clarify the standards for determining whether a mark has acquired distinctiveness through secondary meaning. The court introduced a new six-factor test for secondary meaning in the Federal Circuit: “(1) association of the trade dress with a particular source by actual purchasers (typically measured by customer surveys); (2) length, degree, and exclusivity of use; (3) amount and manner of advertising; (4) amount of sales and number of customers; (5) intentional copying; and (6) unsolicited media coverage of the product embodying the mark.”

¹⁴ Procedurally speaking, these competitors are “respondents,” not “defendants.” However, to avoid inevitable confusion when discussing survey evidence, this summary will use the latter term.

¹⁵ *In re Certain Footwear Products*, Inv. No. 337-TA-936 (USITC, July 6, 2016) (Commission Opinion).

The court also clarified the relevant timeframe for analyzing factor 2, the trademark owner's and third parties' prior uses of the mark. The court held that "[t]he critical issue for this factor is whether prior uses impacted the perceptions of the consuming public *as of the relevant date*." Therefore, the factfinder should not rely on prior uses that long predated the first potential infringement. Rather, "the ITC should rely principally on uses within the *last five years*" before the relevant date, and "uses older than five years should only be considered relevant if there is evidence that such uses were likely to have impacted consumers' perceptions of the mark as of the relevant date."

Regarding exclusivity of use (under factor 2), the court held that the factfinder should constrain its analysis to third-party uses of the mark that were *substantially similar* to the registered trademark. The ITC had cited several historical examples of third-party uses that bore "at most a passing resemblance" to Converse's actual mark, or that were missing at least one element of the mark. On remand, ITC must disregard such uses, and only consider those uses that were substantially similar to the actual mark.

Finally, the court discussed the defendants' survey evidence. The defendants' expert had surveyed consumers in 2015. The court noted that this would be relevant to determining secondary meaning at the date of *registration* (2013). However, the relevant date for most was the date of *their first use* of the mark, which, in most cases, predated the registration date by 5–10 years. Because secondary meaning needs to be assessed as of that historical date, a contemporary survey would almost definitely be useless.

In *Viacom Int'l v. IJR Capital Investments, L.L.C.*, **891 F.3d 178 (5th Cir. 2018)**, the Fifth Circuit affirmed the district court's grant of summary judgment to plaintiff, Viacom, holding that the common law trademark "The Krusty Krab," a fictional restaurant portrayed in the popular *SpongeBob SquarePants* animated television series, had acquired distinctiveness through secondary meaning.

The facts of this case are discussed in Sections IV and VI, *infra*. Viacom is the parent of Nickelodeon, which has aired *SpongeBob SquarePants* since 1999. The series has been the most-watched animated television series in the U.S. for 15 consecutive years, and has spawned two successful feature films, a Broadway musical, a mobile app, and a wide array of licensed merchandise. The Krusty Krab, the fast food restaurant that employs SpongeBob, is featured as a setting in most episodes of the show and is an element in many of the works and merchandise derived from the show's universe. However, Viacom had never registered "The Krusty Krab" as a trademark. Defendant IJR sought to open actual seafood restaurants named The Krusty Krab. Before IJR

opened any restaurants, Viacom sued and the district court granted summary judgment on trademark infringement and unfair competition.¹⁶

The Fifth Circuit considers seven factors in determining whether a mark has acquired secondary meaning: “(1) length and manner of use of the mark or trade dress, (2) volume of sales, (3) amount and manner of advertising, (4) nature of use of the mark or trade dress in newspapers and magazines, (5) consumer-survey evidence, (6) direct consumer testimony, and (7) the defendant's intent in copying the mark.”

The court found that the first two factors favor Viacom. Although The Krusty Krab was a fictional restaurant, Viacom had used the mark as a “central element of the SpongeBob universe” since 1999, and Viacom had earned millions of dollars in sales of merchandise that prominently featured the mark. On factor three, the “relevant question . . . is not the extent of the promotional efforts, but their effectiveness in altering the meaning of the mark to the consuming public.” Viacom had expended hundreds of millions of dollars on marketing its products and the two *SpongeBob* feature films. The court found that “[t]he effectiveness of this advertising is evident from the success of product sales and the films” and that [w]hile the effectiveness of ‘The Krusty Krab’ mark, specifically, has not been directly proven, its depiction in advertisements is such that the public would recognize the mark as more than an artistic backdrop.”

Because there was no consumer survey and no direct consumer testimony, factors five and six were inconclusive. Factor seven, IJR’s intent was, at best, inconclusive. Hence, the court held that, as a matter of law, the mark had acquired distinctiveness through secondary meaning.

VI. INFRINGEMENT & LIKELIHOOD OF CONFUSION

In *Variety Stores, Inc. v. Wal-Mart Stores, Inc.*, 888 F.3d 651 (4th Cir. 2018), the Fourth Circuit reversed a grant of summary judgment to plaintiff, Variety Stores, finding that the district court had erred in its likelihood of confusion analysis. This ruling also vacated the district court’s order that had directed defendant Walmart to disgorge \$32.5 million in profits.

Plaintiff Variety (and its predecessor) had continuously used the marks THE BACKYARD, BACKYARD, and BACKYARD BBQ on a wide variety of outdoor products, including grills and grill accessories, since the early 1990s. In 1994 Variety’s predecessor registered THE BACKYARD for use on “retail store services in the field of lawn and garden equipment and supplies.” In 2010, Walmart began researching and testing possible names for an in-house brand for grills and grill accessories, eventually

¹⁶ *Viacom Int’l Inc. v. IJR Capital Investments, LLC*, 242 F. Supp. 3d 563 (S.D. Tex. 2017).

settling on BACKYARD GRILL. Walmart had considered adopting the names “Backyard Barbeque” or “Backyard BBQ,” but Walmart’s legal team was aware of Variety’s registration and advised against those. Walmart filed an application for BACKYARD GRILL in 2011, after which Variety filed an opposition and brought this suit.

In December 2015, the district court granted Variety’s motion for partial summary judgment on claims for trademark infringement and unfair competition under federal law and trademark infringement and unfair and deceptive practices under state law. A bench trial on accounting and disgorgement was held in October 2016, after which the court ordered Walmart to disgorge its profits from the BACKYARD products in the amount of \$32,521,671.40. The district court emphasized that Walmart had willfully infringed, noting: “It is difficult to imagine more compelling evidence of intent to confuse than a knowing decision to use a similar mark to sell similar goods.”

On appeal, the circuit court did not directly address the district court’s decision on disgorgement, but reversed the district court’s summary judgment order on liability and vacated all the district court’s subsequent orders. At summary judgment, the district court had applied the Fourth Circuit’s nine-factor likelihood of confusion test and found that all factors except for actual confusion favored Variety. The circuit court disagreed on three factors: strength of plaintiff’s mark, similarity of the marks, and defendant’s intent.

On strength of the mark, the district court had found that Variety’s BACKYARD marks were suggestive, and thus conceptually strong. The circuit court did not resolve whether the marks were descriptive or suggestive, but found that, even if they were suggestive, they were conceptually weak due to extensive use of “Backyard” in third-party party marks (a trademark search yielded 527 marks with the word “backyard,” 23 of which included “grill” in the description of covered goods). Moreover, these third-party uses also created a genuine dispute as to commercial strength. On similarity, the circuit court found that reasonable minds may differ on the similarity between the marks BACKYARD BBQ and BACKYARD GRILL, noting that, in Walmart’s logo, the “Grill” portion of the mark is larger and more prominent than the word “Backyard.”

Finally, on intent, the district court had emphasized that Walmart had acted against the advice of its counsel in adopting the BACKYARD mark and that Walmart representatives had never visited a Variety store to observe how the marks were used, despite the fact that such visits were “a corporate practice at Walmart.” The circuit court found a genuine dispute here as well. Walmart knew about Variety’s registration of THE BACKYARD, but that registration only covered gardening supplies, and Walmart claimed it did not know that Variety used BACKYARD BBQ on grills. Further, Walmart arguably showed good faith by not adopting similar marks it had considered, like BACKYARD BARBEQUE. Finally, while Walmart had not investigated Variety’s

stores, this omission was possibly because Variety was not viewed as a major competitor (like Home Depot or Lowe's).

In *Allstate Insurance Co. v. Kia Motors America, Inc.*, Case No. CV 16-6108 SJO (AGR_x), 2017 WL 6550669 (C.D. Cal. Dec. 22, 2017), appeal docketed, No. 18-55164 (9th Cir. 2018), a California district court found in favor of defendant Kia, ruling that its "Drive Wise" line of high-tech vehicle add-ons did not infringe Allstate's "Drivewise," an insurance rewards program. The court reached this finding despite an advisory jury verdict in favor of Allstate on the issue of likelihood of confusion.

In 2010, Allstate released a "safe driving program" under the DRIVEWISE mark. The program uses telematics technology to monitor users' driving behavior, measuring attributes such as mileage, braking, speed, and time of day when a customer is driving. Customers access the program either by using a small device that connects to a car's computer or through a mobile phone app. Using the program, drivers can earn reward points or discounts from Allstate "for safe driving behavior." In 2015, Kia announced DRIVE WISE, a "sub-brand dedicated to autonomous driving and assistive technologies." Under that brand, Kia marketed several add-on features for its cars like "blind spot detection" and "smart cruise control." Each feature involves a system of sensors and cameras placed around the vehicle to detect and analyze road conditions

Allstate brought suit alleging, *inter alia*, infringement of its DRIVEWISE mark. The court empanelled an advisory jury, which reached a verdict in favor of Allstate on the issue of likelihood of confusion. A bench trial continued on the issue of whether to issue a permanent injunction. The court then issued findings of fact and conclusions of law, finding, despite the jury verdict, that Allstate had not established a likelihood of confusion and thus denying the request for an injunction. In determining the likelihood of confusion, the court applied the Ninth Circuit's 8-factor *Sleekcraft* test.

On the strength of the mark, the Court deemed Allstate's "Drivewise" mark to be both conceptually and commercially weak. Conceptually, the parties stipulated that "Drivewise" is suggestive, which is "inherently weak." Regarding commercial strength, Allstate argued that it had spent \$400 million developing and operating its Drivewise program and \$47 million on advertising. Despite these expenditures, Allstate "offered no expert testimony and conducted no consumer research or survey regarding the strength of [its] mark," and the court held that advertising expense is "an imperfect proxy measurement for whether the mark is remembered and associated in the public mind with the mark's owner" and is "not sufficient to render a suggestive mark strong." Moreover, while Allstate claimed "1.1 million active participants" in the program, it did not explain what "participation" entails, meaning that the real number of regular users could be significantly smaller than that.

Similarity of the marks weighed in favor of confusion; the court found the word marks "nearly identical" in meaning, pronunciation, and appearance. However, the

impact of this finding was mitigated by the conclusion that the products at issue were not closely related. Allstate's Drivewise program is mostly a service; Kia's Drive Wise is a tangible good. Drivewise is free of cost; Drive Wise costs several thousand dollars and requires purchase of a Kia vehicle. Drivewise is a *passive* insurance monitoring device; Drive Wise is an *active* sensor system that exerts control over the vehicle. Additionally, Allstate offered "no expert testimony or survey evidence demonstrating that the consuming public is likely to associate" its mark with Kia's mark. While both products "rely on software" and "relate to drive safety," these characteristics are too broad to establish relatedness.

Defendant's intent and evidence of actual confusion also both weighed against a likelihood of confusion. While Kia did not dispute it was fully aware of Allstate's registration at the time it adopted the Drive Wise name, the name was "independently derived" and adopted under the reasonable belief that, given the products' lack of relation, there would be no consumer confusion. Regarding evidence of confusion, the court noted that Allstate failed to provide any evidence of actual confusion or a likelihood of confusion, "despite having both the means and ability to do so," and thus concluded that "no such confusion can currently be demonstrated."

The remaining factors likewise favored Kia. The court found limited overlap between marketing channels, and no concrete plans for the future expansions resulting in direct competition. Finally, because an automobile is "ordinarily one of the largest purchases made by individual consumers," customers purchasing Kia's products were likely to exercise significant care.

With only one factor weighing in favor of finding a likelihood of confusion, the Court found Allstate failed to meet its burden to show Kia's use of Drive Wise to be likely to cause confusion as to source, sponsorship, affiliation, or approval of Allstate's goods. Accordingly the court denied Allstate's request for a preliminary injunction. An appeal has been filed.

In *Viacom Int'l v. IJR Capital Investments, L.L.C.*, **891 F.3d 178 (5th Cir. 2018)**, the Fifth Circuit affirmed the district court's grant of summary judgment to plaintiff, Viacom, holding that defendant's use of "The Krusty Krab" as a name for seafood restaurants would infringe on Viacom's common law trademark for The Krusty Krab, a fictional restaurant portrayed in the popular *SpongeBob SquarePants* animated television series.

The facts of this case are discussed in Sections IV and V, *supra*. Viacom is the parent of Nickelodeon, which has aired *SpongeBob SquarePants* since 1999. The series has been the most-watched animated television series in the U.S. for 15 consecutive years, and has spawned two successful feature films, a Broadway musical, a mobile app, and a wide array of licensed merchandise. The Krusty Krab, the fast food restaurant that employs SpongeBob, is featured as a setting in most episodes of the show and is an

element in many of the works and merchandise derived from the show's universe. However, Viacom had never registered "The Krusty Krab" as a trademark.

Defendant IJR sought to open actual seafood restaurants named "The Krusty Krab." IJR's owner claimed that the name referred to "the crusted glaze applied to cooked seafood," that he did not consider SpongeBob when originating the name, and that he only became aware of the fictional Krusty Krab when he performed a Google search on the name. IJR filed an intent-to-use trademark application for the name, which was approved by the PTO. IJR also developed a business plan for potential investors, purchased domain names for the restaurant concept, leased property in California, and procured restaurant equipment. Before IJR opened any restaurants, Viacom sued and the district court granted summary judgment on trademark infringement and unfair competition.¹⁷

The Fifth Circuit considers seven likelihood of confusion factors: "(1) the type of mark allegedly infringed; (2) the similarity between the two marks; (3) the similarity of the products or services; (4) the identity of retail outlets and purchasers; (5) the identity of the advertising media used; (6) the defendant's intent; and (7) any evidence of actual confusion." The court noted that "[c]ontext is critical" to this analysis, but acknowledged that because IJR had not yet actually opened a restaurant, the record was limited. Nevertheless, while the court would refrain from "divin[ing] the theme and details of the restaurant," this record did "contain sufficient context to conduct a likelihood-of-confusion analysis."

The first factor, "the type of mark," refers to the strength of Viacom's mark, and "[t]he more distinctive a mark, the stronger the mark." Because the court held that The Krusty Krab had acquired distinctiveness through secondary meaning, this factor favored Viacom. The second factor also favored Viacom, as the Viacom's and IJR's marks were verbatim duplicates of one another.

The third factor likewise supported Viacom. While Viacom had never actually licensed or operated any Krusty Krab seafood restaurants, the court cited Bubba Gump Shrimp Co., a fictional business in the film *Forrest Gump*, which, itself, had been licensed as an actual seafood restaurant. Hence, because "the danger of affiliation or sponsorship confusion increases when the junior user's services are in a market that is one into which the senior user would naturally expand," the factor tilted towards Viacom.

Factors four and five did not necessarily weigh in favor of confusion. Viacom retails through toy stores and online retailers; IJR retails through brick and mortar restaurants. Viacom predominately targets children as consumers, whereas IJR would

¹⁷ *Viacom Int'l Inc. v. IJR Capital Investments, LLC*, 242 F. Supp. 3d 563 (S.D. Tex. 2017).

presumably target adults capable of deciding to eat at a restaurant (although children may influence adults in that regard). And, while IJR had not actually begun to market its restaurants, such marketing would likely consist of local, specialized advertising, which does not necessarily overlap with Viacom's nationally-focused advertising.

Factor six, defendant's intent, also favored IJR. The relevant inquiry is "whether IJR intended to derive benefits from Viacom's reputation by using The Krusty Krab mark." The district court had found that that IJR acted in bad faith because IJR's owner was aware of Viacom's use of the mark before he submitted his trademark application. The circuit court, however, held that "mere awareness of the senior user's mark does not establish bad intent," and noted IJR's owner's testimony that he was initially unaware of the SpongeBob connection and that "the name was created to reference seafood with a crust on it." While a jury might not find this testimony credible, at summary judgment, it left a genuine issue of material fact.

Finally, actual confusion, the seventh factor, favored Viacom. The record contained various anecdotal examples of confusion. Additionally, Viacom presented an *Eveready* consumer survey finding that 30% of respondents indicated that a restaurant named The Krusty Krab was "operated by, affiliated or connected with, or approved or sponsored by Viacom" and that 35% of respondents "associated" such a restaurant with Viacom. The court held that this survey was methodologically flawed: it asked if "THE KRUSTY KRAB restaurant is affiliated or connected with any other company or organization," a question which resembles "a mere word-association test." Nevertheless, this flaw did not rise to the level of a "substantial defect," and, thus, while the survey was given little weight, the district court did not abuse its discretion in admitting it as evidence. Because actual confusion is a "low bar," the survey and the anecdotal evidence were sufficient to favor Viacom.

Weighing the factors together, the court found no genuine issue of material fact as to likelihood of confusion, and affirmed the district court's grant of summary judgment to Viacom.

VII. FAIR USE

In *Sazerac Brands, LLC v. Peristyle, LLC*, 892 F.3d 853 (6th Cir. 2018), the Sixth Circuit affirmed a district court's grant of summary judgment to defendant, Peristyle, holding that Peristyle's use of "Old Taylor" to describe its historic distillery was descriptive fair use. In *dicta*, the court also signaled a willingness to revisit the Sixth Circuit's "trademark use" threshold for infringement, observing that the test may be at odds with the text of the Lanham Act.

The Old Taylor Distillery was built by Colonel Edmund Haynes Taylor, Jr. in 1887, and was once known as "the most magnificent plant of its kind in Kentucky." The distillery eventually fell into financial ruin and was closed in 1972. In 2014, Peristyle,

purchased and renovated the distillery. As of now, Peristyle operates under the name Castle & Key, but during the renovation, it referred to its location as “the Former Old Taylor Distillery” or simply “Old Taylor.” At the same time, plaintiff, Sazerac, owned the trademark rights to “Old Taylor” and “Colonel E.H. Taylor” and produced bourbon under both names. Sazerac brought suit for, *inter alia*, trademark infringement. The district court granted Peristyle summary judgment, finding that Sazerac had not met its burden under the Sixth Circuit’s threshold “trademark use” test.¹⁸

The Sixth Circuit affirmed the district court’s judgment, but on different grounds. Rather than applying the circuit’s “trademark use” test, the court focused on descriptive fair use. Descriptive fair use has two elements: the defendant must (i) “use the label in a descriptive or geographic sense” and (ii) “do so fairly and in good faith.” On the first element, the court held that Peristyle did use the Old Taylor name in a descriptive and geographic manner. While Peristyle had not yet begun selling its bourbon, when it does, the bourbon will be called “Castle & Key,” and “Old Taylor” will not appear on the bottle. Hence, Peristyle “referred to Old Taylor to pinpoint the historic location where Peristyle planned to make a new bourbon, not to brand that bourbon.” For example, the company distributed flyers, posters, and social media posts that referred to “The Historic Site of The Old Taylor Distillery” or “VIP Mailing List for the Former Old Taylor Distillery.” Rather than “trade off the goodwill of Sazerac,” Peristyle was “enjoying the goodwill already ingrained in the property it purchased.” “The contrast,” the court noted, “is as stark as comparing a bourbon to a scotch.”

On the second element of fair use, good faith, the court again found in favor of Peristyle. While Peristyle did not always preface “Old Taylor” with “former” or “historic,” context invariably indicated that the name referred to the physical distillery in a descriptive manner. While the distillery itself featured enormous “Old Taylor Distillery” signs, those signs existed prior to Peristyle’s purchase of the building, and Peristyle planned to introduce “Castle & Key” signs next to those. And, while Peristyle conducted commercial activities at the distillery (like hosting a wedding and renting barrel-aging warehouse space to third parties), such use did not negate fair use. The issue “is not whether the competitor engaged in commercial or non-commercial activity; it is whether the competitor used the mark descriptively or non-descriptively.”

Finally, the court addressed the Sixth Circuit’s “trademark use” test. In the Sixth Circuit, plaintiffs carry a threshold burden to show that the defendant is using a mark “in a ‘trademark’ way” that “identifies the source of their goods,” and only if the plaintiff clears this test does the court proceed to likelihood-of-confusion analysis and affirmative

¹⁸ *Sazerac Brands, LLC v. Peristyle, LLC*, No. 3:15-CV-00076-GFVT, 2017 WL 4558022 (E.D. Ky. July 14, 2017).

defenses. The district court had ruled in Peristyle’s favor on this ground, not on fair use. The circuit court noted that, in almost all situations, as in this case, the “non-trademark use” element of this test is identical to the “descriptive use” element of a fair use defense. Nevertheless, the court acknowledged criticism of this test from other circuits and leading academic authorities, and stated that, under a different fact pattern, “we might wish to reconsider whether our test respects the language of the [Lanham Act].” Specifically, the court noted that its test “effectively shifts the burden of statutory fair use from the defendant to the plaintiff” and, because the test does not require that the defendant acts in good faith, it “truncates” the defendant’s burden.

In *Dr. Seuss Enterprises, L.P. v. Comicmix LLC*, 300 F. Supp. 3d 1073 (S.D. Cal. 2017), the district court denied defendant’s motion to dismiss plaintiff’s claims of trademark infringement and unfair competition, finding that defendants’ parodic combination of *Star Trek* and Dr. Seuss books could not satisfy the elements of nominative fair use.

Plaintiff Dr. Seuss Enterprises (“DSE”) is the assignee and owner of copyright and alleged trademark rights in the works of the late Theodor S. Geisel, better known under his pseudonym “Dr. Seuss.” Defendants created a Kickstarter campaign to fund creation and distribution of a book called *Oh the Places You’ll Boldly Go!* (“*Boldly*”), which combines aspects of Dr. Seuss’s works, primarily *Oh the Places You’ll Go!* (“*Go!*”), with elements of the *Star Trek* universe (“to go boldly....”). Defendants labeled their work as a parody and disclaimed any association with CBS Studios or DSE. DSE sent two C&D letters to Defendants, as well as a takedown notice to Kickstarter, which promptly disabled access to Defendants’ campaign. After unsuccessful communications with Defendants, DSE brought suit in the United States District Court for the Southern District of California, alleging copyright and trademark infringement, as well as unfair competition. The copyright aspects of the case are not discussed in these materials.

Defendants moved to dismiss this complaint alleging, *inter alia*, that the trademark claims were barred by the defense of nominative fair use. That motion was granted, but the court gave DSE leave to amend its complaint.¹⁹ DSE filed an amended complaint and Defendants again moved to dismiss asserting nominative fair use.

The court briefly addressed the validity of DSE’s marks. DSE alleged ownership of a large number of common law and registered trademark rights, including a common law right in the title *Oh the Places You’ll Go*. The court noted that book titles are descriptive, and thus require secondary meaning in order to be protectable marks. DSE’s amended complaint alleged, with “little explanation,” that this mark was “distinctive and ha[s] acquired secondary meaning in the minds of the public, and [is] readily associated

¹⁹ *Dr. Seuss Enterprises, L.P. v. ComicMix LLC*, 256 F. Supp. 3d 1099 (S.D. Cal. 2017).

with . . . Dr. Seuss.” Accepting this bare allegation as true at the motion to dismiss stage, the court held that the mark may be valid. Likewise, the court declined to assess the validity of the other myriad marks claimed by DSE at the motion to dismiss stage. For the purposes of analyzing the fair use defense, the court focused solely on defendants’ use of the *Go!* Title, including “the words and the appearance of the title as it appears on the cover of the book.”

The court defined nominative fair use as “use of another’s trademark to identify the trademark owner’s goods or services.” To show nominative fair use in the Ninth Circuit, defendants must establish the three elements set out in *New Kids on the Block v. News Am. Pub. Inc.*, 971 F.2d 302, 308 (9th Cir. 1992): “(i) the product or services in question must be one not readily identifiable without use of the trademark; (ii) only so much of the mark or marks may be used as is reasonably necessary to identify the product or service; and (iii) the user must do nothing that would, in conjunction with the mark, suggest sponsorship or endorsement by the trademark holder.”

The first factor is satisfied “when a trademark also describes a person, a place or an attribute of a product” and there is “no descriptive substitute for the trademark.” Defendants easily met this element: there is no descriptive substitute for a book’s title to describe that book. Defendants also satisfied the third element. Not only had they not done anything to suggest sponsorship or endorsement, they also included a disclaimer on the copyright page of *Boldly* that stated, “[t]his is a work of parody, and is not associated with or endorsed by CBS Studios or Dr. Seuss Enterprises, L.P.”

However, Defendants were unable to satisfy the second element. Defendants’ mash-up used not only the exact words of *Go!*’s title, it also used the original font “down to the shape of the exclamation point.” Defendants could have conveyed that the book was a *Star Trek* twist on *Go!*, without using the original font; the court cited numerous Ninth Circuit cases finding against defendants on this second element when they went beyond mere word marks and incorporated “distinctive lettering.”

After this ruling, Defendants again moved to dismiss DSE’s trademark claims, this time arguing that Defendants’ use of DSE’s marks merited First Amendment protection under the *Rogers v. Grimaldi* test for expressive works. That issue is addressed in Section VIII, *infra*.

In ***Chanel, Inc. v. WGACA, LLC*, No. 18 CIV. 2253 (LLS), 2018 WL 4440507 (S.D.N.Y. Sept. 14, 2018)**, the district court denied in part defendant’s motion to dismiss on nominative fair use and first sale doctrine grounds. The defendant, WGACA (“what goes around comes around”) sells secondhand luxury accessories and apparel. It uses Chanel’s trademark and brand in its advertising and promotion. For example, one of its retail stores “is decorated with a facsimile of a giant Chanel No. 5 perfume bottle” and its social media pages “include quotations of Coco Chanel” and use the hashtag “#WGACACHANEL” to refer to Chanel products. Additionally, WGACA made various

guarantees of authentication, including a website section stating that each of WGACA's items "has been carefully selected, inspected and is guaranteed authentic" and letters of authenticity sent to customers, which state that items sold are, e.g., "authentic Chanel decoration[s]." Chanel sued, alleging various Lanham Act and state law claims. WGACA moved to dismiss, alleging, inter alia, that its use of Chanel's marks was protected under both the nominative fair use doctrine and the first sale doctrine.

The Second Circuit does not treat nominative fair use as an affirmative defense.²⁰ Rather, Second Circuit courts assess nominative fair use as part of the likelihood of confusion analysis, applying their traditional *Polaroid* factors but inserting three additional factors: (i) "whether the use of the plaintiff's mark is necessary to describe both the plaintiff's product or service and the defendant's product or service, that is, whether the product or service is not readily identifiable without use of the mark; (ii) "whether the defendant uses only so much of the plaintiff's mark as is necessary to identify the product or service"; and (iii) "whether the defendant did anything that would, in conjunction with the mark, suggest sponsorship or endorsement by the plaintiff holder, that is, whether the defendant's conduct or language reflects the true or accurate relationship between plaintiff's and defendant's products or services."

Here, applying these factors, the court found that WGACA's use of Chanel's marks may create a likelihood of confusion. First, WGACA's Chanel-branded items would be "readily identifiable" as Chanel without WGACA's extensive use of Chanel's marks, including use of the #WGACACHANEL hashtag. Second, Chanel plausibly alleged that WGACA displayed Chanel-branded goods more prominently than other luxury-brand goods, and thus "stepped over the line into a likelihood of confusion" by using the Chanel's marks "too prominently or too often, in terms of size, emphasis, or repetition." Finally, by using the hashtag #WCAGACHANEL and WGACA's guarantees of authentication "may be taken as suggesting sponsorship or endorsement by Chanel."

On the first sale doctrine, the court noted that the defense was limited to situations where a "purchaser resells a trademarked article under the producer's trademark, and nothing more." Here, WGACA allegedly "did much more than laconically resell Chanel-branded products" because "its presentations were consistent with selling on Chanel's behalf." Hence, at least at the motion to dismiss stage, WGACA could not prevail.

VIII. EXPRESSIVE USE

In *Dr. Seuss Enterprises, L.P. v. ComicMix LLC*, No. 16-CV-2779-JLS (BGS), 2018 WL 2306733 (S.D. Cal. May 21, 2018), the district court granted defendant's

²⁰ *Int'l Info. Sys. Sec. Certification Consortium, Inc. v. Sec. Univ., LLC*, 823 F.3d 153, 156 (2d Cir. 2016).

motion for partial judgment on the pleadings, finding that certain aspects of defendants' parodic combination of *Star Trek* and Dr. Seuss books merited First Amendment protection under the *Rogers v. Grimaldi* test for trademark use in an expressive work.

Plaintiff Dr. Seuss Enterprises (“DSE”) is the assignee and owner of copyright and alleged trademark rights in the works of the late Theodor S. Geisel, better known under his pseudonym “Dr. Seuss.” Defendants created a book called *Oh the Places You’ll Boldly Go!* (“*Boldly*”), which combines aspects of Dr. Seuss’s works, primarily *Oh the Places You’ll Go!* (“*Go!*”), with elements of the *Star Trek* universe (“to go boldly . . .”). Defendants labeled their work as a parody and disclaimed any association with CBS Studios or DSE. Nevertheless, DSE brought suit alleging copyright and trademark infringement, as well as unfair competition.²¹ Defendants moved to dismiss the trademark claims, on the alternative grounds of nominative fair use and First Amendment protection under the *Rogers v. Grimaldi* test. In a 2017 decision (discussed in Section VII, *supra*) the court denied the motion as to nominative fair use.

Rogers provides a two-prong test for whether a potentially infringing trademark use in an expressive work is subject to First Amendment protection. First, Defendants' use of the mark “must be relevant to the underlying work.” If so, the second prong requires that the use “may not explicitly mislead consumers about the source or content of the work.”

In this case, the court considered the Defendants' *Rogers* argument on two separate occasions. First, in June 2017, the court held it would not dismiss DSE's claims on *Rogers* grounds.²² For sake of simplicity, the court ignored most of DSE's alleged marks in various aspects of the book, focusing only on DSE's plausible common law right to the book's title, *Oh the Places You'll Go*. With respect to use of the title, the court found that Defendants had clearly satisfied both *Rogers* prongs: there was “no question” that use of the title was relevant to Defendants' artistic purpose, and the book did not explicitly mislead consumers about the source or content of the work. However, in the original *Rogers v. Grimaldi* decision, the Second Circuit stated, in a footnote, that the *Rogers* test “would not apply to misleading titles that are confusingly similar to other titles” because “[t]he public interest in sparing consumers this type of confusion outweighs the slight public interest in permitting authors to use such titles.” On the basis of this “footnote exception,” and because Defendants had not addressed the argument in its briefing, the court denied Defendants' motion as to First Amendment protection.

²¹ The copyright aspects of this case are not described in this summary.

²² *Dr. Seuss Enterprises, L.P. v. ComicMix LLC*, 256 F. Supp. 3d 1099, 1112 (S.D. Cal. 2017).

Fortunately for Defendants, in November 2017, the Ninth Circuit issued a decision in an unrelated case, which expressly held that courts *should not* consider the “footnote exception” in applying *Rogers* to expressive works.²³ Subsequently, Defendants moved for the court to grant partial judgment on the pleadings on the First Amendment issue, in light of the intervening decision. This time around, Defendants prevailed. Re-applying the *Rogers* test, the court noted that the first prong (artistic relevance) is a “low bar—the level must merely be above zero.” Since Defendants’ book’s title was undoubtedly relevant to the parody book’s artistic content, this prong was clearly satisfied. On the second prong, the court found that while Defendants’ parody used a similar title and copied numerous stylistic aspects of the original book, it was not explicitly misleading. Such similarity may be confusing but it is not an *explicit* statement that the work is associated with or endorsed by DSE.

Shortly after the Dr. Seuss case, in *Gordon v. Drape Creative, Inc.*, **897 F.3d 1184 (9th Cir. 2018)**, the Ninth Circuit once again clarified its *Rogers* jurisprudence. The case addressed whether plaintiff, who had created a massively viral YouTube video and trademarked catchphrases used in that video, could bring an infringement suit against defendants, greeting card companies that used slight variations of the catchphrases in their cards.

The plaintiff, Christopher Gordon, is the author of *The Crazy Nastyass Honey Badger*, an online video featuring National Geographic footage of a honey badger overlaid with Gordon’s humorous narration.²⁴ In the video, Gordon repeats variations of the catchphrases “Honey Badger Don’t Care” and “Honey Badger Don’t Give a S---,” as a honey badger hunts and eats its prey. The video became a cultural sensation: it has been viewed over 89 million times on YouTube, and was the subject of numerous pop-culture references in television shows, magazines, and social media. Gordon produced and sold goods with the catchphrases, such as books, wall calendars, t-shirts, costumes, plush toys, mouse pads, mugs, and decals, and eventually registered “Honey Badger Don’t Care” for various classes of goods, including greeting cards. Defendants, two greeting cards companies, produced various cards using the catchphrases with small variations. For example, one card featured a picture of a honey badger on the front with the message “It’s Your Birthday”; the inside of the card just said “Honey Badger Don’t Give a S---.” Plaintiff sued for trademark infringement, but the district court granted summary judgment for defendants under the *Rogers* test for expressive use of trademarks.

²³ *Twentieth Century Fox Television v. Empire Distrib., Inc.*, 875 F.3d 1192 (9th Cir. 2017), *cert. denied sub nom., Empire Distrib. Inc. v. Twentieth Century Fox Television*, No. 17-1383, 2018 WL 1609822 (U.S. Oct. 1, 2018).

²⁴ The video is available here: <https://www.youtube.com/watch?v=4r7wHMg5Yjg>.

When assessing potential trademark infringement in an artistically expressive work, the Ninth Circuit eschews the likelihood of confusion test and applies the Second Circuit’s *Rogers v. Grimaldi* test for whether the use is protected by the First Amendment. In this case, the court clarified the burden of proof to apply on that test. First, the defendant “must come forward and make a threshold legal showing that its allegedly infringing use is part of an expressive work protected by the First Amendment.” If the defendant succeeds, the plaintiff bears a “heightened burden” of satisfying not only the traditional likelihood of confusion test but also at least one of the two *Rogers* prongs: that the mark is either not artistically relevant to defendant’s underlying work or that the mark explicitly misleads consumers as to the source or content of the work.

Here, defendants easily met their initial burden: greeting cards, although not high art, are clearly expressive works. However, after reviewing the five cases in which the Ninth Circuit had previously applied the *Rogers* test, the court noted that this case demonstrates “*Rogers*’s outer limits” with respect to the first *Rogers* prong (artistic relevance). On one hand, the threshold on this prong is low: “the level of artistic relevance . . . must merely be above zero.” On the other hand, in this case, while Defendants’ use of the marks was clearly relevant to the cards *as a whole*, it was not necessarily relevant to the “defendants’ own artistry.” In order for *Rogers* to be satisfied, the defendant must use the mark “for artistic reasons,” rather than “merely to appropriate the goodwill inhering in the mark or for no reason at all.” In other words, “the mark must both relate to the defendant’s work and the defendant must add his own artistic expression beyond that represented by the mark.”

Ultimately, the court reversed the district court, finding that there remained a triable issue of fact “as to whether defendants added their own artistic expression, as opposed to just copying [plaintiff’s] artistic expression.” Notably, Gordon’s agent had met with Defendants’ parent corporation to discuss a possible licensing deal. The parent corporation rejected the deal but, shortly thereafter, Defendants unilaterally developed their own line of cards. Defendants’ president, who drafted the cards, could not recall what inspired them. These facts suggested that Defendants may have “simply used [plaintiff’s] mark in the same way that [plaintiff] was using it—to make humorous greeting cards in which the bottom line is ‘Honey Badger don’t care.’” Hence, a jury could find that the cards were “only intelligible to readers familiar with [plaintiff’s] video and deliberately trade on the goodwill associated with [plaintiff’s] brand.”

IX. DAMAGES

In *Stone Creek Inc. v. Omnia Italian Design Inc.*, No. CV-13-00688-PHX-DLR, 2018 WL 1784689 (D. Ariz. Apr. 12, 2018), *appeal docketed*, No. 18-15914 (9th Cir. 2018) the district court found that although the defendant had *intentionally copied* plaintiff’s trademark, the defendant had not *willfully infringed* that mark and, thus, could not be held liable for disgorgement of profits.

Plaintiff Stone Creek was a manufacturer and seller of furniture based in Arizona; it registered its STONE CREEK mark in Arizona in 1992 and federally in 2012. Defendant Omnia was Stone Creek's business partner; since 2002, the two worked under an agreement under which Omnia manufactured and supplied leather furniture branded with the STONE CREEK mark for the plaintiffs to sell in its retail stores.

In 2008, Omnia began to supply its own furniture bearing the STONE CREEK label to another retailer client in the Midwest. Omnia took this step without notifying or asking permission from Stone Creek. Omnia "copied the logo directly from Stone Creek's materials" and "plastered the mark onto a host of items" including warranty cards, as well as, "binders, leather samples, and color boards for display in . . . stores." Stone Creek was eventually contacted by multiple customers including one customer who purchased the other company's furniture but was led to Stone Creek's website by the STONE CREEK mark on the warranty card. As the court noted, "[i]n a move not recommended when litigation is certainly impending," an Omnia executive sent an email to Stone Creek stating, "[i]n this day of internet shopping and surfing, it is unfortunate and probably a nuisance for you that your stores are receiving inquiries regarding these products due to the similar name."

Despite these facts, the trial court entered a bench trial verdict in Omnia's favor, finding that there had been no likelihood of confusion, primarily because while Stone Creek exclusively marketed in furniture in Arizona, Omnia marketed its furniture in the Midwest.²⁵ The Ninth Circuit reversed, holding that the district court had misapplied the *Sleekcraft* factors and holding that Omnia was indeed liable for trademark infringement.²⁶ The circuit court also addressed a longstanding circuit split concerning the standard for awarding disgorgement of profits. Specifically, the circuit court endorsed the Federal Circuit's view that "willfulness remains a prerequisite for awarding a defendant's profits." The circuit court remanded for a determination on whether Omnia's infringement was indeed willful as a matter of law.

On remand, the district court found that Omnia did not willfully infringe Stone Creek's mark. Stone Creek had argued that Omnia's "deliberate adoption" of an identical mark compelled the conclusion that Omnia's infringement had been willful. However, the court held that willful infringement requires an "intent to deceive," either by "exploit[ing] the advantage of an established mark" or "attempt[ing] to gain the value of an established name of another." In this case, the consumers targeted by Omnia were not aware of Stone Creek's mark, as the two parties marketed their furniture in wholly

²⁵ *Stone Creek Inc. v. Omnia Italian Design Inc.*, No. CV-13-00688-PHX-DLR, 2015 WL 6865704, at *1 (D. Ariz. Nov. 9, 2015).

²⁶ *Stone Creek, Inc. v. Omnia Italian Design, Inc.*, 875 F.3d 426 (9th Cir. 2017), *cert. denied*, 138 S. Ct. 1984, 201 L. Ed. 2d 248 (2018).

distinct geographical regions. Additionally, Omnia did not copy the mark because it had intended to capitalize on Stone Creek’s reputation; rather, they adopted the name because it “sounded ‘American’” and it was “convenient . . . because the marketing materials and logo were already prepared.” Further, Omnia’s failure to run a trademark search or otherwise exercise care to avoid infringement did not constitute conclusive evidence of willfulness.

Finally, the court found that even if Omnia had willfully infringed, Stone Creek would still not be entitled to disgorgement of Omnia’s profits. Because Omnia’s consumers were not aware of Stone Creek’s brand, they had experienced no actual confusion, and, thus, they must have purchased the infringing furniture for reasons unrelated to a false affiliation with Stone Creek. Thus, the court held, Omnia’s profits were not attributable to its infringement, and, therefore, such profits should not be disgorged.

X. ATTORNEYS’ FEES

In *Nantkwest, Inc. v. Iancu*, 898 F.3d 1177 (Fed. Cir. 2018), the Federal Circuit, sitting *en banc*, reversed the original panel’s decision holding that a statute permitting the USPTO to recover “all the expenses of the proceedings” from a patent applicant’s appeal of an adverse decision includes the pro-rata share of the attorneys’ fees the United States Patent and Trademark Office incurred to defend applicant’s appeal. The case may carry significant implications for *ex parte* appeals of TTAB decisions under the Lanham Act.

Nantkwest is the assignee of an application for a patent directed to a method of treating cancer by administering natural killer cells. The USPTO rejected this application on obviousness grounds. The Patent Trial and Appeal Board (PTAB) affirmed the examiner’s rejection and Nantkwest filed an appeal to the district court under 35 U.S.C. § 145. Section 145 permits a patent applicant to appeal a PTAB decision to the Eastern District of Virginia, but states, “All the expenses of the proceedings shall be paid by the applicant” regardless of the outcome. In this case, the USPTO prevailed on the merits²⁷ and subsequently moved to recover \$111,696.39 of the USPTO’s fees under the § 145 expense provision. The district court granted the request for expert fees but denied the attorneys’ fees, citing the “American Rule” under which litigants pay their own attorneys’ fees, win or lose, unless a contract or statute *specifically and explicitly* provides otherwise.²⁸ On appeal, a 2–1 panel of the Federal Circuit reversed, holding

²⁷ *CoNKwest, Inc. v. Lee*, Case No. 113-cv-01566-GBL-TCB, 2015 WL 13628157 (E.D. Va. Sept. 2, 2015). This merits decision was affirmed in a *separate* opinion of the Federal Circuit, *sub nom*, *Nantkwest, Inc. v. Lee*, 686 F. App’x 864 (Fed. Cir. 2017).

²⁸ *Nankwest, Inc. v. Lee*, 162 F. Supp. 3d 540 (E.D. Va. 2016).

that even if the “American Rule” applied to § 145, the term “all the expenses” included attorney fees.²⁹ The Federal Circuit voted *sua sponte* to hear the appeal *en banc*.³⁰ With four judges dissenting, the court reversed the panel’s decision and affirmed the district court judgment.

The PTO argued, first, that § 145 does not even implicate the American Rule because the American Rule only applies to statutes that specifically shift fees in favor of a prevailing party. Section 145, on the other hand, shifts fees to the PTO, *regardless* of which party prevails. The *en banc* court disagreed, holding that numerous Supreme Court cases implied that no such limitation on the American Rule exists.

Having established that the American Rule does apply to § 145, the court held that the statute’s statement that “[a]ll the expenses of the proceedings shall be paid by the applicant” lacked the “specific and explicit congressional authorization required to displace the American Rule.” While the American Rule does not require any “magic words,” the language of § 145 is “at best ambiguous.” The court pointed to numerous statutes that distinguish between recovery of “expenses” and “attorneys’ fees.” Indeed, several other provisions of the Patent Act itself specifically reference “attorneys’ fees,” indicating that § 145’s use of the term “expenses” would not include attorneys’ fees. The dissent disagreed, arguing that “*all expenses*” plainly included the expense of the PTO staff attorneys’ salaries, and noting that because the PTO does not retain outside counsel in these hearings, such salaries are properly considered *expenses* rather than *fees*.

Both the dissent and majority provided several dictionary definitions from the nineteenth century (contemporaneous with the drafting of § 145) and arguments concerning the statute’s legislative history. With respect to policy considerations, the court noted that § 145 proceedings are quite rare, and that even if the PTO litigated 10 such cases per year at a cost of \$1 million, when spread among more than 627,000 annual patent applications the price to the government was quite small.

Although *Nantkwest* is a patent case, it looms large for trademark practitioners. INTA filed amicus briefs for both the panel and *en banc* hearings of the case.³¹ Just as Patent Act § 145 permits appeals of PTAB decision to a district court, the Lanham Act permits *ex parte* appeals of TTAB decisions under 15 U.S.C. § 1071(b)(1). Moreover, in

²⁹ *Nantkwest, Inc. v. Matal*, 860 F.3d 1352 (Fed. Cir. 2017).

³⁰ *NantKwest, Inc. v. Matal*, 869 F.3d 1327 (Fed. Cir. 2017).

³¹ See, “INTA Files Amicus Brief in Patent Case with Broad Implications for Trademark Litigants,” https://www.inta.org/INTABulletin/Pages/International_Amicus_Committee_Update_Nantkwest_Matal_7303.aspx.

language very similar to § 145, § 1071(b)(3) provides that, for such appeals, “all the expenses of the proceeding shall be paid by the party bringing the case, whether the final decision is in favor of such party or not.”

In accord with the original *Nantkwest* panel’s holding on § 145, the Fourth Circuit recently held that § 1071(b)(3) does require trademark applicants to pay the USPTO’s attorneys’ fees in *ex parte* appeals, regardless of the outcome of the case.³² The *en banc* *Nantkwest* majority did not reach any holding on the Lanham Act, but did expressly decline to follow the *Shammas* court’s reasoning. Indeed, the court found that, apart from the *Shammas* holding, there is no other federal statute “requiring a private litigant to pay the government’s attorneys’ fees without regard to the party’s success in the litigation.”

In *Tobinick v. Novella*, **884 F.3d 1110 (11th Cir. 2018)**, the Eleventh Circuit joined an emerging consensus among the circuits, holding that the “exceptional case” standard for awarding attorneys’ fees under the Patent Act, as defined in the Supreme Court’s *Octane Fitness* decision, also applies to cases brought under the Lanham Act.

Under Section 35(a) of the Lanham Act, attorneys’ fees may only be awarded in “exceptional” cases.³³ Until recently, many circuit courts, including the Eleventh Circuit, required a showing of culpable conduct, such as bad faith, fraud, malice, or knowing infringement, before a case could be found “exceptional.” However, in *Octane Fitness*,³⁴ the Supreme Court interpreted the term “exceptional cases” in the context of Patent Act’s attorneys’ fees provision (§ 285), holding that an “exceptional” case “is simply one that stands out from others with respect to the substantive strength of a party’s litigating position . . . or the unreasonable manner in which the case was litigated.” Although *Octane Fitness* defined “exceptional case” under the Patent Act, not the Lanham Act, numerous circuits have concluded that the *Octane* standard for attorney fees should be applied in trademark cases.³⁵

³² *Shammas v. Focarino*, 784 F.3d 219 (4th Cir. 2015).

³³ 15 U.S.C. § 1117(a).

³⁴ *Octane Fitness LLC v. Icon Health & Fitness, Inc.*, 134 S. Ct. 1749 (2014).

³⁵ *E.g.*, *Romag Fasteners, Inc. v. Fossil, Inc.*, 866 F.3d 1330 (Fed. Cir. 2017) (interpreting Second Circuit law); *Baker v. DeShong*, 821 F.3d 620 (5th Cir. 2016); *SunEarth, Inc. v. Sun Earth Solar Power Co.*, 839 F.3d 1179 (9th Cir. 2016); *Georgia-Pac. Consumer Prods. LP v. von Drehle Corp.*, 781 F.3d 710 (4th Cir. 2015); *Slep-Tone Entm’t Corp. v. Karaoke Kandy Store, Inc.*, 782 F.3d 313 (6th Cir. 2015); *Fair Wind Sailing, Inc. v. Dempster*, 764 F.3d 303 (3d Cir. 2014).

In this case, the plaintiff, Tobinick, is an internist and dermatologist who patented an injection treatment for spinal pain, neurological dysfunction, and Alzheimer's. The defendant, Novella, criticized the treatment in a blog post, claiming the method was unsupported by medical evidence. The plaintiff sued claiming, *inter alia*, false advertising under the Lanham Act. In 2015, the district court granted summary judgment on the Lanham Act claim, on the grounds that the defendant's blog post was not commercial speech and, therefore, was not actionable under the Lanham Act.³⁶ In 2017, the Eleventh Circuit affirmed.³⁷

The defendant also moved for attorneys' fees under the Lanham Act, arguing that the lawsuit constituted an "exceptional case" under § 35(a). At that point, Eleventh Circuit precedent governed that an "exceptional case" required a finding that the offending party had engaged in subjective bad faith or fraud.³⁸ Despite this precedent, the district court followed the recent near-unanimous holdings of other circuits and applied the *Octane Fitness* standard.³⁹ On appeal, the Eleventh Circuit affirmed, effectively overturning its pre-*Octane* "exceptional case" precedents and holding that "to be an 'exceptional case' under the Lanham Act requires only that a case 'stands out from others,' either based on the strength of the litigating positions or the manner in which the case was litigated."

Applying that standard, the court also affirmed the district court's award of \$223,598.75 in fees.⁴⁰ The court noted that a case will not qualify as "exceptional" "merely because one side has zealously pursued or defended its claim" especially on an issue (like the definition of commercial speech) with "no directly controlling precedent." Nevertheless, the fee award was appropriate in this case, where plaintiff had "responded to a number of adverse decisions by accelerating the pace of his filings, repeatedly seeking to add parties and claims and bringing what the court viewed as baseless motions for sanctions and accusations of perjury."

³⁶ *Tobinick v. Novella*, 142 F. Supp. 3d 1275, 1278 (S.D. Fla. 2015).

³⁷ *Tobinick v. Novella*, 848 F.3d 935 (11th Cir. 2017).

³⁸ *See, e.g., Burger King v. Pilgrim's Pride Corp.*, 15 F.3d 166 (11th Cir. 1994); *Tire Kingdom, Inc. v. Morgan Tire & Auto, Inc.*, 253 F.3d 1332 (11th Cir. 2001).

³⁹ *Tobinick v. Novella*, 207 F. Supp. 3d 1332 (S.D. Fla. 2016).

⁴⁰ The court also affirmed the district court's award of an additional ~\$36,000 in attorneys' fees under the California anti-SLAPP statute. That aspect of the case is not discussed in this summary.

Similarly, in *Verisign, Inc. v. XYZ.COM LLC*, 891 F.3d 481 (4th Cir. 2018), the Fourth Circuit clarified its own “exceptional case” standard under *Octane Fitness*. In 2015, the Fourth Circuit became one of the first circuits to apply *Octane Fitness* to the Lanham Act, holding that a court may find a case “exceptional” if it determines that either “(1) there is an unusual discrepancy in the merits of the positions taken by the parties, based on the non-prevailing party's position as either frivolous or objectively unreasonable; (2) the non-prevailing party has litigated the case in an unreasonable manner; or (3) there is otherwise the need in particular circumstances to advance considerations of compensation and deterrence.”⁴¹

In this case, the plaintiff, Verisign, is the exclusive operator of the .com and .net top-level domains (“tld’s”); defendant, XYZ.com, marketed domains under the .xyz tld. Verisign brought suit under the Lanham Act, alleging that XYZ had made numerous false and misleading claims in marketing .xyz domain names and disparaging Verisign’s registry. In 2015, the district court granted summary judgment to XYZ.com on the merits,⁴² and the Fourth Circuit affirmed.⁴³ XYZ.com then moved for attorneys’ fees. The district court denied the motion, holding that, under the Lanham Act, the party seeking attorney fees’ must prove its entitlement to fees with “clear and convincing evidence.” The district also suggested that, in order to prove an “exceptional case” under any of the Fourth Circuit’s aforementioned three post-*Octane* factors, the moving party must show evidence of bad faith or independently sanctionable conduct.

On appeal, the Fourth Circuit reversed. Regarding burden of proof, the court held that a prevailing party need only prove an exceptional case by a *preponderance of the evidence*, rather than by *clear and convincing evidence*. The former was the standard of proof applied by the Supreme Court in *Octane Fitness*, and the Fourth Circuit saw no reason to depart from that standard under the Lanham Act. Additionally, every other circuit that had addressed the standard of proof question had likewise settled on “clear and convincing evidence.”

Regarding a “bad faith” requirement, the circuit reversed again, holding that, post-*Octane*, a “losing party’s conduct need not have been independently sanctionable or taken in bad faith in order to merit an award of attorney fees to the prevailing party under the Lanham Act.” Additionally, the court overturned its own pre-*Octane Fitness* jurisprudence, which had established that while a prevailing *plaintiff* seeking attorney

⁴¹ *Georgia-Pac. Consumer Prods. LP v. von Drehle Corp.*, 781 F.3d 710 (4th Cir. 2015).

⁴² *Verisign, Inc. v. XYZ.com, LLC*, No. 1:14-CV-01749, 2015 WL 7430016 (E.D. Va. Nov. 20, 2015).

⁴³ *Verisign, Inc. v. XYZ.COM LLC*, 848 F.3d 292 (4th Cir. 2017).

fees must demonstrate bad faith, a prevailing *defendant* might qualify for an award of attorney fees upon a showing of “something less than bad faith.”⁴⁴ The court held that this dual standard was no longer sound in a post-*Octane* world.

Hence, at this time, the Third, Fourth, Fifth, Sixth, Ninth, and Eleventh Circuits have all held that *Octane Fitness* changed the standard for fee-shifting under the Lanham Act, and the Federal Circuit, interpreting Second Circuit law, has done the same.⁴⁵ The Seventh Circuit has applied earlier contrary case law to a Lanham Act fee dispute, but did so without mentioning *Octane Fitness*.⁴⁶ As of now, the development of an actual circuit split on this issue appears unlikely.

XI. INJUNCTIVE RELIEF

In *Commodores Entertainment Corp. v. McClary*, 879 F.3d 1114 (11th Cir. 2018), *cert. denied*, No. 18-47, 2018 WL 3349494 (U.S. Oct. 1, 2018), the Eleventh Circuit affirmed the district court’s grant of a permanent injunction barring the defendant, a former member of The Commodores, from using several marks connected to that band name in a manner other than fair use.

The facts of this case are set out in Section II, *supra*. The case concerns rights to the name “The Commodores,” the prominent funk/soul band. Plaintiff, Commodores Entertainment Corp. (“CEC”) is a corporation formed by the band in 1979, which registered four trademarks with the USPTO for the word mark “THE COMMODORES” and the word mark “COMMODORES” with a design. Defendant McClary is a former member of the band who, after leaving, continued to use variations of “The Commodores” name, performing as, *e.g.*, “The 2014 Commodores,” and “The Commodores Featuring Thomas McClary.” CEC sued, claiming *inter alia*, trademark infringement. In 2014, the district court granted CEC a preliminary injunction barring McClary from using CEC’s marks “in a manner other than fair use.” 2014 WL 5285980 (M.D. Fla. Oct. 15, 2014). The Eleventh Circuit affirmed. 648 Fed. Appx. 771 (11th Cir. 2016). In 2018, after a two-week trial, the district court granted CEC’s motion for judgment as a matter of law, ruling that CEC had rights to the marks at issue and that

⁴⁴ *Retail Services, Inc. v. Freebies Publishing*, 364 F.3d 535 (4th Cir. 2004).

⁴⁵ The Second Circuit itself has not yet reached the issue. *See Dynamic Concepts, Inc. v. Tri-State Surgical Supply & Equip., Ltd.*, 716 F. App’x 5, 17 (2d Cir. 2017) (declining to address whether district court erred in requiring bad faith for award of attorney fees in light of *Octane Fitness*); *Penshurst Trading Inc. v. Zodax L.P.*, 652 F. App’x 10, 12 (2d Cir. 2016) (assuming without deciding that *Octane Fitness* applies to Lanham Act cases).

⁴⁶ *See Burford v. Accounting Practice Sales, Inc.*, 786 F.3d 582, 588 (7th Cir. 2015).

McClary does not, and converted the preliminary injunction into a permanent injunction. McClary filed an interlocutory appeal of the JMOL and the injunction.⁴⁷

McClary argued that the injunction was overbroad because of its extraterritorial reach: it barred him from use of marks abroad, as well as in the U.S. The court disagreed. The court cited *Steele v. Bulova*, 344 U.S. 280 (1952), for the proposition that Congress has the authority to project the impact of trademark laws beyond United States borders, and applied the Eleventh Circuit’s three-factor analysis for permitting extraterritorial application of the Lanham Act: (i) whether the defendant is a U.S. corporation; (ii) whether the foreign activity had substantial effects in the U.S.; and (iii) whether exercising jurisdiction would interfere with the sovereignty of another nation.

Here, both parties were U.S. citizens, McClary’s group is managed in the U.S. by a U.S. citizen, and his use of the marks abroad was likely to create confusion both abroad and within the United States. Finally, there was no record that defendants held foreign trademarks with which the Court’s holding would conflict. As a result, the extraterritorial nature of the district court’s injunction was not an abuse of discretion.

Defendant’s other argument concerning overbreadth—that he was prevented from “hold[ing] himself and his music out to the public in an historically accurate way”—was moot because both the plaintiff and the district court had acknowledged that the injunction’s allowance of fair use would not foreclose McClary from billing himself as “Thomas McClary, founder of The Commodores,” and that McClary is “free to make fair use of the Commodore Marks to provide historically accurate information about his tenure as a Commodore.

Other issues in this opinion are summarized in Section II, *supra*.

XII. IRREPARABLE HARM

In *adidas Am., Inc. v. Skechers USA, Inc.*, 890 F.3d 747 (9th Cir. 2018), the Ninth Circuit revisited its standards for establishing a likelihood of irreparable harm in trademark cases. Adidas (plaintiff) and Skechers (defendant) are two of the largest shoe companies in the U.S. This case concerned two Skechers shoe designs that Adidas alleged infringed its own trade dress and trademarks. First, Adidas alleged that one Skechers design (the “Onix”) infringed the unregistered trade dress of Adidas’s iconic “Stan Smith” shoe. Second, Adidas alleged that a different Skechers design (the “Cross Court”) infringed and diluted Adidas’s Three-Stripe trademark. Adidas moved for a

⁴⁷ The circuit court’s affirmation of the JMOL is discussed in Section II, *supra*.

preliminary injunction prohibiting Skechers from selling either shoe. The district court granted the motion as to both shoes.⁴⁸

Regarding the Stan Smith design, the court affirmed the district court's findings that the trade dress had acquired secondary meaning: Adidas had sold 40 million pairs of the shoe, and Skechers had intentionally copied much of the shoe's design. Applying the *Sleekcraft* factors, the court also affirmed the district court's finding of a likelihood of confusion between the Stan Smith and Skechers's Onix design, because, *inter alia*, the two shoes were "nearly identical." The court also affirmed most of the district court's findings on likelihood of confusion and dilution with respect to Skechers's infringement of the Three-Stripe mark.

On irreparable harm, the court applied the standard from its 2013 *Herb Reed* decision, under which "evidence of loss of control over business reputation and damage to goodwill can constitute irreparable harm, so long as there is concrete evidence in the record of those things."⁴⁹ With respect to the Stan Smith shoe, the court affirmed the district court's finding of irreparable harm. The court cited Adidas's "significant efforts . . . invested in promoting the Stan Smith through specific and controlled avenues such as social media campaigns and product placement," its efforts to carefully control the supply of Stan Smith shoes, and surveys showing that approximately twenty percent of respondents believed Skechers's Onix was made by, approved by, or affiliated with Adidas.

However, with respect to the Three-Stripe infringement, the court reversed the district court, holding that Adidas had *not* shown a likelihood of irreparable harm. Adidas argued that Skechers harmed Adidas's ability to control its brand image because consumers who see others wearing Skechers's three-stripe shoes associate the allegedly lesser-quality Skechers with Adidas and its own Three-Stripe mark. But, Adidas did not set forth evidence showing that consumers actually did view Skechers as a lower-quality brand, except for surveys of Adidas's own employees. Additionally, this "loss of control" theory was in tension with Adidas's theory of post-sale confusion. Because the allegedly infringing shoes bore Skechers's logo, post-sale confusion could only exist if the consumer viewed the shoes "from a distance." From that distance, consumers would be unlikely to be able to distinguish the quality of the shoes. Hence, "even if Skechers does make inferior products, there is no evidence that Adidas's theory of post-sale confusion would cause consumers to associate such lesser-quality products with Adidas" and, even if there some consumers were confused, Adidas had not provided "concrete evidence" that such confusion would yield irreparable harm.

⁴⁸ *Adidas Am., Inc. v. Skechers USA, Inc.*, 149 F. Supp. 3d 1222 (D. Or. 2016).

⁴⁹ *Herb Reed Enterprises, LLC v. Fla. Entm't Mgmt., Inc.*, 736 F.3d 1239 (9th Cir. 2013).

In dissent, Judge Clifton argued that Adidas had indeed shown irreparable harm for both shoes. He noted that Adidas was entitled to rely on its employees' testimony to establish that Skechers was a lower-end brand, and that Skechers did not dispute that testimony. Additionally, even without such testimony, loss by Adidas of control over its mark was by itself irreparably harmful." To emphasize the potential harm of post-sale confusion, Judge Clifton also referred to his own experience in private practice where he was retained by Louis Vuitton to combat the sale of cheaper imitations.

Judge Clifton distinguished this case from the facts in *Herb Reed*, where the Ninth Circuit similarly found no likelihood of irreparable harm despite the fact that the plaintiff was likely to succeed on the merits. Unlike here, the plaintiff in *Herb Reed* presented basically zero evidence of irreparable harm. Therefore, while *Herb Reed* held that a plaintiff could not merely rely on the presumption of harm, it "did not disclaim the logic" behind the presumption. In most cases, if the plaintiff can establish a likelihood of infringement, "it is not a big leap" to find irreparable harm.

XIII. REVERSE PASSING OFF

In *OTR Wheel Engineering, Inc. v. West Worldwide Servs., Inc.*, **897 F.3d 1008 (9th Cir. 2018)**, the Ninth Circuit affirmed a district court judgment finding defendant liable for *inter alia* reverse passing off.

Plaintiff, OTR, and defendant, West, both sell tires for industrial use. West wanted to sell "355-size" tires to one of OTR's existing customers. To do so, West approached OTR's Chinese manufacturer and requested a set of 355-size tires. When the manufacturer advised that it would take a long time to make a mold for West's tires, West asked the manufacturer to just use OTR's molds and take out the nameplate, so that "nobody will know." The manufacturer agreed and West successfully poached OTR's customer. OTR sued, bringing numerous Lanham Act and state law claims. A jury found West liable for reverse passing off and some of the state law claims, with actual damages in the amount of \$967,015.

"Passing off" occurs when a producer misrepresents his own goods or services as someone else's, whereas "reverse passing off" is the opposite: the producer misrepresents someone else's goods or services as his own. Reverse passing off is actionable under § 43(a) of the Lanham Act if it constitutes a "false designation of origin." In its 2003 *Dastar* decision, the Supreme Court held that "origin" refers to "the producer of the tangible goods that are offered for sale, and not to the author of any idea, concept, or communication embodied in those goods." Consequently, "a reverse passing off claim cannot be brought to prevent the *copying* of intellectual property." "Copying" is dealt with through copyright and patent law, not through trademark law. Instead, reverse passing off, is only appropriate when a defendant passes off the plaintiff's actual products as defendant's own.

Citing *Dastar*, West argued that by using OTR's mold, he was *copying* OTR's tire design, rather than *passing off* a genuine OTR tire as his own. The court disagreed. There was evidence that West asked the Chinese manufacturer to fill one of OTR's orders in advance, so that he could take some and provide to his prospective client as a demo. Because these tires were literally intended for OTR, a reasonable jury could conclude the tires were actually OTR's products rather than merely copies of OTR's designs.

The court distinguished this result from *Kehoe*, a seemingly identical Sixth Circuit case from 2015.⁵⁰ In that case, a manufacturer used molds to produce goods for a customer and subsequently reused those molds to manufacture produce additional units to sell in competition with the customer. The Sixth Circuit held that this was copying, not reverse passing off. However, in that case, the manufacturer produced the rival goods *only after* completing the customer's order, and thus, it did not pass off the customer's goods.

Other aspects of this case are discussed in Section III, *supra*.

XIV. LACHES

In *Pinkette Clothing, Inc. v. Cosmetic Warriors Ltd.*, 894 F.3d 1015 (9th Cir. 2018), the Ninth Circuit addressed the effect of two recent Supreme Court cases on whether a defendant may apply laches to a trademark cancellation claim. Those cases, *Petrella*⁵¹ and *SCA Hygiene*,⁵² respectively held that laches is not available as a defense to claims for copyright or patent infringement brought within the limitations periods prescribed under the Copyright and Patent Acts. Here, the Ninth Circuit found that the logic of those cases does not apply to the Lanham Act, and, thus, laches remains a viable defense to a trademark cancellation claim.

Defendant, CWL, has marketed cosmetics under the LUSH mark since the mid-1990s, and operates about 940 LUSH retail stores in 49 countries. Plaintiff, Pinkettee, sells young women's clothing under several different labels, one of which is LUSH. Pinkettee has sold clothing under that name since 2003 and successfully registered a trademark for LUSH in 2010. CWL claims it had no actual knowledge of Pinkettee's LUSH mark until late 2014, when it applied for its own trademark registration for use of LUSH on clothing and was rejected on account of Pinkettee's preexisting registration.

⁵⁰ *Kehoe Component Sales Inc. v. Best Lighting Products, Inc.*, 796 F.3d 576 (6th Cir. 2015).

⁵¹ *Petrella v. Metro-Goldwyn-Mayer, Inc.*, 572 U.S. 663 (2014).

⁵² *SCA Hygiene Prod. Aktiebolag v. First Quality Baby Prod., LLC*, 137 S. Ct. 954 (2017).

In June 2015—about four years and eleven months after Pinkette’s registration issued—CWL finally filed a petition with TTAB to cancel Pinkette’s registration. Pinkette responded by filing an action in district court, seeking a declaratory judgment that either it did not infringe on CWL’s trademark rights, or alternatively that laches bars CWL from asserting its rights against Pinkette. The case went to trial, after which the jury returned a special verdict finding for CWL on infringement and cancellation claims but finding (in an advisory capacity) for Pinkette on its laches defense. The district court agreed on laches, and entered judgment for Pinkette, holding that laches barred CWL’s claims.

On appeal, the Ninth Circuit began by discussing the Supreme Court’s holdings in *Petrella* and *SCA Hygiene*, and held that those cases do not preclude application of laches to trademark claims. The logic underlying those cases was a concern that laches would override the Copyright and Patent Acts’ respective statutes of limitations. The Lanham Act has no statute of limitations; instead, it vests courts with the power to grant relief according “to the principles of equity.”

Nevertheless, CWL argued that laches could not apply where a *cancellation* claim is brought within the five-year period before a registered mark becomes incontestable. 15 U.S.C. § 1064(1). The court found this unconvincing. Notably, § 1069 *expressly* establishes laches as a potential defense in “all inter partes proceedings” before the PTO, including cancellation proceedings. Additionally, incontestability is not a statute of limitations: it merely limits the grounds on which cancellation may be sought rather than barring an action entirely.

Having established that laches remained an applicable defense to cancellation and infringement claims, the court proceeded to review the district court’s application of laches in this case. The Ninth Circuit analyzes laches in a two-step process. First, the court looks to whether the most analogous state statute of limitations” expired prior to the suit. If so, there is a strong presumption in favor of laches. In this case, the applicable state statute was California’s four-year statute of limitations for trademark infringement actions. CWL was on constructive notice of its claims no later than when Pinkette’s registration issued, but CWL waited almost five years to bring its suit. Therefore, the court applied a strong presumption in favor of laches.

Second, the court assessed the equity of laches through the Ninth Circuit’s *E-Systems* factors: (i) “strength and value of trademark rights asserted;” (ii) “plaintiff’s diligence in enforcing mark;” (iii) “harm to senior user if relief denied;” (iv) “good faith ignorance by junior user;” (v) “competition between senior and junior users;” and (vi) “extent of harm suffered by junior user because of senior user’s delay.”

The first factor favored CWL—Pinkette did not dispute that CWL’s marks were strong and valuable. The second factor favored Pinkette, because CWL waited almost five years to petition for cancellation. The third factor was neutral. While Pinkette’s use

would diminish CWL's control over its brand, the two companies had successfully coexisted from 2003 through 2014, and the jury had found that none of Pinkette's profits were attributable to infringement.

The fourth factor favored Pinkette. Pinkette was "open and notorious" in its use of the mark, Pinkette's principals credibly testified that they brainstormed the LUSH name independently from CWL, and "most importantly," there was no evidence that Pinkette sought to free-ride on CWL's good will or otherwise take advantage of the marks' similarity.

The fifth factor weighed in favor of Pinkette as there was no evidence of competition between the two companies. The sixth factor also favored Pinkette, since during the nearly five years that CWL neglected to bring suit, Pinkette "continued to build a valuable business around its trademark" by pursuing trade shows and advertising and significantly expanding its warehouse.

With at least four factors favoring Pinkette, the court held that these factors "validate" the aforementioned strong presumption in favor of laches, and, thus, the court affirmed the district court's grant of summary judgment in favor of Pinkette.

SECTION 4

Trade Secrets Law Update



Presented by

Peter Brody
Ropes & Gray LLP
Washington, DC

Trade Secret Litigation After the Defend Trade Secrets Act (DTSA)

Defend Trade Secrets Act

1. “Defend Trade Secret Act of 2016” (2016)
 - a. Introduced July 29, 2015 in both houses
 - b. President signed the bill into law on May 11, 2016
2. DTSA Key features
 - a. Rights of owners of trade secret
 - b. Trade secret definition
 - c. Potential injunction relief
 - i. Under what circumstances do courts grant injunctions?
 - ii. No specific provision
 - d. Potential economic recovery
 - e. Potential for exemplary damages
 - f. Potential for recovery of attorneys’ fees
 - g. 3-year statute of limitations
 - h. Does not pre-empt state law
 - iii. Except for whistleblower protections
 - i. Ex parte seizures

Post Defend Trade Secret Act

1. 30% increase in trade secret case filings since DTSA
2. Possible reasons for increase:
 - a. DTSA provides opportunity to leverage stronger and more consistent rules of procedure, and enhanced protections and remedies
 - b. Companies opting for trade secret protection instead of patent protection
 - c. Greater workforce mobility
3. Unlike patent litigation, federal trade secret cases are not geographically clustered in certain district courts but rather are generally evenly spread out. However, the district courts with the most trade secret litigation are C.D. Cal., N.D. Ill., S.D.N.Y., D.N.J., and E.D. Pa.

Ex Parte Seizures

1. Express provision for ex parte seizure orders “to prevent the propagation or dissemination of a trade secret that is the subject of the action”

2. Must be an affidavit or verified complaint
 - a. Why a noticed injunction proceeding would be inadequate
 - b. Establishing likely success on the merits, that irreparable harm will occur without seizure, and that harm to applicant “substantially” outweighs harm to any third party
3. Burden of proof is on applicant for the order
 - a. Applicant liable for wrongful or excessive seizure
4. Seizure is only available in “extraordinary circumstances” and target must be in “actual” possession
5. Seizure only by federal law enforcement with necessary assistance from state officials or technical experts (bound by confidentiality)—not the applicant
6. Court controls when and how seizure is carried out
 - a. Whether force may be used to obtain information from locked areas
 - b. Whether to have a special master (bound by confidentiality) sort the information
7. Federal Judicial Center required to develop “best practices” for seizures and for handling electronically stored information
8. Requirements under 18 U.S.C. § 1836(b)(2)
 - a. Rule 65 Order or other equitable relief would be inadequate because party would evade, avoid, or otherwise not comply with such an order
 - b. Immediate and irreparable injury will occur in absence of the seizure
 - c. Harm to the applicant outweighs the harm to the legitimate interests of the opposing party and substantially outweighs the harm to any third parties
 - d. Likelihood of success on trade secret claim
 - e. Actual possession of the trade secret and any property to be seized
 - f. Description with reasonable particularity of the matter to be seized and location
 - g. Opposing party would destroy, move, hide, or otherwise make such matter inaccessible to the court if given notice
 - h. Applicant has not publicized the requested seizure
9. Trends
 - a. Courts continue to favor FRCP 65 TROs and preliminary injunctions.
 - i. One way to show that a Rule 65 order is inadequate is by establishing that the defendant is likely to destroy evidence.
 - ii. Bare allegations are not sufficient; must show that the defendant had concealed evidence or disregarded court orders in the past.
10. Illustrative Cases Declining to Grant Ex Parte Seizures

- a. *OOO Brunswick Rail Mgmt. v. Sultanov*, 2017 WL 67119, Civ. Action No. 5:17-cv-00017 (N.D. Cal. Jan. 6, 2017) (denying request for civil seizure instead ordering preservation of devices at issue pursuant to Rule 65)
- b. *Dazzle Software II, LLC v. Kinney*, Civ. Action No. 1:16-cv-12191 (E.D. Mich. July 18, 2016) denying request for civil seizure instead ordering preservation of devices at issue pursuant to Rule 65)
- c. *Balearia Caribbean Ltd. Corp. v. Calvo*, Civ. Action No. 1:16-cv-23300 (S.D. Fla. Aug 5, 2016) (plaintiff may not rely on bare assertions that the defendant, if given notice, would destroy relevant evidence. Rather, the plaintiff must show that the defendant, or persons involved in similar activities, had concealed evidence or disregarding court orders in the past”).

11. Illustrative Cases Granting Ex Parte Seizures

- a. *Mission Capital Advisors LLC v. Romaka* (S.D.N.Y. July 29, 2016) (defendant claimed he deleted files but forensics later discovered a “trove” of misappropriated files)
- b. *Blue Star Land Servs., LLC v. Coleman*, Civil Action No. 17-cv-931 (W.D. Okla. Dec. 8, 2017) (defendants misappropriated 20,000 documents while employed after learning of a large new project and threatened to usurp opportunity if not given 66% of company among other misconduct).
- c. *Axis Steel Detailing, Inc. v. Prilex Detailing LLC*, No. 2:17-CV-00428-JNP, 2017 WL 8947964, at *1 (D. Utah June 29, 2017) (defendants “had a high level of computer technical proficiency, and there had been attempts by the defendants in the past to delete information from computers, including emails and other data.”).

12. Practical Tips

- a. Educate the court and law enforcement
- b. Submit detailed proposed order, and include catchall provision and deadline
- c. Ensure the proper secure storage of the assets, possibly proposing use of a third-party custodian
- d. Anticipate real-time execution problems
- e. Identify and educate a neutral technical expert

DTSA Damages

1. Damages remedies available under the DTSA are similar to those under the Uniform Trade Secrets Act, or UTSA.
2. A small number of cases have damages awards under the DTSA. In five of these cases, damages were awarded on default judgment. Most are mixed lump sum damages or attorneys’ fees and costs.
 - a. *Solarcity Corporation v. Girma*—court awarded \$61,360 actual damages as well as \$122,720 trebling damages for willfulness. In two cases, defendants received attorneys’ fees and costs for successfully defending trade secret claims.

- b. *Steves and Sons, Inc. v. Jeld-Wen, Inc.*—jury awarded \$1.2 million each for state and DTSA trade secret misappropriation claims, totally \$2.4 million in Trade Secret damages.
- c. *Dalmatia Import Group, Inc. v. Foodmatch Inc. et al.*—jury awarded \$500,000 in damages as one award under both state law and the DTSA

DTSA Appeals

1. Very few appellate decisions to date:
 - a. *First Western Capital Management, Co. v. Malamed*—Lawsuit under both the DTSA and the Colorado trade secrets law against a former employee accused of stealing customer lists. The Tenth Circuit reversed the district court’s grant of a preliminary injunction to First Western, holding that a violation of the DTSA does not create a presumption of irreparable harm.
 - b. Two Ninth Circuit opinions in federal criminal cases briefly mentioned the DTSA, noting that the DTSA had changed the definition of a trade secret for both criminal and civil purposes but declining to apply the new definition because the events of the case predated the DTSA’s 2016 enactment.

EU Directive on Trade Secrets

1. EU’s first such directive to create unified approach to trade secrets, adopted in 2016
2. Creates baseline minimum level of protection which each member state was required to implement in its national laws by June 2018
 - a. Uniform definition of a trade secret
 - b. Trade secret must be subject to reasonable protection measures (intent to keep secret no longer sufficient)
 - c. Reverse engineering generally allowed
 - d. Employees have more freedom to bring knowledge and experience to their next employer
3. Differences from DTSA:
 - a. No new procedural tools in the EU Directive; no ex parte seizures
 - b. No provision for enhanced damages for willful/malicious misappropriation in the EU Directive
 - c. EU Directive contains broader protection for whistleblowers than the DTSA

Trade Secret Litigation in the ITC

1. The International Trade Commission is an independent, quasi-judicial agency tasked with enforcing Section 337 of the Tariff Act, 19 U.S.C. § 1337
2. Trade statute protecting U.S. industries from injuries caused by unfair acts in the importation of goods to the United States
3. The litigation of trade secrets at the ITC is a relatively recent phenomenon, spurred by *TianRui Group Co. v. Int'l Trade Comm'n*, 661 F.3d 1322 (Fed. Cir. 2011), which held that a misappropriation occurring abroad could be remedied by an exclusion order on any importation of goods resulting from the misappropriation:
 - a. Cast steel railway wheels made in China, using trade secret process misappropriated in China
 - b. Extraterritoriality: The ITC may reach imports that relate to trade secret theft that occurred outside the United States. *Id.* at 1329
 - c. Choice of law: A “single federal standard” governs misappropriation as an “unfair act” under Section 337—not state or foreign law. *Id.* at 1327.
 - d. Domestic industry injured by misappropriation and importation need not use the trade secret domestically. *Id.* at 1335
4. Advantages of the ITC
 - a. Speed
 - b. Powerful, self-enforcing exclusionary remedy
 - c. In rem jurisdiction (no personal jurisdiction required)
 - d. Extraterritorial concerns may be minimized
 - e. Flexible evidentiary rules
 - f. Detailed factual record and opinions
 - i. No black box jury verdicts
 - ii. Can help with appeals
 - iii. Efficiencies for parallel litigation (domestic and foreign venues having range of remedies)
5. Disadvantages of the ITC
 - a. Speed
 - b. Expensive
 - c. No damages
 - i. But fines are available for violations of exclusion orders
 - d. Requires substantial up-front work and diligence
 - e. ITC must consider public interest
 - f. Potential for presidential disapproval
 - g. Uncertainty for untested Section 337 theories

Other Emerging Issues Post- DTSA

1. Other Emerging Issues
 - a. Reconciling competing standards
 - b. Does California's rule regarding identifying trade secrets with specificity before discovery apply to federal DTSA actions?
 - c. Trade secret cases involving emerging technologies like blockchain, CRISPR, and AI

Trade Secret Litigation After the Defend Trade Secrets Act

Peter M. Brody

ROPES
& GRAY

ROPES & GRAY LLP

Defend Trade Secrets Act

- “Defend Trade Secrets Act of 2016” (DTSA)
 - Introduced July 29, 2015 in both houses
 - President signed the bill into law on May 11, 2016
 - Applies to any misappropriation “for which any act occurs on or after the date of the enactment” of the DTSA.

2

ROPES & GRAY

Defend Trade Secrets Act

- DTSA – Key Features

- An owner of a trade secret may bring a federal civil action for injunctive relief or damages if aggrieved by misappropriation of a trade secret “related to a product or service used in, or intended for use in, interstate or federal commerce.”
- Trade secret definition – requires that protected information not be known or readily ascertainable to “persons who can obtain economic value from its disclosure or use” in line with the UTSA
- Potential injunctive relief
 - Court may grant an injunction “provided the order does not prevent a person from accepting an offer of employment under conditions that avoid actual or threatened misappropriation”
 - No specific provision (as there is under UTSA) for terminating injunction once information has ceased to be a trade secret

3

ROPES & GRAY

Defend Trade Secrets Act

- DTSA – Key Features (cont’d)

- Potential economic recovery—actual damages, unjust enrichment damages, or in lieu of damages, a reasonable royalty
- Potential for exemplary damages of 2 times actual damages
- Potential for recovery of attorney’s fees by either side if claim made or opposed in bad faith or if misappropriation willful or malicious
- 3 year statute of limitations
- Does not pre-empt state law
 - Except for whistleblower protections
- Ex parte seizures (more later)

4

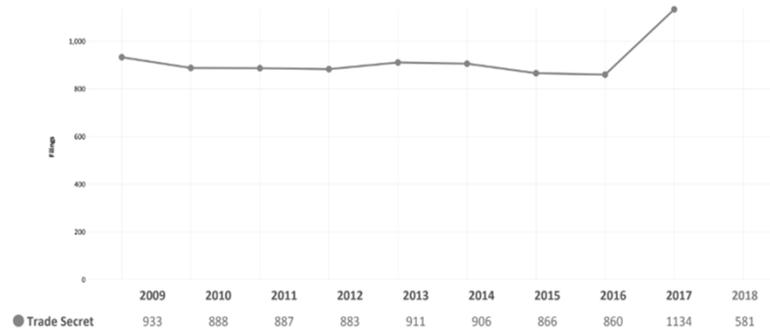
ROPES & GRAY

Post-DTSA

- 30% increase in trade secret case filings since DTSA

– Lex Machina Trade Secret Report (mid-2018)

Figure 1: All Trade Secret Cases Filed from 2009 to 2018 Q2



5

ROPES & GRAY

Post-DTSA

- Possible reasons for post-DTSA increase in trade secret case filings:
 - DTSA provides opportunity to leverage stronger and more consistent rules of procedure, and enhanced protections and remedies
 - Companies opting for trade secret protection instead of patent protection
 - Greater workforce mobility

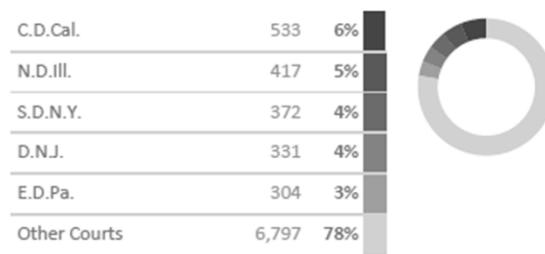
6

ROPES & GRAY

Post-DTSA

- Unlike patent litigation, federal trade secret cases are not geographically clustered in certain district courts but rather are generally evenly spread out. (Lex Machina Trade Secret Report).
- However, the district courts with the most trade secret litigation are:

Figure 3: Trade Secret Litigation Top District Courts by Filings from 2009 to 2018 Q2



7

ROPES & GRAY

Post-DTSA

- In the first two years of the DTSA, DTSA claims were filed in 77 of the 94 federal district courts in the U.S.

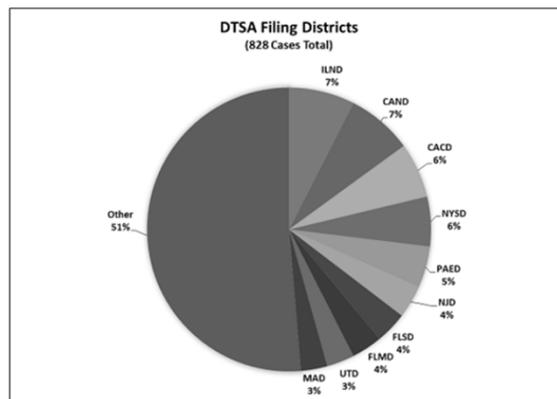


Figure 2 – Federal District DTSA Filing Activity (May 11, 2016 – May 10, 2018)[4]

8

ROPES & GRAY

Post-DTSA

- Overlap of trade secret cases with other claims
 - Lex Machina Trade Secret Report

Figure 4: Overlap of Trade Secret Cases with Other Lex Machina Practice Areas, Cases Filed from 2009 to 2018 Q2

Case Types	Cases
Trade Secret	8849
Trade Secret Alone	2723
Commercial	5192
Trademark	1927
Copyright	971
Patent	528
Antitrust	94
Securities	33
Employment	12

ROPES & GRAY

Ex Parte Seizures

- Express provision for *ex parte* seizure orders “to prevent the propagation or dissemination of a trade secret that is the subject of the action”
- Must be an affidavit or verified complaint
 - Explaining why a noticed injunction proceeding would be inadequate
 - Establishing likely success on the merits, that irreparable harm will occur without seizure, and that harm to applicant “substantially” outweighs harm to any third party
- Burden of proof is on applicant for the order
 - Applicant liable for wrongful or excessive seizure

10

ROPES & GRAY

Ex Parte Seizures

- Seizure is only available in “extraordinary circumstances” and target must be in “actual” possession
- Seizure only by federal law enforcement with necessary assistance from state officials or technical experts (bound by confidentiality)—not the applicant
- Court controls when and how seizure is carried out
 - Whether force may be used to obtain information from locked areas
 - Whether to have a special master (bound by confidentiality) sort the information
- Federal Judicial Center required to develop “best practices” for seizures and for handling electronically stored information

11

ROPES & GRAY

Ex Parte Seizures

- Requirements under 18 U.S.C. § 1836(b)(2)
 - Rule 65 Order or other equitable relief would be inadequate because party would evade, avoid, or otherwise not comply with such an order
 - Immediate and irreparable injury will occur in absence of the seizure
 - Harm to the applicant outweighs the harm to the legitimate interests of the opposing party and substantially outweighs the harm to any third parties
 - Likelihood of success on trade secret claim
 - Actual possession of the trade secret and any property to be seized
 - Description with reasonable particularity of the matter to be seized and location
 - Opposing party would destroy, move, hide, or otherwise make such matter inaccessible to the court if given notice
 - Applicant has not publicized the requested seizure

12

ROPES & GRAY

Ex Parte Seizures

- Trends
 - Courts continue to favor FRCP 65 TROs and preliminary injunctions.
 - One way to show that a Rule 65 order is inadequate is by establishing that the defendant is likely to destroy evidence.
 - Bare allegations are not sufficient; must show that the defendant had concealed evidence or disregarded court orders in the past.

13

ROPES & GRAY

Ex Parte Seizures

- Illustrative Cases Declining to Grant Ex Parte Seizures
 - *OOO Brunswick Rail Mgmt. v. Sultanov*, 2017 WL 67119, Civ. Action No. 5:17-cv-00017 (N.D. Cal. Jan. 6, 2017) (denying request for civil seizure instead ordering preservation of devices at issue pursuant to Rule 65)
 - *Dazzle Software II, LLC v. Kinney*, Civ. Action No. 1:16-cv-12191 (E.D. Mich. July 18, 2016) denying request for civil seizure instead ordering preservation of devices at issue pursuant to Rule 65)
 - *Balearia Caribbean Ltd. Corp. v. Calvo*, Civ. Action No. 1:16-cv-23300 (S.D. Fla. Aug 5, 2016) (plaintiff may not rely on bare assertions that the defendant, if given notice, would destroy relevant evidence. Rather, the plaintiff must show that the defendant, or persons involved in similar activities, had concealed evidence or disregarding court orders in the past”).

14

ROPES & GRAY

Ex Parte Seizures

- Illustrative Cases Granting Ex Parte Seizures

- *Mission Capital Advisors LLC v. Romaka* (S.D.N.Y. July 29, 2016) (defendant claimed he deleted files but forensics later discovered a “trove” of misappropriated files)
- *Blue Star Land Servs., LLC v. Coleman*, Civil Action No. 17-cv-931 (W.D. Okla. Dec. 8, 2017) (defendants misappropriated 20,000 documents while employed after learning of a large new project and threatened to usurp opportunity if not given 66% of company among other misconduct).
- *Axis Steel Detailing, Inc. v. Prilex Detailing LLC*, No. 2:17-CV-00428-JNP, 2017 WL 8947964, at *1 (D. Utah June 29, 2017) (defendants “had a high level of computer technical proficiency, and there had been attempts by the defendants in the past to delete information from computers, including emails and other data.”).

Ex Parte Seizures

- Practical Tips

- Educate the court and law enforcement
- Submit detailed proposed order, and include catchall provision and deadline
- Ensure the proper secure storage of the assets, possibly proposing use of a third-party custodian
- Anticipate real-time execution problems
- Identify and educate a neutral technical expert

DTSA Damages

- Damages remedies available under the DTSA are similar to those under the Uniform Trade Secrets Act, or UTSA.
 - Economic remedies include: (1) damages for actual loss caused by the misappropriation of the trade secret; and (2) damages for any unjust enrichment caused by the misappropriation of the trade secret that is not addressed in computing damages for actual loss; or (3) in lieu of damages measured by any other methods, the damages caused by the misappropriation measured by imposition of liability for a reasonable royalty for the misappropriator's unauthorized disclosure or use of the trade secret.
- A small number of cases have damages awards under the DTSA. In five of these cases, damages were awarded on default judgment. Most are mixed lump sum damages or attorneys' fees and costs.
 - *Solarcity Corporation v. Girma*—court awarded \$61,360 actual damages as well as \$122,720 treble damages for willfulness. In two cases, defendants received attorneys' fees and costs for successfully defending trade secret claims.
 - *Steves and Sons, Inc. v. Jeld-Wen, Inc.*—jury awarded \$1.2 million each for state and DTSA trade secret misappropriation claims, totally \$2.4 million in Trade Secret damages.
 - *Dalmatia Import Group, Inc. v. Foodmatch Inc. et al.*—jury awarded \$500,000 in damages as one award under both state law and the DTSA.

17

ROPES & GRAY

DTSA Appeals

- Very few appellate decisions to date:
 - *First Western Capital Management, Co. v. Malamed*—Lawsuit under both the DTSA and the Colorado trade secrets law against a former employee accused of stealing customer lists. The Tenth Circuit reversed the district court's grant of a preliminary injunction to First Western, holding that a violation of the DTSA does not create a presumption of irreparable harm.
 - *Fres-co Systems USA Inc. v. Hawkins*, Lawsuit under both the DTSA and Pennsylvania law against an employee accused of stealing confidential information (such as customer lists and long-term strategies). The Third Circuit, in an unpublished decision, remanded the preliminary injunction to the district court for further analysis, explaining that showing irreparable harm for purposes of a DTSA suit can be satisfied even by a threat of misappropriation but that the likelihood of success showing requires proof that the supposedly confidential information fell within the DTSA.
 - Two Ninth Circuit opinions in federal criminal cases briefly mentioned the DTSA, noting that the DTSA had changed the definition of a trade secret for both criminal and civil purposes but declining to apply the new definition because the events of the case predated the DTSA's 2016 enactment.

18

ROPES & GRAY

EU Directive on Trade Secrets

- EU's first such directive to create unified approach to trade secrets, adopted in 2016
- Creates baseline minimum level of protection which each member state was required to implement in its national laws by June 2018
 - Uniform definition of a trade secret
 - Trade secret must be subject to reasonable protection measures (intent to keep secret no longer sufficient)
 - Reverse engineering generally allowed
 - Employees have more freedom to bring knowledge and experience to their next employer
- Differences from DTSA:
 - No new procedural tools in the EU Directive; no ex parte seizures
 - No provision for enhanced damages for willful/malicious misappropriation in the EU Directive
 - EU Directive contains broader¹⁹ protection for whistleblowers than the DTSA

ROPES & GRAY

Trade Secret Litigation in the ITC

- The International Trade Commission is an independent, quasi-judicial agency tasked with enforcing Section 337 of the Tariff Act, 19 U.S.C. § 1337
- Trade statute protecting U.S. industries from injuries caused by unfair acts in the importation of goods to the United States
- The litigation of trade secrets at the ITC is a relatively recent phenomenon, spurred by *TianRui Group Co. v. Int'l Trade Comm'n*, 661 F.3d 1322 (Fed. Cir. 2011), which held that a misappropriation occurring abroad could be remedied by an exclusion order on any importation of goods resulting from the misappropriation:
 - Cast steel railway wheels made in China, using trade secret process misappropriated in China
 - Extraterritoriality: The ITC may reach imports that relate to trade secret theft that occurred outside the United States. *Id.* at 1329.
 - Choice of law: A “single federal standard” governs misappropriation as an “unfair act” under Section 337—not state or foreign law. *Id.* at 1327.
 - Domestic industry injured by misappropriation²⁰ and importation need not use the trade secret domestically. *Id.* at 1335.

ROPES & GRAY

Trade Secret Litigation in the ITC

- *Manitowoc Cranes LLC v. Sany America Inc. and Sany Heavy Industry Co., Ltd.*, No. 1:13-cv-00677 (E.D. Wisc. Dec. 11, 2017)
 - The Eastern District of Wisconsin found that defendants were precluded from re-litigating in the district court claims of trade secret misappropriation brought by plaintiff previously at the ITC.
 - Plaintiff had filed a Section 337 complaint in the ITC alleging trade secret misappropriation against defendants
 - ALJ issued an initial determination finding that defendants misappropriated trade secrets
 - Finding was subsequently upheld by the Commission and Federal Circuit.
 - Following the Federal Circuit's affirmance, the co-pending Eastern District of Wisconsin action, which had been stayed pending the ITC Investigation, had been reopened.

21

ROPES & GRAY

Trade Secret Litigation in the ITC

- Advantages of the ITC
 - Speed
 - Powerful, self-enforcing exclusionary remedy
 - In rem jurisdiction (no personal jurisdiction required)
 - Extraterritorial concerns may be minimized
 - Broad subpoena power
 - Flexible evidentiary rules
 - Sophisticated staff, including ALJs
 - Detailed factual record and opinions
 - No black box jury verdicts
 - Can help with appeals
 - Efficiencies for parallel litigation (domestic and foreign venues having range of remedies)
 - Independence

ROPES & GRAY

Trade Secret Litigation in the ITC

- Disadvantages of the ITC
 - Speed
 - Expensive
 - No damages
 - But fines are available for violations of exclusion orders
 - Requires substantial up-front work and diligence
 - ITC must consider public interest
 - Potential for presidential disapproval
 - Uncertainty for untested Section 337 theories

ROPES & GRAY

Other Emerging Issues Post-DTSA

- Other Emerging Issues
 - Reconciling competing standards
 - Does California's rule regarding identifying trade secrets with specificity before discovery apply to federal DTSA actions?
 - Trade secret cases involving emerging technologies like blockchain, CRISPR, and AI

24

ROPES & GRAY

SECTION 5

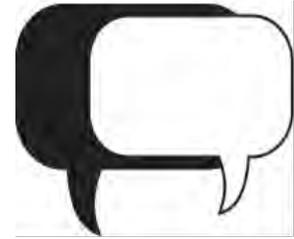
Advertising Law Update



Presented by

Laura Brett

Director, National Advertising Division
Advertising Self-Regulation Council
Washington, DC



Digital Marketing Digest

The Advertising Industry's Self-Regulatory System monitors advertising in all media, including digital marketing, to assure that advertising claims are truthful, accurate and not misleading. The self-regulatory system is a service of the advertising industry and the Council of Better Business Bureaus (CBBB).

Although compliance with self-regulatory decisions is voluntary, the self-regulatory system enjoys a high rate of compliance with its decisions – more than 90 percent of companies that appear before one of the self-regulatory units agree to abide by the terms of decisions that require advertising to be modified or discontinued.

The Advertising Self-Regulatory Council (ASRC) is the governing body for advertising industry self-regulation. ASRC's 11-member Board of Directors is comprised of the top leadership of the American Advertising Federation (AAF), American Association of Advertising Agencies (AAAA), Association of National Advertisers (ANA), CBBB, Direct Marketing Association (DMA), Electronic Retailing Association (ERA) and Interactive Advertising Bureau (IAB).

The Self-Regulatory Programs:

- **NAD** – The National Advertising Division (NAD) monitors national advertising in all media, enforcing high standards of truth and accuracy. NAD examines advertising claims made for goods and services as diverse and critical as telecommunications, infant nutrition, over-the-counter medications and dietary supplements and “green” products. NAD accepts complaints from consumers, competing advertisers and local Better Business Bureaus. NAD's decisions represent the single largest body of advertising decisions in the U.S. In addition to its own monitoring, NAD provides a fast, expert forum for the resolution of competitors' disputes. NAD handles about 150 cases each year and publicly reports its formal decisions.

Advertising Self-Regulatory Council • 112 Madison Avenue, 3rd Fl. • New York, NY • 10016 •

www.asrcreviews.org

©2018 Council of Better Business Bureaus. NAD®, CARU® and ERSP® are trademarks of the Council of Better Business Bureaus.

- Accountability Program – The Online Interest-Based Advertising Accountability Program charged with ensuring industry compliance with the Self-Regulatory Principles for Online Behavioral Advertising (Principles). The Principles require third parties to provide consumers with an easy-to-use mechanism that allows the consumer to exercise choice regarding the collection and use of data from their device for online behavioral advertising (OBA) purposes.
- CARU – Recognizing the special vulnerability of young children, the Children's Advertising Review Unit holds advertisers to high standard of truth and appropriateness when they direct advertising to young children. Among other things, CARU's guidelines provide that advertisers cannot state or imply that their products will make children more popular with their peers, advertise vitamins or other products that carry "keep out of reach of children" labels, or advertise products that are unsafe for young children to use. CARU examines advertising in all media, including electronic media, and monitors Websites and online services such as apps to assure that they are compliant with CARU's guidelines and the Children's Online Privacy Protection Act (COPPA).
- ERSP – Developed with the Electronic Retailing Association, the Electronic Retailing Self-Regulation Program (ERSP) examines the truth and accuracy of core claims made in electronic direct-response advertising. ERSP monitors the \$170 billion direct-response marketplace, providing a strong self-regulatory presence on the frontier of electronic commerce.

ASRC programs are funded through a variety of sources — membership dues to the CBBB make up a substantial portion. The remainder is provided through the support of industry associations (ERA, CRN, Digital Advertising Alliance), the direct support of children's advertisers and child-directed media and revenue from the sale of products and services.

National Advertising Division

Epson America, Inc.
3LCD Projectors
Case #6183 (5.01.18)

NAD recommended that the advertiser modify two websites, 3lcd.com and colorlightoutput.com, which it used to explain information about 3LCD technology to disclose Epson's connection to the website at the top of the landing page, as well as on each page within the website, so that the disclosure is easy to notice, read and understand. The challenger asserted that the material connection between the advertiser and these websites was not clearly and conspicuously disclosed. NAD determined that the disclosures were not clear and conspicuous because appeared in small font on busy webpages that feature colorful images and large text headlines. In addition, the disclosures appeared at the bottom of each webpage and require consumers to scroll to the bottom of long webpages in order to view them.

Epson agreed to comply with NAD's recommendation.

Carma Laboratories, Inc.
Carmex Cold Sore Treatment
Case #6182 (4.27.18)

After the commencement of this challenge, the advertiser agreed to permanently discontinue certain challenged claims in its digital advertising. These included claims in social media posts which the challenger alleged were express or implied claims with a reasonable takeaway that Carmex Cold Sore Treatment speeds healing, shortens symptom duration, prevents cold sores, or stops progression of the virus. Additionally, the advertiser agreed to discontinue its use of testimonials and reviews on its website, retailer websites, and via social media, making claims about Carmex Cold Sore treatment that were not supported and modify any incentivized reviews to disclose the existence of a material connection between the reviewer and Carma Labs. Finally, the advertiser also agreed to permanently discontinue the claim that Carmex Cold Sore Treatment was "improved." In reliance on the advertiser's representations, NAD did not review these claims (or the alleged implied claims stemming therefrom) on their merits. The voluntarily discontinued and modified claims will be treated, for compliance purposes, as though NAD recommended their discontinuance or modification and the advertiser agreed to comply.

Shell Oil Company
Shell V-Power NiTRO+ Premium Gasoline
Case # 6065 (3.16.17)

NAD recommended that Shell Oil Company discontinue the use of a video in its advertising because the video did not disclose the material connection between the maker of the video and Shell. The YouTube channel, "Engineering Explained," featured the host walking viewers through Shell's claims for SVPN+ and the underlying testing. The host was not a Shell employee, Shell did not produce or have editorial rights over the video, and the video was not paid advertising. The host did not receive any fees or honorarium, but Shell covered his travel to its facilities as part of the featured event. However, NAD determined that this potentially significant financial connection between Shell and the host required disclosure, as it could impact the weight that consumers give to the statements made about the benefits of SVPN+.

Shell appealed the NAD's recommendation to the NARB.

The NARB (#221 – 11.14.17) recommended that Shell modify the Fenske "Engineering Explained" video appearing on Shell's website and in any Shell advertising to clearly and conspicuously disclose in the video itself any material connection – including payments made by Shell to Mr. Fenske for travel expenses or for other reasons – between Shell and Mr. Fenske.

The advertiser agreed to comply with the NARB decision.

Beauty Science Group, Inc.
Hair La Vie
Case # 6055 (2.21.17)

NAD recommended that Beauty Science Group, Inc. advise ConsumersSurvey.org that they cannot make unsupported claims, including through the use of testimonials, that the advertiser cannot itself substantiate and that the advertiser must clearly and conspicuously disclose the relationship between itself and ConsumersSurvey.org in order to be effective. Beauty Science Group has an affiliate marketing relationship with ConsumerSurvey.org. ConsumerSurvey.org has two webpages which feature Hair La Vie. Consumers are likely to weigh ConsumersSurvey.org's recommendation of Hair La Vie differently if consumers have knowledge that ConsumerSurvey.org receives compensation for purchases of Hair La Vie from its website. Also, paid endorsements may not convey any express or implied claims that would be misleading if made directly by the advertiser. Because Beauty Science Group failed to support its claims that Hair La Vie grows thicker, stronger, or fuller hair, ConsumersSurvey.org could not make the unsupported claims.

Beauty Science Group agreed to comply with NAD's recommendations.

Kardashian, Kourtney, et. al.
FitTea
Case # 6046 (1.18.17)

Kourtney Kardashian, Khloe Kardashian and Kylie Jenner agreed to modify their social media posts about FitTea to disclose that they were being paid to endorse the product. NAD raised concerns that the Kardashians failed to disclose in any way their material connection to FitTea, a connection that consumers would not expect when viewing their social media posts about the product. When a social media post expresses a personal opinion about how much a poster likes a product or how frequently the poster uses a product, consumers might not understand whether the post is a paid endorsement or the post is spontaneous, without any payment or other compensation being exchanged. Consumers are likely to weigh an opinion differently if it is a paid endorsement for a product. As a result, such a payment is a connection that is material to consumers and should be disclosed. NAD did not review this matter on its merits. The voluntarily modified advertising will be treated, for compliance purposes, as though NAD recommended its modification and the advertisers agreed to comply.

The advertiser declined to submit an Advertiser's Statement after voluntarily modifying their advertising.

Reckitt Benckiser LLC
Finish® Automatic Dishwasher Detergent
Case # 6043 (1.4.17)

To the extent that Reckitt Benckiser LLC provides incentives to dishwasher manufacturers for their recommendations or endorsements of its products, NAD determined that it should disclose this connection when it advertises that it is the "#1 World's Recommended Brand."

RB appealed this finding in NAD's decision. The NARB affirmed NAD's decision.

Fit Products, LLC
FitTea
Case # 6042 (12.28.16)

NAD appreciated Fit Products' voluntary modifications to social media posts republished on Fit Products' website. NAD will treat these modifications, for compliance purposes, as though NAD recommended their discontinuance and the advertiser agreed to comply.

NAD recommended that Fit Products, LLC discontinue posting customer testimonials that made the claims Fit Products agreed to permanently discontinue or that NAD recommended should be discontinued. NAD cautioned Fit Products that it should insure

that its paid endorsers avoid conveying messages for which it lacked support. Finally, NAD advised Fit Products to separate its endorsements and testimonials from its product reviews as well as to prominently disclose that the reviews on its website are authentic user reviews and that Fit Products does not edit those reviews.

Fit Products agreed to comply with NAD's recommendations.

BA Sports Nutrition, LLC
Body Armor SuperDrink
Case # 6026 (11.21.16)

NAD recommended that BA Sports Nutrition, LLC discontinue reposting or linking to content on its social media pages that conveys the message that BodyArmor is "all natural" or that falsely denigrates Gatorade as "junk." When an advertiser reposts or links to third party content on its own social media pages, it is using that content as advertising and is thus responsible for the truthfulness and accuracy of the messages reasonably conveyed by the content it links to or re-posts.

BA Sports Nutrition agreed to comply with NAD's recommendations.

Goop, Inc.
Moon Juice Action Dust and Brain Dust Dietary Supplements
Case # 5977 (7.16.16)

Goop elected to permanently discontinue advertising claims for its Moon Juice Action Dust and Brain Dust dietary supplements challenged by the National Advertising Division. Goop is an online lifestyle publication founded by celebrity Gwyneth Paltrow. The dietary supplements at issue were featured in Goop's online store together with an apparent endorsement by Ms. Paltrow. The product efficacy claims and the endorsement imposed an obligation on Goop to verify that the products provided the benefits claimed. The obligation to insure that advertising claims are truthful extend to third-party or affiliate entities who "persuad[e] the audience of the value or usefulness of a . . . product" engage in "national advertising." Because Goop discontinued the advertising, NAD did not review these claims on their merits. The voluntarily discontinued claims will be treated, for compliance purposes, as though NAD recommended their discontinuance and the advertiser agreed to comply.

Goop accepted the decision of the NAD and voluntarily and permanently discontinued the advertising.

Vestagen Technical Textiles, Inc.

Vestex Fabric
Case # 5972 (7.13.16)

NAD recommended that articles cited by Vestagen as evidence of the need for apparel made from its Vestex material appearing on its website, in advertising and sales materials or on its blog that were authored by current or former Vestagen employees clearly and conspicuously disclose the material connection to the advertiser and/or be labeled as advertising.

Vapore, LLC
MyPurMist Handheld Steam Inhaler
Case # 5971 (7.12.16)

NAD recommended that Vapore discontinue the claim that its MyPurMist Handheld Steam Inhaler received "More 5-star reviews than any other steam inhaler." Where the 5-star reviews were verified, this does not guard against the potential for double-counting of reviews, which undermines the reliability of the reviews. In addition, certain reviews were too dated to be considered sufficiently reliable. Further, star ratings do not indicate why the rating was given, and they may have been given for reasons other than the attributes mentioned in the commercial. However, NAD noted that nothing in this decision precluded Vapore from making a more qualified claim about its product being highly-rated.

NAD also determined that the disclaimer relating to the material connection between the Dr. Berger and Vapore was clearly and conspicuously disclosed in the television commercial. However, NAD recommended that the version of this disclaimer, which appears in a YouTube video of a doctor's testimonial, be modified to refer to MyPurMist instead of Vapore and that the reference to MyPurMist be easier to read, notice and understand.

Vapore agreed to comply with NAD's recommendations.

Jumpsport, Inc.
Trampolines
Case # 5970 (7.11.16)

A purportedly third-party review site for trampolines that was actually owned and operated by trampoline manufacturer JumpSport, Inc. was misleading and should be discontinued, according to the National Advertising Division in a challenge by competitor Vuly Trampolines Pty. Ltd. Product reviews generated by an advertiser must be clearly identified and not in a format that makes them appear to be independent editorial content. www.TrampolineSafety.com appeared to be operated by an independent third party, but is owned, operated, and controlled by JumpSport. The reviews and ratings were established by JumpSport. The advertising format was

inherently misleading to consumers. Even if a disclosure could cure this false impression, as argued by JumpSport, the disclosures on the website were not clear and conspicuous.

JumpSport agreed to comply with NAD's recommendations.

Joyus, Inc.

Dr. Brandt's Needles No More Wrinkle Relaxing Cream

Case # 5956 (5.19.16)

NAD recommended that Joyus, an online shopping retailer, disclose that its "Stuff We Love" page was advertising and not editorial content. Joyus is an e-commerce platform for lifestyle products. Joyous brings consumers online shopping using videos to showcase new products. NAD was concerned that advertising for Joyus products appeared in a format that made it look like the advertising was editorial content. The FTC has advised that advertising should be identifiable as advertising to avoid misleading consumers into believing that an advertisement is independent and impartial. Consumers did not know that "Stuff We Love" was promoting products for sale in the videos before watching the shopping video. As a result, consumers could give greater credence to claims made in the product descriptions than they would if they were aware that this is a form of advertising for those products, and further, consumers may interact with this content because they think it is editorial and not advertising. NAD therefore recommended that Joyus (in collaboration with People Magazine) revise the link so that it is clear that by clicking on the "Stuff We Love" link, consumer will be taken to a list of items for sale by Joyus. The link itself or text surrounding the link should advise consumers that the content to which consumers are linking is an advertisement or make clear that the links are "shopping" links.

Joyus, Inc. voluntarily discontinued advertising claims for Dr. Brandt's Needles No More Wrinkle Relaxing Cream, which the National Advertising Division treated as though NAD recommended their discontinuance and the advertiser agreed to comply. NAD asked Joyus to substantiate claims about the efficacy of the advertised product. The claims were discontinued by Joyus after the commencement of this challenge.

Joyus agreed to comply with NAD's recommendations.

KLF International, Inc.

Venus Factor Weight Loss System for Women

Case # 5938 (3.15.16)

KLF International, Inc. voluntarily and permanently discontinued advertising for its Venus Factor Weight Loss System for Women on its website and in promotional videos after the National Advertising Division opened a review of certain express claims. KLF explained that some of the challenged claims were not made by KLF but were made by affiliates. It further explained it takes it takes several steps to insure that advertising by its affiliates

for Venus Factor is truthful and accurate. NAD appreciated the efforts taken by KLF to insure that marketing by its affiliates is truthful, accurate and not misleading. NAD did not review the claims on their merits, and the voluntarily discontinued claims will be treated as though NAD recommended their discontinuance.

KLF agreed with NAD's analysis and appreciated NAD's efforts to ensure fair and truthful advertising in the fitness industry.

SharkNinja Operating LLC
Shark Rocket DeluxePro
Case # 5929 (2.11.16)

NAD recommended that Shark clearly and conspicuously disclose the material connection between itself and consumers in its advertising. The consumers in the commercial signed up for a product testing program in which they are provided with Shark vacuums and contacted weekly to discuss their experiences with the vacuum. The consumers were not told that they can keep the vacuum or that they will receive anything of value in exchange for a positive review. Some consumers were then asked if they would be willing to allow filming of a test with their vacuum, but were not told that they would appear in a television advertisement. NAD questioned whether the use of a product for free, even when it is borrowed, might materially affect the weight or credibility of an endorsement because a purchasing decision generally involves weighing costs and benefits of one product as compared to another. NAD was also concerned that the multiple interactions between the company and the consumer was a connection that a reasonable consumer would not reasonably anticipate when viewing an infomercial proclaiming "real people, real results."

SharkNinja agreed to comply with NAD's recommendations in its future advertising.

New WinCup Holdings, Inc.
Vio Cups
Case # 5902 (11.9.15)

NAD appreciated that WinCup removed its Facebook post which included a "biodegradable" claim without any qualifying language. This was necessary to meet FTC regulations requiring that biodegradability claims be qualified where the product will not decompose within one year after customary disposal. Further, unless WinCup is capable of properly qualifying its biodegradability claims on Twitter, NAD recommended that it refrain from making biodegradability claims on this platform. With regard to WinCup's Vio video on YouTube, NAD recommended that the qualification in the description box be moved in immediate proximity to the heading "Vio™ Biodegradable* Foam Cups," and that the font size be increased to a size that is more easily visible. With regard to the Vio video itself, NAD determined that the qualifications for WinCup's biodegradability claims were sufficiently clear and prominent.

The Scotts Company, LLC
Ortho Home Defense, Ortho Bug-B-Gon, Ortho Weed-B-Gon
Case # 5889 (10.5.15)

NAD appreciated Scotts' voluntary discontinuance of the challenged commercials, and the claims therein. In reliance on the advertiser's representation that these claims have been permanently discontinued, NAD did not review these claims on their merits. The voluntarily discontinued claims will be treated, for compliance purposes, as though NAD recommended their discontinuance and the advertiser agreed to comply.

NAD was satisfied that Scotts took sufficient and proper remedial steps upon learning that its customer reviews were written and posted without the required disclosure indicating they were incentivized. A sweepstakes to win a \$25 Visa gift card was run by Scotts as an incentive for consumers to review Scotts products, thus providing a level of engagement and a connection between the consumers and the advertiser that was not expected and must be disclosed. Once Scotts became aware that consumers were not including the proper disclosure as part of their sweepstakes entry, it took several remedial steps in order to address the possible misimpression that a positive entry was unincentivized.

Scotts was pleased that the NAD has agreed that Scotts took sufficient and proper action in connection with reviews generated pursuant to a sweepstakes and accepted NAD's decision to consider the spots and challenged claims presented therein "discontinued" in light of a lack of evidence in the record and not based on a determination regarding the merits of the challenge.

Euro-Pro Operating, LLC
Shark Rotator Powered Lift-Away NV650 Vacuum
Case # 5860 (7.6.15)

Reviews relied upon by lacked important indicia of reliability and representativeness to provide a reasonable basis to support its broad "More 5-Star Ratings online than any other vacuum brand" claim. Dyson, Inc. challenged Euro-Pro's advertising claim that its Shark Rotator Powered Lift-Away NV650 vacuum received "More 5-Star Online Ratings." The "online ratings" claim reasonably conveyed the message that Euro-Pro conducted an extensive compilation of reliable and representative "5-Star" online-wide reviews in support of its claim. Euro-Pro gathered 5-star review data from online retailer websites comprising the top 85% of online retailers. The websites that were subject to Euro-Pro's analysis did not have consistent policies as to how long consumer reviews were displayed, which meant that some may have been more heavily weighted towards the review of outdated models. Such inconsistencies and uncertainties were particularly problematic when attempting to combine reviews from various sources to support a single, broad superiority claim. Even if NAD accepted Euro-Pro's tally of reviews for the

seven sites considered in support of its claim, NAD questioned the reasonableness of selection of a \$149.99 price point (or above) for its calculation of 5-star reviews. This unnecessarily narrowed the limited data upon which Euro-Pro based its claim.

Euro Pro agreed to **take NAD's findings into consideration** in its future advertising and supports the self-regulatory process.

Pursuit of Research, LLC
Nutriveda Dietary Supplement
Case # 5725 (6.16.2014)

Pursuit of Research, LLC was required to properly disclose the association between it and a website that directly or indirectly promoted Pursuit of Research's dietary supplement. Pursuit of Research maintained "The Cherub Foundation" website, which hosts a blog and forums where parents can lend support and offer information with each other regarding their children's pressing health and neurological issues. NourishLife, LLC argued that the Cherub Foundation, which links to the Pursuit of Research, was used to sell Nutriveda without disclosing its close ties to the Pursuit of Research. NAD recommended that Pursuit of Research clearly and conspicuously disclose on the Cherub Foundation website and on the Cherub Foundation blog post the material connection between the Cherub Foundation and the Nutriveda product that is promoted in a manner that is easy to notice, read and understand.

Pursuit of Research **agreed to comply with NAD's recommendations.**

General Mills, Inc.
Yoplait Blended Greek Yogurt
Case # 5715 (5.19.14)

NAD determined that General Mills could support certain claims made for its Yoplait "Greek" yogurt in online advertising and social media, but recommended the advertiser discontinue or modify other claims. The claims at issue were challenged by Chobani, Inc. and included, "The Greek Yogurt Taste-Off is on: Yoplait Greek Is Significantly Preferred over Chobani;" "People agree Yoplait Greek Blueberry tastes better than Chobani Blueberry with fruit on the bottom.* *Based on a nationwide, double-blinded taste test of Yoplait Greek Blueberry yogurt and Chobani Blueberry Fruit on the Bottom Yogurt;" and "In a national taste test, nearly 2 out of 3 Americans agree that Yoplait Greek tastes better than Chobani."

NAD reviewed both the reliability of a taste test comparing Yoplait Greek blueberry flavor to Chobani blueberry fruit on the bottom, as well as the advertising campaigns surrounding the taste test results. NAD determined that the taste test between the two brands' blueberry flavored yogurt was reliable and supported certain versions of the advertiser's claims about consumers' preferences of blueberry flavored yogurt. However,

the advertiser taste preference claims concerning blueberry-flavored yogurt appeared alongside user generated content in social media, including Twitter, Facebook and Tumblr that it encouraged consumers to share. NAD considered whether, in this context, the claims conveyed a broader taste preference message than was supported by the taste test results. NAD recommended that in future advertising the advertiser more clearly **separate its claims about Yoplait's taste test results on Yoplait Greek blueberry and Chobani blueberry fruit on the bottom from the comments it has solicited on taste preferences.**

Finally, NAD recommended that when the advertiser offers incentives for product reviews, it advise reviewers of their disclosure obligations, and – to the extent that General Mills is aware of a material connection – it discontinue re-posting reviews on social media or modify such re-postings to clearly and conspicuously disclose any material connection between the reviewer and General Mills.

Taboola, Inc.
Online Advertising
Case # 5708 (5.5.14)

NAD recommended that Taboola clearly disclose that it was linking consumers to sponsored content rather than news stories. Congoo, LLC, an Internet-based advertising company, challenged the practices of competitor Taboola with respect to the way it displayed image-plus-text ad units. Taboola and its competitors purchase advertising space from a variety of online publishers on behalf of clients. Congoo argued that **Taboola's ad units were so vaguely labeled as to confuse consumers into believing they were going to be linked to editorial content when they were actually directed to an advertisement.** NAD recommended that Taboola modify its disclosures to disclose that it was linking consumers to sponsored content.

While Taboola strongly believed that its current disclosure methods were best-in-class and far surpass what other recommendation platforms are using, Taboola agreed to modify the appearance of its disclosures in future iterations of its widget, as recommended by NAD.

American Media, Inc.
Shape Water Boosters
Case # 5665 (12.18.13)

NAD recommended that American Media clearly and conspicuously designate content as advertising when it advertises its SHAPE-branded products in its SHAPE magazine. In an article that appeared to be an editorial about the health value of hydration was an advertisement for Shape Water Boosters. NAD was concerned that consumers may give **more credence to the advertiser's objective claims about the product's attributes** because of the context in which the claims appeared. American Media argued that

because consumers were aware of the connection between the magazine and the SHAPE-branded product, it has no obligation to disclose that its promotion of SHAPE-Branded products was advertising. There was also an editor's note on page 32 of the magazine that disclosed the connection between SHAPE Magazine and SHAPE Water Boosters. Although consumers may be aware that SHAPE Water Boosters were related to SHAPE magazine, those same consumers can reasonably attach different weight to recommendations made in an editorial context than recommendations made in an advertising context. Consumers may reasonably believe that editorial recommendations in SHAPE magazine are independent of the influence of a sponsoring advertiser. Thus, the NAD recommended that American Media clearly and conspicuously designate content as advertising when it promotes SHAPE-branded products.

American Media agreed to modify the format in which it promotes its branded products.

Nutrisystem (Pinterest)

“Real Consumers. Real Success.”

Case # 5479 (6.29.12)

NAD, following its review of “Real Consumers. Real Success.” – a Pinterest board maintained by Nutrisystem, Inc. – determined that the weight-loss success stories “pinned” to such boards represent consumer testimonials and require the complete disclosure of material information. NAD noted its appreciation that Nutrisystem took immediate steps to provide such disclosures.

Nutrisystem's “Real Consumers” pinboard featured photos of “real” NutriSystem customers and highlighted their weight-loss successes. The customer's name, total weight loss and a link to the NutriSystem website appeared below each photo.

Claims at issue in NAD's review included:

- “Christine B. lost 46lbs on Nutrisystem.”
- “Michael H. lost 125 lbs. on Nutrisystem.”
- “Lisa M. lost 115 lbs. on Nutrisystem.”
- “Christine H. lost 223 lbs. on Nutrisystem.”

Upon receipt of NAD's inquiry, the company asserted that necessary disclosures were inadvertently omitted from Pinterest. The advertiser stated that the testimonials at issue had appeared on Pinterest for less than two months, and said the disclosures were added immediately upon receipt of NAD's letter.

CHIPOTLE MEXICAN GRILL (YouTube)

Chipotle Restaurants

Case # 5450 (4.18.12)

NAD determined that Chipotle Mexican Grill could support implied claims made in an animated feature, “Back to the Start,” that all animals which provide the meat for Chipotle products are naturally raised.

The advertising at issue appeared on the YouTube website, online at Chipotle.com, on Chipotle’s Facebook page, in movie theaters in advance of feature films, and on television. It uses stop-motion animation to depict a farmer’s journey to sustainable farming.

NAD requested that the advertiser provide substantiation for two implied messages:

- *Chipotle’s goal is to exclusively use “naturally-raised” meat in its restaurants*
- *Chipotle has already achieved this goal and all of the animals which provide the meat (pork, chicken and beef) for Chipotle products are, in fact, “naturally-raised.”*

The video – a first for Chipotle – was directed by London-based John Kelly and featured a cover of the Coldplay song “The Scientist,” sung by music icon and family farm advocate Willie Nelson.

Following its review of the evidence in the record, NAD found that the advertiser provided a reasonable basis for the two messages implied in the “Back to the Start” film – both its aspirational message and the message that all of the animals which provide the meat for Chipotle are, in fact, “naturally-raised” according to Chipotle’s own definition of the term.

However, NAD cautioned the advertiser that, although its implied messages are currently substantiated, to the extent that supply constraints result in shortages of “naturally-raised” meats in particular markets, future advertising may need to disclose this fact.”

Coastal Contact, Inc. (Facebook)
Like-Gated Ad Campaign
Case #5387 (10.25.11)

In a case of first impression, NAD determined that the display of the total number of “likes” on the Facebook page of Coastal Contacts, Inc., conveys a general social endorsement.

NAD determined that the display of Facebook “likes” on a company’s Facebook fan page can mean many things to consumers, including that consumers like the company, product or service, that the individual who “liked” the content entered a like-gated promotion contest or sweepstakes, or that the consumer wanted to share some content on the company’s page with their “friends.”

Because actual consumers “liked” the Coastal page, and those consumers who participated in the like-gated promotion received the benefit of the promotion, NAD determined that Coastal had the general social endorsement that the “likes” convey. NAD noted for the record, however, that the outcome of the case would have been quite different if the evidence in the record demonstrated that consumers who participated in the like-gated promotion could not or did not receive the benefit of the offer, or that the advertiser used misleading or artificial means to inflate the number of Facebook “likes.”

With respect to the statements made in press releases to the investor community, NAD recommended that Coastal clarify that the number of Facebook “fans” or “likes” noted in the press releases is based on the total number of “fans” or “likes” the Company has received from all of its Facebook pages globally.

NAD further recommended that Coastal Contacts, Inc., discontinue an “up to 70 percent” savings claims and modify advertising that promoted “free” products.

LALA-USA, Inc. (YouTube)
La Crème Real Dairy Creamer
Case #5359 (08.08.11)

This case involved in part a series of “Cow Tip” vignettes that claimed competing non-dairy creamers contained ingredients also found in paint, glue, shampoo and shaving cream, and that some non-dairy creamers are flammable and contain trans fat. The vignettes were also linked to YouTube videos where non-dairy creamers were shown as a replacement for glue or paint. During the course of NAD’s review, the advertiser said it would permanently discontinue the challenged vignettes and claims, an action that NAD found necessary and proper.

NAD determined that the challenged advertisements did not convey an implied all-natural claim and concluded that the advertiser could support the claims “100% Dairy” and “Real Dairy.”

Bridgestone Golf, Inc.
Golf Ball Fitting
Case #5357 (08.02.11)

Bridgestone argued that its name on Twitter is not advertising. Section 1.1(A) of the *NAD/NARB Procedures* states that the term “national advertising” includes commercial

messages “in any medium...if it has the purpose of inducing a sale or other commercial transaction or persuading the audience of the value or usefulness of a company, product or service . . . and if the content is controlled by the advertiser.” “In any medium” clearly encompasses social media sites. Twitter is an information network where anyone can read, write and share messages of up to 140 characters. These messages, or Tweets, are public and available to anyone interested in them. Twitter users subscribe to an advertiser’s messages by following its account. Subscribers receive them in a feed of all the accounts to which they have subscribed. Further, NAD has previously considered other social media claims that have appeared on YouTube and Facebook and determined that when claims are controlled or disseminated by the advertiser they may be considered national advertising.

With regard to the advertiser’s Twitter account, one of the names the advertiser reserved was “1BallFitter.” It is common Twitter practice when categorizing and organizing Tweets or searching for other Tweets about a particular topic that Twitter users will place a hash tag (“#”) in front of the topic heading. NAD determined that when Twitter users use the “#1BallFitter” to Tweet about or find Tweets about the advertiser’s golf ball fittings, they understand the meaning of the “#” symbol to be a “Number 1” claim, particularly since “1Ballfitter” standing alone is confusing at best and literally (i.e., that the advertiser has only one ball fitter) not the message the advertiser wishes to convey.

Consequently, NAD determined that it has jurisdiction to consider claims made on Twitter because they constitute “national advertising” within the meaning of NAD Procedure § 1.1(A).

Children’s Advertising Review Unit

Cartoon Doll Emporium
www.CartoonDollEmporium.com
Case #5743 (7.17.14)

CartoonDollEmporium.com was described as a safe, carefully moderated gaming website and social network where children can play games, make friends, upload photos, enter contests, invite friends, create avatars, and purchase and acquire virtual goods.

Upon review, CARU found that the site: employed an age-screening process that allowed visitors to go back the original registration screen and change their ages, circumventing certain privacy protections; did not include a link to its privacy policy or inform the parent or guardian that personally identifiable information (PII), including full names and street addresses, could be shared by children in its direct notice to parents or guardian, allowed children to disclose PII without first obtaining parental consent, allowed children to upload photos of themselves and attach captions that included PII

without first obtaining parental consent; contained advertisements for products that were rated for mature audiences; did not obtain parental consent before allowing third parties to collect information that was then used to recognize users over time and across different websites for advertising purposes.

CARU recommended that the operator modify its privacy practices to bring the site into compliance with CARU's guidelines and the federal Children's Online Privacy Protection Act (COPPA), which the company agreed to do. The company, in its advertiser's statement, said that it has "reviewed the case decision and accepts CARU's decision in its entirety and has already made all of the changes recommended by CARU.

SPIL Games, BV
Girlgogames.com
Case #5533 (1.9.13)

CARU recommended that the SPIL Games, NV, operator of the website, girlgogames.com, modify its site to better protect the privacy of child visitors. The company agreed to do so.

CARU was concerned that the website, which allows members to create profiles, view profiles of others, allowed children under 13 to disclose personally identifiable information without first providing parental notice or obtaining parental consent. CARU was also concerned that the site invited children to register for the site using social media tools, such as Facebook and Twitter, which do not permit participation by children under age 13.

The operator agreed to make the changes recommended by CARU, including the disabling of its feature that allowed log-in through social media and removed links to Twitter.

Electronic Retailing Self-Regulation Program (ERSP)

CONSUMERAFFAIRS.COM, INC.
ConsumerAffairs.com
Case #353 (9/4/2014)

ERSP reviewed online advertising claims for ConsumerAffairs, including:

- "Consumer Affairs is a consumer news and advocacy organization founded in 1998 by James R. Hood, a veteran Washington, D.C. journalist and public affairs executive. Our website includes consumer news, recall information and tens of thousands of pages of consumer reviews."
- "ConsumerAffairs.com is a private, non-governmental entity that empowers consumers by providing a forum for their reviews."

The challenger also expressed concerns regarding the filtering of reviews on the website; a lack of disclosure to consumers that describes how the ratings system operates; the message that ConsumerAffairs.com is a consumer advocacy organization; and the lack of disclosures describing the material connection between Consumer Affairs clients and their review pages.

ConsumerAffairs is a website that publishes stories on various topics and compiles consumer news, recall information, consumer resolutions, and company features along with press releases and alerts from different public sources. The site also maintains a publicly searchable database of consumer reviews of companies; each page pertaining to a company on the website includes a five-star "satisfaction rating" based upon complaints and reviews.

As the marketer's website encompasses all aspects of customer contact, including products, services, sales and complaints, ERSP did not object to the marketer's characterization of its website as a "... consumer news and advocacy organization."

ERSP found that the relationship between ConsumerAffairs and its accredited members was not adequately disclosed and thus, recommended the marketer clearly and conspicuously disclose the material connection it has with its accredited members throughout its website.

ERSP also recommended that ConsumerAffairs modify its website to clearly and conspicuously disclose to visitors of the website that reviews and complaints upon which the satisfaction ratings are based are displayed differently for accredited members and nonaccredited members.

EUROPHARMA
Curamin
Case #361 (2/4/2015)

ERSP considered whether EuroPharma failed to adequately inform consumers of the material connection between EuroPharma and the website TerryTalksNutrition.com, which features Terry Lemerond, a founder and president of EuroPharma. The marketer asserted that the TerryTalksNutrition site is a third-party, educational website containing information relating to health and nutrition and that the content is based on the opinions and experience of Mr. Lemerond.

EuroPharma said that as a demonstration of good faith, future references on the site will be made only to ingredients and not specific formulas. EuroPharma also explained that it had removed links from the blog to EuroPharmaUSA.com and Curamin.com.

LIQUID HCG DIET, LLC (Twitter)

*Liquid HCG Diet
Case #246 (6.16.10)*

Claims for the homeopathic Liquid HCG Diet product appeared on Twitter. In particular, the twitter claims attested to the effectiveness of the Liquid HCG Diet. The marketer argued that they were not behind the posting of messages related to their product on twitter, and were unaware of how the messages appeared on the Twitter page of "jessicastewart9."

ERSP looked to the FTC Guides Concerning the Use of Endorsements and Testimonials in Advertising, which point out that an advertisement that contains an endorsement that relates to the experience of one or more consumers on a central or key attribute of the **product will be interpreted as representing that the endorser's experience is** representative of what consumer can generally expect to achieve. ERSP determined that the weight-loss and diet success results attested to on individual Twitter pages is considered advertising for the purpose of communicating general expectation of the product. According to ERSP, without any information to the contrary which may lead consumers to understand that the statements are unrepresentative of typical product performance, these representations must be independently supported by the marketer. In addition, ERSP noted that the fact that the marketer did not know about a consumer making a particular claim does not absolve the marketer from responsibility of the accuracy of the claims.

*URBAN NUTRITION, LLC (Blogs)
WeKnowDiets.com (and affiliated websites)
Case #219 (8.11.09)*

In this case, ERSP examined advertising claims on the marketer's websites, which were formatted as independent product-review sites.

The challenger argued that the marketer presented itself as an unbiased and independent resource for consumers when there was a potentially material connection between the marketer, the websites and the products reviewed. The challenger also argued that the marketer failed to disclose that it had compensated the individuals writing the product reviews.

Preliminarily, ERSP pointed out that the language on the weknowdiets.com website would appear to indicate that the information was based upon independent assessments of the products. However, the marketer conceded to ERSP that it owned and controlled the weknowdiets.com site, along with other affiliated websites.

It was clear to ERSP that because the marketer owned not only the websites, but several **products being reviewed on the site, this relationship constituted a "material connection"** that would have a significant effect on the weight or credibility given to the endorsement by that audience. ERSP also concluded that because the marketer hosts and exercises

editorial control over the websites for the purposes of disseminating reviews of products that directly compete with the marketer's own products, it is imperative that the placement of the disclosures regarding material connections be of such prominent nature that consumers understand the relationship of the marketer and the products being reviewed immediately upon visiting the site.

INNOVATIVE MEDIA, INC. d/b/a www.PhantomPlate.com (Second Life)
PhotoBlocker Spray
Case #196 (12.3.08)

ERSP's first case involving advertising that appeared in social media. The advertising at issue was found in Second-Life, which is an internet-based, 3D virtual community that allows users to explore, meet other residents, socialize and create and trade items with each other. ERSP determined preliminarily that advertising within online games may be considered national advertising.

The product, Photoblocker Spray, is designed to be sprayed onto the face of motor vehicle license plates, which will conceal the license plate numbers and/or letters from photo-radar traffic cameras. ERSP concluded that the legality of the product is a material condition in consumers purchasing the product – marketers must inform consumers that the product may not be used legally in certain states.

The ASRC Online Archive is an exclusive resource for the advertising industry and contains decisions authored by the:

- Children's Advertising Review Unit
- Electronic Retailing Self-Regulation Program
- National Advertising Division
- National Advertising Review Board

The full text of each decision issued by the advertising industry's self-regulatory system is available by subscription.

For more information about the ASRC Online Archive, please contact Saveeta Dhanai. She can be reached at 212.705.0115, or by email at sdhanai@asrcbbb.org.

SECTION 6

Right of Publicity Update



Presented by

Megan K. Bannigan
Debevoise & Plimpton LLP
New York, NY

2019 National CLE Conference: Right of Publicity Update

Megan K. Bannigan, Debevoise & Plimpton LLP

INTRODUCTION

This year in right of publicity law was marked by significant developments in high-stakes cases across a wide variety of media platforms, including videogames, film and television, social media, advertising and promotion, and music. The past year has demonstrated the extent to which outcomes diverge depending on the type of speech at issue, the nature of the creative work and the scope of liability under the state law. With so much hanging in the balance, the law remained in the spotlight, grabbing headlines as centenarian actress Olivia de Havilland sued FX Networks and fantasy sports sites *FanDuel* and *DraftKings* came under fire for unauthorized use of athletes' names and likenesses. These lawsuits, among other closely watched cases, illustrate the difficulty courts continue to face in balancing the First Amendment freedom of expression against the property and privacy rights of individuals.

State laws protecting the individual right of publicity vary significantly with respect to scope and duration. This was highlighted over the last year in the **videogame** context. New York, for example, does not recognize a common law right of publicity and recently held that the statutory right will be construed narrowly, covering only "name, portrait, picture or voice." *Lohan v. Take-Two Interactive Software, Inc.*, 97 N.E.3d 389, 393 (N.Y. 2018). California, on the other hand, recognizes both a statutory and a common law right of publicity, allowing plaintiffs in the ongoing lawsuit against videogame publishers Electronic Arts to proceed under the common law even where their claim was not supported under the statute. *See Davis et al. v. Electronic Arts, Inc.*, No. 10-CV-03328-RS, 2018 WL 1609289, at *1 (N.D. Cal. April 3, 2018).

While use of celebrity likeness in videogames continues to be risky business, the recent holding by the California Court of Appeal in *De Havilland v. FX Networks*, 21 Cal. App. 5th 845 (Ct. App. 2018), shows that **television and film**, depending on what you are looking to do, may be a safer haven. The *De Havilland* decision outlined critical First Amendment protection to creators of docudramas, biopics, documentaries and other expressive works involving the realistic depiction of celebrity. The California Court of Appeals was clear that right of publicity law is not defined by the industry custom of paying a life-rights acquisition fee. The First Amendment does not require acquisition agreements before a celebrity (or anyone for that matter) may be depicted in an expressive work, so long as the likeness is "one of the raw materials" from which the original work is synthesized.

In the world of **fantasy sports**, the Indiana Supreme Court recently held that uses of players' names, pictures and statistics in online fantasy sports games and related advertisements are of "newsworthy value." Accordingly, the unauthorized use of athletes' names and likeness in

operating and promoting fantasy sports is not actionable under Indiana’s right of publicity statute.

In cases involving commercial (non-newsworthy) use of an individual’s likeness in **advertising or promotional materials** the Sixth Circuit holding in *Roe v. Amazon.com*, 714 F. Appx. 565 (6th Cir. 2017), raises a critical question at the heart of right of publicity protection: whether the commercial value of an individual’s persona should be determined by looking at (1) whether the defendant derived commercial value from the unauthorized use or (2) the independent commercial value in plaintiff’s identity. The Sixth Circuit choice the second approach, *id.* at 568, and, if other courts follow, non-celebrities will face a nearly insurmountable obstacle in recovering under a right of publicity theory for the commercial exploitation of their identity. Another pending case, *Brophy v. Almanzar*, No. 8:17-cv-01885, 2017 WL 4865544 (C.D. Cal. Oct. 26, 2017), also involving the appropriation of personal photographs published in the public domain for commercial purpose, and – if fully litigated – may offer further guidance for creators incorporating photographs circulating the public domain into new creative works, including whether Brophy’s right of claim is preempted by the federal copyright law as defendants maintain. *See* Mot. to Dismiss, *Brophy v. Almanzar*, No. 8:17-cv-01885 at *2 (C.D. Cal. Apr. 2, 2018).

There were also developments with respect to post-mortem publicity rights. The District Court of Minnesota followed the majority approach to hold that the right of publicity is descendible under the common law, even where no post-mortem statutory right of publicity exists. This outcome raises the larger issue of how post-mortem rights may be accurately valued. The difficulty involved in assessing post-mortem rights was highlighted in a recent dispute between singer Whitney Houston’s estate and the IRS over the valuation of Houston’s estate. A settlement was ultimately reached, but the dispute is indicative of the IRS’s ongoing effort to include the right of publicity among the property comprising the estate and to collect taxes accordingly.

VIDEO GAMES

New York

Gravano v. Take-Two Interactive Software, Inc., 97 N.E.3d 396 (N.Y. 2018)

Lohan v. Take-Two Interactive Software, Inc., 97 N.E.3d 389 (N.Y. 2018)

- The *Lohan* and *Gravano* decisions coming out of New York’s highest court represent a significant victory for both Take-Two Interactive Software, producer of Grand Theft Auto (GTA), and the creative industry more broadly.

- Lindsey Lohan and former “Mob Wives” star Karen Gravano brought claims Take-Two Interactive for unauthorized use of their likeness in Grand Theft Auto V in violation of their right to privacy under New York Civil Rights Law § 51.
- Lohan alleged that “Lacy Jonas,” a blonde woman encountered in a storyline entitled “Escape Paparazzi,” misappropriated Lohan’s “portrait and voice.” 97 N.E.3d 389 at 391. Gravano alleged that the GTA V character, Andrea Bottino, made unauthorized use of Gravano’s likeness and family history. *Gravano v. Take-Two Interactive Software, Inc.*, 142 AD 3d 776, 777 (App. Div. 2016).
- The New York Court of Appeals determined that digital avatars may constitute a “portrait” within the meaning of New York’s privacy statute, but found that avatars in question were not sufficiently recognizable as Lohan or Gravano to constitute “portraits” as a matter of law.” 97 N.E.3d 389 at 394.
 - With regard to Lohan’s claim, the Court of Appeals explained, “the artistic renderings are indistinct, satirical representations of the style, look, and persona of a modern, beach-going young woman that are not reasonably identifiable as the plaintiff.”
 - With regard to Gravano’s claim, the Court found nothing in the Bottino avatar sufficiently evocative of Gravano to violate the law, explaining that the “defendants never referred to Gravano by name or used her actual name in the video game, never used Gravano herself as an actor for the video game, and never used a photograph of her.”
- The decisions provide the following critical safe-guards for expressive works, including videogames:
 - The New York right of publicity statute will be construed narrowly, covering only “name, portrait, picture or voice.”
 - The decisions confirmed that a judge may decide at the pleading stage whether an expressive work features an actionable “portrait.”
 - The Appellate Division decision affirmed long-standing New York precedent by holding that expressive works like books, movies, television, plays, and sometimes videogames, are not “advertising” or “trade” and accordingly fall beyond the scope of the right of publicity statute. 142 A.D.3d 776 at 777.

Ninth Circuit

***Davis et al. v. Electronic Arts, Inc.*, No. 10-CV-03328-RS, 2018 WL 3956212 (N.D. Cal. Aug. 17, 2018)**

- Videogame publisher Electronic Arts (EA) fared less favorably in the District Court for the Northern District of California against retired NFL football players Michael E. Davis, Vince Ferragamo and Billy Joe Dupree. The retired players brought a class action against EA for violating plaintiffs’ statutory and common law rights of publicity through unauthorized use of their likenesses in the *Madden NFL* video game franchise. *See Davis et al. v. Electronic Arts, Inc.*, No. 10-CV-03328-RS, 2018 WL 1609289 at *1 (N.D. Cal. April 3, 2018).
- The District Court held that the players’ claim may proceed against EA under the common law right of publicity, finding that the avatars in question may effectively evoke the persona of individual players when coupled with various contextual clues.
- Liability will largely rest on whether the factfinder determines that the avatars in question are readily identifiable as the individual players.
 - The District Court cited *White v. Samsung Elecs. Am., Inc.*, 971 F.2d 1395 (9th Cir. 1992) for the general proposition that “likeness” as used in § 3344 is construed more narrowly than California common law. 2018 WL 3956212 at *1 (N.D. Cal. Aug. 17, 2018).
 - “Likeness” under California’s common law right of publicity is construed more broadly than the statutory right, allowing plaintiffs to demonstrate use of likeness by reference to more than just the appearance of the avatar alone, including such identifying characteristics as a “player’s position, years in the NFL, height, weight, skin tone, and skill level in different aspects of the game.” *See Davis et al. v. Electronic Arts, Inc.*, No. 10-CV-03328-RS, 2018 WL 1609289 at *1 (N.D. Cal. April 3, 2018).
- The District Court rejected EA’s First Amendment defense, affirming the Ninth Circuit finding that the use of players’ likenesses was not transformative since the avatars at issue, if found to be readily recognizable as the plaintiffs, are engaged in the very activity for which the plaintiffs have derived their fame. *Id.* at *3.
- In August 2018, the District Court affirmed its denial of class certification. *Davis v. Elec. Arts Inc.*, No. 10-cv-03328-RS (N.D. Cal. Aug. 17, 2018). Players will still be permitted to litigate their respective claims on an individual basis, but the denial of class certification does likely reduce potential damages faced by the defendants.

FANTASY SPORTS

Indiana

***Daniels v. FanDuel, Inc.*, 884 F.3d 672 (7th Cir. 2018), certified question accepted, 94 N.E.3d 696 (Ind. 2018)**

***Daniels v. FanDuel, Inc.*, No. 18S-CQ-00134, 2018 WL 5275775 (Ind. Oct. 24, 2018)**

- Former college football players, Akeem Daniels, Cameron Stingily and Nicholas Stoner, brought action against fantasy sports sites, FanDuel and DraftKings, for unauthorized use of their names and likeness in operating and promoting fantasy sports contests. Defendants claimed that they were protected from liability under Indiana’s right of publicity statute, Ind. Code § 32-36-1-1(c), since their conduct fell under either the “newsworthy exception” or the “public interest exception.”
- The District Court for the Southern District of Indiana dismissed the complaint finding that the use was exempt as both “newsworthy” and as “concerning a matter of public interest.” No. 1:16-cv-01230-TWP-DKL, 2017 WL 4340329 at *5-9 (S.D. Ind. Sept. 29, 2017).
- On appeal, the Seventh Circuit certified the following question of statutory interpretation to the Supreme Court of Indiana:

“Whether [under Indiana’s right of publicity statute] online fantasy-sports operators that condition entry on payment, and distribute cash prizes, need the consent of players whose names, pictures, and statistics are used in the contests, in advertising the contests, or both.”
- The Indiana Supreme Court held narrowly that “online fantasy sports operators that condition entry to contests on payment and distribute cash prizes do not violate the Indiana right of publicity statute when those organizations use the names, pictures and statistics of players without their consent because the use falls within the meaning of ‘material that has newsworthy value, an exception under the statute.’” 2018 WL 5275775 at *1.
- When the case returned to the Seventh Circuit, the appellate panel dismissed college athletes’ claim against FanDuel and DraftKings, finding that the Indiana Supreme Court’s decision settled the matter. *Daniels v. FanDuel, Inc.*, No. 17-3051 at *3 (7th Cir., Nov. 29, 2018). The Seventh Circuit declined to address plaintiffs’ argument that the fantasy games constituted illegal gambling, explaining “if a state prosecutor brings such charges, it will be for the state judiciary” to resolve. *Id.* The Seventh Circuit also reiterated that players might still have a claim if they could demonstrate that the use of their names created a likelihood of confusion over endorsement. *Id.*

TELEVISION

California

***De Havilland v. FX Networks, LLC*, 21 Cal. App. 5th 845 (Ct. App. 2018), review denied (July 11, 2018)**

- Actress Olivia de Havilland brought action against FX Networks for violating her right of publicity by using her name and identity in the docudrama *Feud: Bette and Joan* without her permission.
- The trial court denied FX Network’s anti-SLAPP motion to strike, but the Court of Appeals reversed, ruling that the motion to strike de Havilland’s claims should have been granted. 2017 WL 4682951 at *13 (Cal. Super. Sept. 29, 2017).
- The Court of Appeals emphasized the role of the First Amendment in protecting expressive works, even when those expressive works realistically “portray real people.” 21 Cal. App. 5th 845, 850.
 - The decision clarified that the First Amendment protects FX from liability for Catherine Zeta-Jones’ unauthorized portrayal of de Havilland in the docudrama: “Whether a person portrayed in one of these expressive works is a world-renowned film star—‘a living legend’—or a person no one knows, she or he does not own history. Nor does she or he have the legal right to control, dictate, approve, disapprove, or veto the creator’s portrayal of actual people.” *Id.* at 850, 857.
 - The court also explained that industry custom does not dictate the scope of First Amendment protection. Producers will sometimes enter into “acquisition agreements” before depicting a celebrity in a television series or film, but the “First Amendment simply does not require such acquisition agreements.” *Id.* at 860.
- The Court of Appeals stopped short of holding that docudramas like the one at issue could claim categorical exception from the right of publicity, but still found that the use of de Havilland’s likeness in *Feud* was sufficiently transformative to claim First Amendment protection. *Id.* at 863.

***Sivero v. Twentieth Century Fox Film Corp.*, No. B266469, 2018 WL 833696 (Cal. Ct. App. Feb. 13, 2018), *reh’g denied* (Mar. 2, 2018), *review denied* (May 23, 2018).**

- Frank Sivero, a film actor best known for his performances in *The Godfather Part II* (Paramount Pictures 1974) and *Goodfellas* (Warner Bros. 1990), sued Fox for violating his statutory and common law right of publicity by using his name and likeness on *The Simpsons* without his permission. *The Simpsons* introduced the Sivero lookalike character in October 1991 when a “mafia henchman known as Louie who resembled Sivero’s character in *Goodfellas*” appeared as one of “one of two henchmen for a mafia boss known as Fat Tony.” 2018 WL 833696 at *1. This character has since appeared in fifteen subsequent episodes, the movie and videogames based on the television show.

- The Court of Appeals granted Fox’s motion to strike the complaint under the California anti-SLAPP statute, finding that the First Amendment protects the use of Sivero’s likeness in *The Simpsons* because the depiction of Sivero was “Simponsized” and not a literal likeness. *Id.* at *10.
 - The character based on Sivero “is a cartoon character with yellow skin, a large overbite, no chin, and no eyebrows. [He] has a distinctive high-pitched voice which, as the trial court pointed out, has ‘no points of resemblance to [Sivero].’” *Id.*
 - The court explained that because “the cartoon distortions as well as the comedic portrayal” render Louie far from a “satisfactory substitute for a conventional depiction of Sivero,” Sivero’s right of publicity was not threatened by the resemblance. *Id.*

Merchandising and Promotion

Second Circuit

***Khaled et al v. Bordenave et al*, No. 1:18-CV-05187, 2018 WL 2761578 (S.D.N.Y June 8, 2018)**

- Entertainer, Khaled M. Khaled, popularly known as “DJ Khaled,” filed a complaint against Curtis Bordenave and his company Business Moves Consulting Inc. for trademark infringement and violating Khaled’s and his three year old son’s right of publicity under New York Civ. Rights L. § 50.
- Khaled maintains that his son Asahd Tuck Khaled became “instantly famous in his own right upon his birth in October 2016” such that Business Moves violated Asahd’s right of publicity by producing tee-shirts bearing the name Asahd in connection with their products and services. 2018 WL 2761578 at *2. Khaled claims that the appropriation is manifest because the spelling of his son’s name is “distinctive” as a “non-traditional spelling of the name ‘Assad.’” *Id.* at *10.
- Bordenave registered a series of marks playing off Khaled’s and his son’s fame including, We the Best Lifestyle; Asahd; Asahd Couture, which he changed to A.S.A.H.D. Couture; and A.S.A.H.D. A Son And His Dad. *Id.* at *23. Khaled alleges that through these registrations Bordenave sought to wrongfully trade on Khaled’s and his son’s fame, in addition to infringing Khaled’s trademark rights in the catchphrase, “We the best.”
- Khaled further alleges that Bordenave’s use of “Asahd” on products and services deliberately referenced his son in an attempt to exploit the child’s fame.
- The case is still pending before the District Court for the Southern District of New York.

Ninth Circuit

***Brophy v. Almanzar*, No. 8:17-CV-01885, 2017 WL 4865544 (C.D. Cal Oct. 26, 2017**

- Keven Michael Brophy, Jr.—a “family man with minor children”—brought a claim against Belcalis Almanzar (popularly known as “Cardi B”) for misappropriating the “unique likeness” of his body art. 2017 WL 4865544 at *1.
- In 2016, Cardi B released her first album—*Gangsta Bitch*—featuring a “sexually charged image” of an individual bearing Brophy’s tattoo “wedged between her legs.” The Complaint alleges that since Cardi B skyrocketed to fame, the “image and likeness on the *Gangsta Bitch* cover is now widely displayed across the internet, including on iTunes, Amazon, and Spotify,” negatively impacting Brophy’s life and exposing him to unwanted attention and commentary. *Id.* at *1.
 - The tattoo at issue spans Brophy’s entire back “depicting a tiger battling a snake, with other interrelated tattoos that continue around his torso and along his arms.” *Id.*
 - Brophy is not a celebrity, but boasts a following of “nearly 10,000” on Instagram. *Id.* Working for a “surfing and lifestyle company,” Brophy’s back and tattoo is frequently exposed and he alleges the tattoo has become readily recognizable among his “wide-ranging community of fellow professionals and friends.” *Id.*
- Defendants allege that the album cover is the result of photoshopping a copyrighted photograph of Brophy’s back tattoo found in the public domain onto the back of another individual. *See* 8:17-cv-01885-CJC-JPR at *2 (C.D. Cal. May 1, 2018). Defendants argue that when an individual’s likeness is captured in a copyrighted artistic visual work (the photograph of Brophy’s back) and that copyrighted work is in turn incorporated into another copyrighted work (the album cover), a right of publicity claim interferes with the exclusive rights of the copyright holder in the photograph and is preempted by section 301 of the Copyright Act. The District Court accordingly must first determine whether Brophy’s right of publicity claim is preempted under the § 301 of Copyright Act.
- If the District Court finds that Brophy’s claim is not preempted, defendants may still prevail by showing that the use is sufficiently transformative to claim protection under the First Amendment. The matter is currently pending in the District Court for the Central District of California.

***Scott v. Citizen Watch Co. of Am., Inc.*, No. 17-CV-00436-NC, 2018 WL 1626773 (N.D. Cal. Apr. 4, 2018)**

- Colonel David Randolph Scott, a retired astronaut and the mission commander for NASA’s 1971 Apollo 15 voyage, brought suit against defendants—Citizen Watch Company of America, Inc. (“Bulova”), a watch manufacturer, and Sterling Jewelers, Inc. dba Kay Jewelers, a retailer that sells Bulova watches—for violating his right of publicity under the

statutory and common law by using his name, title, photo, and voice without his permission in the marketing and promotion of a commemorative “Moon Watch.”

- The wristwatch in question, the “Special Edition Moon Chronograph Watch,” was intended to replicate Scott’s personal Bulova chronograph worn during the Apollo 15 moon landing.
- The advertisements and promotional materials associated with the Moon Watch featured Scott’s name, title and photograph, in addition to video containing an audio clip of Scott’s voice. 2018 WL 1626773 at *2.
- Bulova moved for summary judgment under several theories, the strongest of which was that the use was protected under the First Amendment as a matter of public interest.
- The District Court denied the motion to the majority of claims. It determined that the public interest exemption does not apply to Bulova’s use of Scott’s identity in the marketing and promotional materials associated with the Moon Watch. The court explained that, although the “fact that Bulova manufactured Scott’s original chronograph certainly gives Bulova greater license to boast about its connection to the Apollo 15 mission,” the defendants’ use of Scott’s identity in their advertisements may “cross the event horizon into the black hole of misappropriation.” *Id.* at *8.

Seventh Circuit

***Martin v. Wendy’s Int’l, Inc.*, 714 F. Appx. 590 (7th Cir. 2018), cert. petition filed May 23, 2018 (pending)**

- Johannes T. Martin, record holder for consecutive kicks of a footbag (commonly associated with the Hacky Sack brand), brought a right of publicity claim against Wendy’s and Guinness World Records related to a promotional campaign involving Wendy’s Kids’ Meals featuring “Guinness World Records record-breaking toys.” 714 F. Appx. 590 at 591.
- Martin alleged that Wendy’s and Guinness used his identity for commercial purposes without his written consent in violation of the Illinois Right of Publicity Act, 765 ILCS 1075/1–1075/60, by offering a Kids’ Meal which included a footbag accompanied by an instructional card explaining that: “Back in 1997, Ted Martin made his world record of 63,326 kicks in a little less than nine hours!”
- The Seventh Circuit affirmed the District Court’s dismissal of Martin’s claim, explaining that the use of Martin’s name was beyond the scope of the statute since Illinois right of publicity statute does not apply to the “use of an individual’s name in truthfully identifying the person as the author of a particular work or program or the performer in a particular performance.” *Id.* at 592.

Sixth Circuit

***Roe v. Amazon.com*, 714 F. Appx. 565 (6th Cir. 2017)**

- John and Jane Roe brought claims against an individual author, Greg McKenna, and his book’s online retailers, Amazon.com, Barnes & Noble Booksellers, Inc. and Smashwords, Inc. (“Corporate Defendants”), for violating their right of publicity by publishing a book with their engagement photo on the cover without their permission.
- McKenna found the photograph on the photographer’s website and downloaded it for use on his book cover without obtaining plaintiffs’ permission or providing compensation.
- The District Court granted the Corporate Defendants motion for summary judgment, and Plaintiffs ultimately dismissed claims against McKenna in their entirety with prejudice. *See Stipulated Dismissal and Entry, Roe v. Amazon.com*, No. 3:15-cv-111 (S.D. Ohio June 7, 2018).
- The Sixth Circuit affirmed the grant of summary judgment, finding that the plaintiffs failed to demonstrate the Corporate Defendants made use of the engagement photograph for commercial purpose.
 - The court explained that celebrity status is not necessary to bring a right of publicity claim, but plaintiffs must still “demonstrate that there is value in associating an item of commerce with [their] identity.” *See Landham v. Lewis Galoob Toys, Inc.*, 227 F.3d 619, 624 (6th Cir. 2000).
 - Because the plaintiffs failed to demonstrate commercial value in associating their likeness with the online retailers, the Sixth Circuit affirmed summary judgment for Corporate Defendants.

Music

Second Circuit

***Estate of Smith v. Cash Money Records, Inc.*, No. 14-CV-2703, 2018 WL 2224993 (S.D.N.Y. May 15, 2018)**

- This lawsuit began as a claim for copyright infringement against Drake after Drake’s record label failed to obtain the musical composition license to sample an album by jazz artist James Oscar Smith. The sampling was ultimately ruled fair use, but Drake countersued Smith’s music production company—Hebrew Hustle Inc.—and its owner, Stephen Hacker, for publishing a photo of the rapper on their website without permission.

- Hacker conceded that the photo was published without permission, but protested that the photo was one of many on the website and was not used for commercial advantage as required under the right of publicity statute. 2018 WL 2224993 at *8.
- The District Court considered whether establishing unauthorized use of a celebrity’s likeness demonstrates that the use was “to the commercial advantage” of the defendant as a matter of law, finding that unauthorized use of celebrity likeness is *likely* to the defendant’s advantage, but unauthorized use does not itself establish as a matter of law that such use was to the commercial advantage of the defendant. *Id.* at 11.
- The case is currently pending before Judge William H. Pauley III in the District Court for the Southern District of New York.

Eighth Circuit

***Paisley Park Enterprises, Inc. v. Boxill*, 299 F. Supp. 3d 1074 (D. Minn. 2017)**

- This case arises from a dispute surrounding the possession and commercial exploitation of five previously unreleased musical recordings by Prince, who died in April 2016.
- In resolving the dispute, the District Court of Minnesota held that the right of publicity is descendible under Minnesota’s common law, following the majority approach. Accordingly, the court denied defendant’s motion to dismiss.

U.S. Tax Court

***Estate of Houston v. Commissioner*, 1098-16 (U.S. Tax Court, Dec. 26. 2017)**

- The estate of the late award-winning singer and actress, Whitney Houston, battled the IRS over the valuation of Houston’s estate, including her postmortem right of publicity.
- Houston’s estate claimed that the IRS had inflated valuations of the singer’s intellectual property in record royalties, merchandising, publicity and movie rights to the tune of \$11 million dollars. The estate had claimed that Houston’s right of publicity was worth just under \$200,000, while the IRS claimed that it was worth more than \$11.7 million.
- Whitney Houston’s estate ultimately entered a stipulation with the IRS on December 26, 2018 settling the estate’s tax bill.
- The settlement was for \$2 million, but did not specify how her right of publicity was valued.

Social Media

California

***Cross v. Facebook, Inc.*, 14 Cal. App. 5th 190 (Ct. App. 2017), review denied (Oct. 25 2017)**

- “Country-rap” singer Mikel Knight sued Facebook for among other things, violating his right of publicity by running unrelated ads from Facebook advertisers adjacent to content critical of Knight’s involvement in two fatal car accidents.
- The California Court of Appeals affirmed the trial court’s order granting Facebook’s anti-SLAPP motion and striking the complaint in its entirety, finding that Facebook did not use Knight’s name or likeness for commercial purposes for the following reasons:
 - Facebook did not use Knight’s identity because the pages at issue were posted by third parties.
 - Knight failed to establish that Facebook appropriated his name “for purposes of advertising or selling” as required under the statute. The court found no evidence that Facebook obtained a commercial advantage through the use of Knight’s name; the evidence demonstrated that even when advertisements appeared adjacent to the page at issue, they made no use of Knight’s name or likeness.

Right of Publicity Update

Megan K. Bannigan

Debevoise & Plimpton LLP, New York, NY

Debevoise
& Plimpton

VIDEO GAMES

Lohan v. Take-Two Interactive Software, Inc., 97 N.E.3d 389 (N.Y. 2018)



Debevoise
& Plimpton

VIDEO GAMES

Gravano v. Take-Two Interactive Software, Inc., 97 N.E.3d 396 (N.Y. 2018)



Debevoise
& Plimpton

VIDEO GAMES

Davis et al. v. Electronic Arts, Inc., No. 10-CV-03328-RS, 2018 WL 3956212 (N.D. Cal. Aug. 17, 2018)



Debevoise
& Plimpton

FANTASY SPORTS

Daniels v. FanDuel, Inc., 884 F.3d 672 (7th Cir. 2018), *certified question accepted*, 94 N.E.3d 696 (Ind. 2018)

Daniels v. FanDuel, Inc., No. 18S-CQ-00134, 2018 WL 5275775 (Ind. Oct. 24, 2018)

SIDNEY CROSBY
 Pittsburgh Penguins | #87 C
 DraftKings Salary: \$9,000
 Next Game: Phi@Pitt (04/01 8:00 PM ET)

2014 SEASON STATS

GP	G	A	PTS	PPG
71	25	54	79	4.1

STATISTICS

	GP	G	A	PTS	+/-	PIM	HITS	BS	FW	FOL	SOG	%	PPG	PPA	SHG	SHA	TOIG	FPPG
Last Game	1	0	1	1	1	2	0	1	10	13	3	0.000	0	1	0	0	19.2	4.2
Last Ten Games	9	3	9	12	2	2	5	2	103	114	30	.100	2	3	0	0	20.6	4.3
2014 Season	71	25	54	79	8	45	60	29	727	746	215	.116	10	21	0	0	19.6	4.1

LATEST PLAYER NEWS
 March 28 (11:31:55 PM ET)
 UPDATE: Crosby collected three points -- including a goal and two assists -- in a 5-2 victory over the Coyotes on Saturday.
 ANALYSIS: The Pens superstar has scored six goals and 20 points in his last 14 games after going through a seven-point, 13-game stretch. He leads the NHL with 79 points (25 goals, 54 assists) in 70 games.
 March 21 (11:48:49 PM ET)

AROUND THE LEAGUE
 Greg Wyshynski
 New Puck Daddy: Puck Daddy Power Rankings: Alex Ovechkin, playoff ticket drives, NHL Draft
<http://t.co/zqkCy2zjD> an hour ago
 Greg Wyshynski
 April 15, 2014 - When I confronted Marek about using "cutouts" in interviews, #MvsW 2 hours ago

Debevoise & Plimpton

TELEVISION

De Havilland v. FX Networks, LLC, 21 Cal. App. 5th 845 (Ct. App. 2018), *review denied* (July 11, 2018)



Debevoise & Plimpton

6

TELEVISION

Sivero v. Twentieth Century Fox Film Corp., No. B266469, 2018 WL 833696 (Cal. Ct. App. Feb. 13, 2018), *reh'g denied* (Mar. 2, 2018), *review denied* (May 23, 2018).



Debevoise
& Plimpton

MERCHANDISING AND PROMOTION

Khaled et al v. Bordenave et al, No. 1:18-cv-05187, 2018 WL 2761578 (S.D.N.Y. June 8, 2018)



Debevoise
& Plimpton

MERCHANDISING AND PROMOTION

Brophy v. Almanzar, No. 8:17-cv-01885, 2017 WL 4865544 (C.D. Cal Oct. 26, 2017)



Debevoise
& Plimpton

MERCHANDISING AND PROMOTION

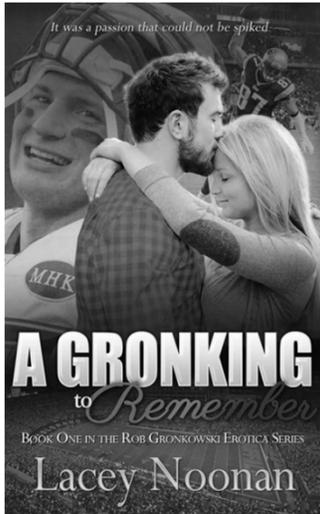
Martin v. Wendy's Int'l, Inc., 714 F. Appx. 590 (7th Cir. 2018), cert. petition filed May 23, 2018 (pending)



Debevoise
& Plimpton

MERCHANDISING AND PROMOTION

Roe v. Amazon.com, 714 F. Appx. 565 (6th Cir. 2017)

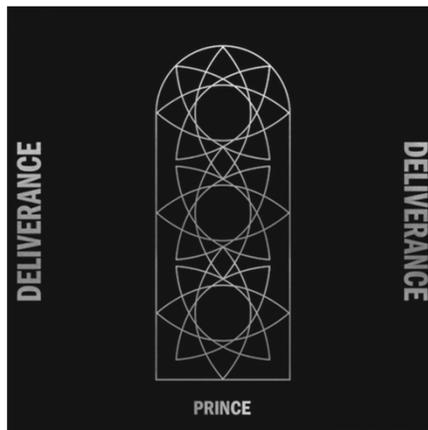


Debevoise
& Plimpton

11

MUSIC

Paisley Park Enterprises, Inc. v. Boxill, 299 F. Supp. 3d 1074 (D. Minn. 2017)



Debevoise
& Plimpton

SOCIAL MEDIA

Cross v. Facebook, Inc., 14 Cal. App. 5th 190 (Ct. App. 2017), review denied (Oct. 25 2017)

The screenshot shows a Facebook page for "Public Awareness of Mikel Knight and The Maverick Dirt Road Street Team". The page layout includes a cover photo of a truck, a left-hand navigation menu with options like "Home", "About", "Photos", "Posts", "Community", and "Info and Ads", and a "Create a Page" button. The main content area displays a post by "Bobby Wildcat Throgmorton" with a photo of two young men in football jerseys and text stating "Me and my little brother did and died in that wreck". Below this is another post by "Bobby Wildcat Throgmorton" with text "I worked for him and my little brother died out there. His funeral was never PAID for...". The right-hand sidebar contains "About" information, a "Send Message" button, a website link "www.savingcountrymusic.com/the-sound-of-dec", and a "Related Pages" section listing "Mikel Knight" (Musician/Band), "Upchurch" (Musician), and "Bradley Mitchell" (Public Figure).

**Debevoise
& Plimpton**

13

SECTION 7

PLENARY SESSION

Much More Fun With Ethics at the Movies



Presented by

Larry J. Cohen, Ph.D., J.D.

Cohen's Counsel

Bethel, VT

REFLECTIONS ON STRIVING FOR THE ETHICAL AND PROFESSIONAL PRACTICE OF LAW

Larry J. Cohen
January 2019

In December 2014, I was preparing to deliver what I thought then would be the last ethics program I would ever teach. I was preparing as well to close out my career as a practicing law. I loved being a lawyer. I had spent more than 30 years practicing law and I still loved it. Turns out I loved it so much that I could not get myself to stop and I am still practicing today. And as it turns out I am still teaching ethics as well.

But back in December 2014, when I thought I was about to put it all behind me I reflected a great deal on what it had meant for me to be a lawyer. I thought a lot about what it takes to deliver legal services. But more than that, those reflections led me to think about what it means to be an ethical and professional lawyer in the world we lived in.

And as I read over now what I wrote then I think about how much harder it is just four years later to be an ethical and professional lawyer in the world we live in today. The world, or at least the society we now live in, has become such a divisive place; it is not so much that people differ in their beliefs, but people seem so entrenched, so certain that they are right and that all opposing views are wrong, so unwilling to listen, so closed to persuasion.

People come to lawyers not so much looking for counsel, but looking for warriors

soldiers who will fight their battles as they define them. People are less willing to hear facts that are contrary to their views; they reconstruct the world as they want to see it.

And this is on top of all of the things already out there challenging lawyers in their practice of their profession. It is not easy to be a lawyer.

It has never been easy. There are so many things that pull and tug at lawyers that make consistently ethical and professional practice a challenge at best and overwhelming at worst. This is not intended to provide an excuse from unethical and unprofessional conduct, but rather a recognition that it is something that takes attention, thought and effort. Over the course of this reflective essay I will talk about why, and I will talk about things that lawyers can do to get there.

Having now stated my purpose I want to be very clear about two things that I will not do here. First, I have no intention of preaching any particular course of action. Such an approach requires one to sit in judgment of others, believing that he or she knows the answer and has the right to tell others how they must act. I believe in the ethics rules and the professionalism principles, and further believe that they are the proper guides to ethical and professional conduct.

But I recognize as well that there is more to life and to the life of a lawyer than those rules and principles and that what in the end drives the behavior of any particular person is a complicated combination of personal beliefs about right and wrong, the genetics and biology that set us in motion and constrain our behavior, the demands of everyday life, personal and professional, and a myriad of other idiosyncratic factors. In

my teaching I have always constrained myself to talk about the rules and principles in the context of the challenges to abiding them, and to talk about the consequences for the client, the public and the lawyer of deviating from them. The goal in the end is to be thoughtful about the choices we make and to be prepared to be held accountable for those choices.

Second, I am not in this reflective essay holding myself out as an example of anything. I am just a person, and pretty average one at that as I look out and compare myself with my colleagues. I have my own strongly held beliefs about right and wrong, and my own capabilities and limitations set by my own genetics and biology. I have pressures on me to act and forebear in any given instance, just like everyone else.

I cannot say and would not for a moment suggest that in thirty-three years of practice I have always complied with every rule and abided every principle. What I can say, and what I would urge on others as a goal, is that I have tried very hard to make compliance and abidance part of my everyday life as a lawyer; that I have taken responsibility for and expressly acknowledged my deviations, that I have tried not to make the same mistake too many times, and that when I have made mistakes I always tried to make amends when the circumstances presented an opportunity to do so.

Holding myself out as I do as a teacher of ethics I have had to deal from time to time with lawyers chiding me, and worse, for what they construed as unethical or professional practice. Who am I, they would say or imply, to teach ethics and professionalism but not to practice it? I cannot think of an instance, even now upon

reflection, where I agreed with them that the conduct in issue was unethical or unprofessional. At the same time, the criticism was then and continues now in each instance to be extraordinarily painful, and to lead me into days or weeks of self-doubt and self-criticism for what I did to bring on such accusation. Each time I came out of that experience determined more than ever to comply and abide, and hopefully at some level I have been true to every such determination.

I also come out of that experience each time with three observations and lessons: first, how hesitant we should all be to sit in judgment of others; second, to see, regrettably, how readily lawyers will use rules and principles, even ethics rules and professionalism principles, as swords to attack others; and third to appreciate how valuable all the rules and principles are as guides to actions which make us better lawyers individually and a better profession collectively.

The remainder of this reflective essay will try to express in more detail what I have learned as I have watched myself and others over thirty-three years of law practice, and what I have gained from the seemingly countless questions asked of me and comments made to me while teaching many hundreds of ethics and professionalism seminars across the country, and working with lawyers to be in the law school ethics courses I taught over a period about fifteen years.

1. What Does it Mean to be a Lawyer?

The simplest and obvious answer to this question is that a licensed attorney can represent individuals and organizations in court. This is, as a practical matter, what

distinguishes being a lawyer from every other profession.

My purpose in raising this issue, however, is not to focus on this legalistic distinction between the permissible scope of the practice of law as compared with the permissible scope of the practice of other professions. Rather, it is to think about why we practice law in the first place and how the personal goals of lawyers bear on ethical and professional practice.

The ethical rules and professionalism principles are not that challenging as guidelines for practice. There are levels of complexities to the rules and subtleties, to be sure. But no lawyer would argue about the most basic things the rules and principles ask of us: keep secrets, avoid conflicts, be honest, don't steal, show respect for the dispute resolution process (especially the courts). Yet lawyers run afoul of even these most basic rules and principles, and we are left to ask why.

Certainly the goals lawyers have in mind for themselves as they enter and then engage in the practice of law play an important role here. The acquisition of wealth, the pursuit of power, the ability to be in control over one's life, recognition among peers, accolades in the public media and the like can be achieved practicing within the rules and principles.

But the rules and principles can get in the way as well, if not generally then certainly in the moment. The media, fiction and nonfiction, is awash with illustrations of lawyers seeking advancement toward such goals being frustrated by even the most basic of the rules and principles. There is nothing sinister about Vinnie Gambini wanting to

help his nephew out of a terrible situation, and in the process prove to himself and others that he is capable of being a good lawyer. In order to do so, however, he must first be permitted to represent his nephew in the Alabama criminal courts. Fearing that having failed the Bar five times and having practiced only civil law, and that for a short period of time, would not impress the Judge sufficiently to allow him to appear pro hoc vice in an Alabama criminal court he takes the expedient step of exaggerating to the point of lying about his credentials. The lie is successful, and he is allowed to represent his nephew. He then proceeds to demonstrate great cunning and skill in achieving real justice. We are left to applaud, literally, his accomplishments, having forgotten or forgiven the fact in order to achieve his great goals he had to lie to the Court.

We all talk in terms of sacrifices that we have to make to achieve our goals. That internal discourse we have about sacrifices should include how we deal with the impediments the ethical rules and professionalism principles present in accomplishing those goals. These impediments confront goal seeking behavior inevitably. They cannot be avoided. When that happens lawyers must ask themselves how important the goals they are seeking are relative to rules we agree to follow and the principles to which we are asked to aspire when we accept the license to practice law.

2. Everyday Challenges to Ethical and Professional Practice

The goals lawyers set for themselves are the macro-level challenges to ethical and professional practice. Every day lawyers confront micro-level challenges in

the details of the daily practice of law.

When I teach ethics to law students, something I have been doing two semesters a year for the past ten years or more, I start out most every class with what I call the “ethical issue of the day.” These are hypotheticals or illustrations based loosely on an ethical issue I confronted myself, an ethical issue about which another lawyer sought my suggestion, or something I witnessed another lawyer doing. There were many reasons I used these illustrations in class, not the least of which is to give the students a chance to see how ethical issues arise and can be dealt with in everyday practice.

The most important reason I bring up the “ethical issue of the day,” however, is that I want the students to appreciate just how readily and frequently lawyers are confronted with ethical and professionalism issues in their practice. Ethics and professionalism are not abstract concepts that we have to deal with just occasionally or from time to time. They come up continuously in practice, perhaps not every day but certainly with great frequency.

Most lawyers attend to the large and unavoidable problems, like questions about whether taking on a new client is permitted when the new client’s interests may be in conflict for a former client the attorney represented. Lawyers may give less thought to things they do more reflexively, like meeting with a client in a busy restaurant to talk about progress in a case, billing a client an extra and unearned tenth of an hour or two for amorphous activities like file review and legal research, avoiding an unwanted telephone call by instructing a staff person to say the lawyer is busy or out of the office when in fact

the lawyer is neither, and encouraging a witness not to talk with the other side.

Few lawyers spend time reading the rules and principles. It is not particularly realistic to expect lawyers to do so. Indeed, that is one of the main reasons, if not the main reason for the requirement to earn three hours of ethics credits a year.

Lawyers do well to be reminded of their obligation to act ethically and to aspire to be professionals in their everyday practice.

These brief experiences with the things that satisfy the ethics requirement may not be enough to remind the lawyer when they come across the myriad of situations in the everyday practice of law that raise ethical and professionalism principles. Better that lawyers have a working understanding or at least appreciation of the principles that underlie ethics and professionalism. Such understanding may not always lead to ethical and professional behavior, but it may cause a red flag to pop up when a lawyer is about to take action and lead to the momentary thought in the situation presented that will result in a choice consistent with the rules and principles.

This is not the place to set forth those principles; that is left to another writing or presentation. One example will make the point. The “3” series of rules, the advocacy rules, guide lawyers in their role as litigants in dispute resolution proceedings, and particularly the courts. The rules in this section are plentiful, detailed and in some instances rather complicated. There is a core interest that underlies all of these rules, however, an interest in cases being decided on their merits. When confronted with an issue in the course of being an advocate lawyers who keep this core interest in mind will

be sensitive to ethical and professionalism issues when they arise and will have at least an idea about the course of action required or encouraged by the ethics rules and professionalism principles.

3. Genetic and Biological Limitations

The first instinct most people have when presented by potentially or actually troubling conduct by a lawyer, whether unethical or unprofessional, is to attribute purposeful or intentional action on the part of the lawyer. This is certainly the image created by the fictional media about lawyers, as bad people seeking to advance their own interest to the detriment of others. That certainly is true of some lawyers, but does it explain all of the behavior that concerns us when we think about the ends being sought by the ethics rules and the professionalism principles.

As I have studied neurology over the years, and especially recently with the greater appreciation of the genetically based and biologically discreet differences among individuals in how the brain drives behavior, I have become more inclined to look past the attribution of someone as a “bad” person and more inclined to think about what is driving the concerning behavior. This is not to excuse unethical and unprofessional behavior when it happens. Rather, the point is to recognize that there may well be more to concerning behavior than ill motivation and therefore the need to think about explanations and solutions that consider the totality of the individual.

For example, over the course of my practice I have from time to time caused some consternation on the part of co-counsel and clients by doing things that need

to be done at the last minute. Such behavior on my part could implicate E.R. 1.3, concerning diligence in the handling of client cases, or E.R. 3.2, diligence in processing cases through the dispute resolution mechanism. For many years I chided myself to get things done sooner and the timing of my work has improved as I have pressed myself toward that end. Yet there continue to be times when I find myself pressed at deadlines, completing motions, drafting letters and like activities. In reflecting on why that happens I find some solace in the fact that I have good intentions, work hard as a general proposition and like most lawyers have to prioritize things that need to be done, leaving some things to be done last.

But as I have looked more closely at myself I have recognized that there is something else at work, something over which I seem to have less ability to manage away as a problem. There is something about the way that I think about problems that is potentiated by the demands of an approaching deadline. Try as I might to work through a problem or issue early, I find in some instances that I have difficulty thinking the matter through very much in advance of the deadline. I have not sought a clinical explanation for why this is so. I have speculated that probably I suffer from some aspect of attention deficit disorder, not much thought about and certainly not something regularly diagnosed during the era when I went to primary and secondary school, in the 1950's and 1960's.

There are solutions to problems grounded in biological and genetic sources. There are compensatory techniques one might try, behavioral counseling that may be helpful, medications that can help with planning and attentiveness. Or perhaps just

knowing that this underlying conditions are present may help the lawyer understand his or her own behavior and organize themselves more productively. The point is to take these matters into consideration as we think about how we can abide our ethical and professionalism obligations and, over the long run, expand our collection of solutions when ethical violations do occur so they we fashion solutions that really will deal with the underlying problem.

4. Practicing Law is Emotionally Wearing

Emotional wear and tear is such a fundamental reality of the everyday practice of law that lawyers rarely talk about it. There are some, and an increasing number it seems, of continuing legal education classes about stress, but nothing that even begins to address the pervasiveness of the emotional damage lawyers experience daily in their practices.

The consequences of this emotional wear and tear have not gone unnoticed. Addictive behaviors, most prominently among them substance abuse, are recognized by the Bar and addressed both through voluntary and diversion programs. In other words, we deal with the results of emotional wear and tear when they reach the point of seriously dysfunctional behavior.

One could make an argument for trying to recognize the consequences of emotional wear and tear sooner, and come up with solutions to these problems. Sensible as this may seem in the abstract, it raises privacy issues that would be and should be of great concern. We are already a highly regulated profession. It would be fair for lawyers

to ask how much more of their Constitutional and civil rights they should be asked to give up to engage in this profession. This is another debate for another time.

My point here is for lawyers to consider the impact of emotional wear and tear far sooner than when the consequences begin manifesting themselves in dysfunctional behavior. In its earliest stages it is entirely predictable that lawyers will seek means of dealing with the activities that cause emotional damage as they try to regulate their lives to a point where the emotional damage is lessened generally. Such activities may well involve conduct that approaches or crosses the border into unethical and unprofessional activity. For example, not returning calls to avoid dealing with challenging clients or lawyers; exaggerating the risk a client faces if a case goes to trial to encourage settlement and so the removal of a case from the caseload and the receipt of funds to deal with a challenging financial circumstance; doing superficial work on a motion just to get it done and out rather than put in the hours that really are needed to produce the quality product that the circumstance requires.

The solution in these situations is to evaluate the resources available relative to the volume of work generally and the level of stress presented by the collection of cases specifically. The result of that evaluation may lead to the adoption of such simple solutions as reducing the volume and content of the caseload, to more challenging solutions like spending more funds on resources to do the work at the loss of profit, to the most challenging solutions like recognition that a change in practice setting is needed. The point is to be thoughtful about how emotional wear and tear may drive one to

unethical and unprofessional practices.

5. The Most Common Conflict Problem

We have six rules dealing with conflicts of interest, E.R. 1.7 through E.R. 1.12. This reflects a recognition of both the pervasiveness of conflicts of interests and the complexity conflict of interest issues presented.

It seems that the greatest attention is paid to conflicts arising where two current clients have conflicting interests (E.R. 1.7(a)(1)) or when the interests of a current client conflicts with the interest of a former client (E.R. 1.9). My impression, however, is that far and away the most common conflict of interest problem is presented when the interests of the client are in conflict with the interests of the lawyer. (E.R. 1.7(a)(2)

(2) there is a significant risk that the representation of one or more clients will be materially limited by the lawyer's responsibilities to another client, a former client or a third person or by a personal interest of the lawyer.

(Emphasis added). When the breadth and depth of a lawyer's personal interests are considered, extending as they do across the lawyer's personal and professional lives, it is easy to see how this very likely is the most prevalent of the conflict of interest problems.

There are two important points to be made here. First, the fact that a lawyer has a personal interest bearing on a representation does not mean this ethical rule is implicated. As set forth in the rule, there must be a "significant risk" that the lawyer's representation of the client will be "materially" limited by the lawyer's personal interest. Thus, when these personal interest issues arise the lawyer may consider whether the risk

is significant and whether the quality and content of the representation will be limited in a material way.

As an aside, this is a good point to remind lawyers that we have a rule, E.R. 1.0, that provides definitions that may be more or less helpful in understanding the scope of an ethical rule. Unfortunately, neither the term “significant” nor the term “material” are defined in E.R. 1.0.

The second important point is that when the risk is significant and the representation may indeed be materially limited, then the lawyer should proceed to engage in a conflict of interest analysis to determine whether waiver is possible, and, if so, seek consent for waiver of the conflict. To that end lawyers will benefit from the guidance provided by comment 2 to E.R.1.7:

[2] Resolution of a conflict of interest problem under this Rule requires the lawyer to: 1) clearly identify the client or clients; 2) determine whether a conflict of interest exists; 3) decide whether the representation may be undertaken despite the existence of a conflict, i.e., whether the conflict is consentable; and 4) if so, consult with the clients affected under paragraph (a) and obtain their informed consent, confirmed in writing. The clients affected under paragraph (a) include both of the clients referred to in paragraph (a)(1) and the one or more clients whose representation might be materially limited under paragraph (a)(2).

The best advice to lawyers, from a risk management standpoint, is to err on the side of caution and address these “personal interest” problems with the client when they arise in practice, even when there may be uncertainty on the part of the lawyer about whether the risk is significant and whether the limitation is material.

6. People Centered Practice

Over the course of a semester long course on ethics there is time to explore with law students how some concepts and conceptualizations work themselves through the ethics rules and professionalism principles. One such conceptualization I find to be especially helpful is to think about the practice of law generally, and about ethics and professionalism in particular, from the perspective of the public, the client and the lawyer.

All of the ethics rules and professionalism principles can be understood in the context of the policy interests they embody and reflect. For example, confidentiality, E.R. 1.6, is important because it provides a context in which clients, feeling secure in their privacy, will be forthcoming with the full scope of information lawyers need to assist them with their troubles. From the public's perspective it serves the policy goal of disputes being resolved on their merits. We can be confident if all of the applicable evidence is before the decision maker then the outcome is credible because all interests have been considered. Individual disputes can be and are resolved and social unrest is minimized or avoided. The reporting rule, E.R. 8.3, serves the policy goal of gaining confidence with the public in the integrity of the legal profession, with lawyers required where egregious circumstances warrant to report misconduct to the Bar for assessment and, if appropriate, corrective action and/or sanctions.

My experience has been, though, that it is a challenge to get law students during ethics courses and lawyers in ethics CLE programs, to look at the rules and principles, and violations of the rules and principles, from these different points of view.

They readily see how their conduct as lawyers may be affected by the rules and principles, and they can relate to the impact of the consequences of rule violations on their own lives. They have trouble seeing the rules and principles from the perspective of the clients and the public however, even when pressed to think about it in those terms.

Years ago I thought how educational and insightful it would be to have law students taking ethics courses make journal entries about depictions of lawyers in the fiction and nonfiction media engaged in activities that implicated ethics rules and professionalism principles. The assignment required students to describe briefly in their journal entries the lawyer's behavior, identify the applicable rule(s) and principle(s) and then project how the depiction might affect how clients, prospective clients, or the public generally might view lawyers and the legal profession in light of what was depicted. The vast majority of the students did very well with the first two parts of the journal assignment, but had extraordinary difficulty looking at these media depictions from the perspective of clients, prospective clients and the public generally. Indeed, the exercise was so challenging for them that I had to resort to passing out examples of what I was seeking, going over with them multiple times what I was looking for in the last section and then inviting them to submit drafts so I could comment on the inevitable problems they had with seeing the events through these other perspectives. In the years that followed I learned to do better at helping the law students understand what I was seeking and why I thought the assignment was a useful exercise, but the journal entries have continued to be challenging assignments for them,

I have never experimented with a like exercise with lawyers, lacking the context in which to do so. I have listened carefully to what lawyers have to say in the hundreds of ethics CLE courses I have taught across the country during the past fifteen years or so. My impression is that lawyers can see readily the intent of the rules from a legalistic perspective and they certainly are sensitive to how violations can affect their own lives. Like the students, though, many lawyers have trouble seeing the impact of reported and depicted violations on how clients and prospective clients think about us and what they expect from us.

I think lawyers would be well served in their practices to give consideration when confronted with circumstances that draw them close to or over the borders of required ethical conduct or aspired professional behavior to consider how non-lawyers may feel about them as lawyers and about our profession generally when they see or learn about these kinds of happenings. Such a person-centered approach to the practice of law would encourage a deeper respect for why the rules exist. Such respect would go beyond mere concern for the consequences of the discipline process, and to what the rules and principles are trying to accomplish in promoting faith and confidence in our profession as a source of help for individuals dealing with troubles in their everyday lives and as a source of fair outcomes and justice.

7. Suspending the Ego

As lawyers we spend the majority of our time working to achieve the client's ends. Inevitably we take sides on the question of who is right and who is wrong.

Cases that cannot be resolved on mutually acceptable terms are resolved through a zero-sum process in which there are decided winners and losers. It should come as no surprise, then, that in their daily work lawyers get very much engaged in pressing positions they believe must be accepted and fighting against positions they believe should be rejected.

The substantive aspects of this process are inevitable in our profession. Less inevitable, and in important respects counter-productive, is the internal need some lawyers have to be seen as the victor, the prevailer, the stronger, the more powerful, the smarter and the like. These ego driven needs can drive lawyers to be excessively demanding in their dealings with other lawyers, to be abusive in their interactions with third parties, to be disrespectful to the Court, and to be insensitive to their clients' anxieties and stresses.

Suspending one's ego can be an extraordinarily liberating experience. The mental and emotional energy reserved alone permits greater focus on what needs to be done for the client and so more time for the lawyer to do other things that matter in the lawyer's personal and professional lives. The point here is not to care less about the quality of one's work or to draw less pleasure from one's successes in practice. Rather, it is not to worry any longer, or at least not to worry as much about how other people think about you. In the process lawyers are likely to find themselves held in even higher regard and enjoy greater esteem when it is the quality of the work performed and the outcomes achieved that do the speaking for the lawyers, rather than actions by the lawyer that insist upon a certain kind of regard and respect.

8. Respect for the Rights of Third Parties

When we decided to go to law school and signed on to be lawyers our expectation was that our central focus would be to advance the interests of the clients we served. This is the area of practice covered by the “1” series of rules.

At some point in our respective practices, earlier for some and later for ours, depending the kind of work we did, we discovered our responsibilities to the advocacy process. This is the area of practice covered by the “3” series of rules. Much to our surprise we further discovered in the course of practice not only that some of the “3” series rules conflicted with duties and obligations we had under the “1” series of rules, but that sometimes we were required or expected to attend to our obligations to the advocacy process even at the expense of the obligations we owed our clients. Indeed, there is an argument to be made that our duty of candor to the Court. E.R. 3.3, may require that we breach the most fundamental of duties we owe our clients, the duties of confidentiality and loyalty, and in the process put the client in harms way.

We tolerate the precedence given the advocacy process, at the expense of the client, because of the importance of the advocacy process in avoiding social unrest and maintaining social cohesion. It is far more difficult to accept the idea that duties we may owe others, third parties, with whom we have no formal relationship and who’s paths we cross only as we pursue the interests of our clients, should enjoy some precedence as well.

For example, E.R. 4.3 provides that in dealing in the course of a

representation with an unrepresented third party we must communicate the fact that we are representing a client, so the third party will know the context in which we are dealing with that person. Further, if the third party seeks advice or direction, we are limited to advising the third party, if we give any advice at all, to consult with a lawyer. The policy interest in this rule is to respect the rights of others and to prevent the lawyer from using greater knowledge about substance and process and greater resources to put the third party at risk of harm. This rule prevents the lawyer from taking action that would benefit the client, such as extracting information from the third party without the filters the third party may use when the third party comes to understand why the lawyer is there.

It is fair to ask why the duties set forth in the "4" series of rules were imposed on lawyers in the first place. There can be no doubt that these rules are impediments to the zealous representation of the client. In the jurisdiction where I have mostly practiced, Arizona, the concept of zealous representation was replaced long ago with representation that "conforms to the requirements of the law." The "4" series of rules may be well be seen as impediments to that as well, though, putting in certain instances the interests of third parties ahead of the interests of the client.

It is not hard to imagine how such other-regarding rules came into being. Certainly one reason had to be too many instances of disrespectful, abusive and unfair conduct by some lawyers in their dealings with third parties. Whatever their source lawyers are as bound to abide these rules as they are the other rules that impose duties and obligations on lawyers.

My experience teaching ethics CLE programs is that this “4” series of rules is the one with which lawyers are least familiar and with which, frankly, they have the most disagreement. Nevertheless, whether to the end of avoiding discipline or to the end of advancing the integrity of the profession lawyers need to familiarize themselves with these rules and conduct their practices consistent with them,

9. Thieves Always Worry that Others Are Stealing from Them

My father, who died at age 92 about a year and a half ago, was a marginally educated person who through his life paid surprisingly close attention to the goings on in the world around him. He was deeply religious, and from the beliefs in his faith and drawing on the experiences in his culture, offered what I think to this day was his most profound observation on life, spoken usually in Yiddish: People Plan and God Laughs. I have confronted that reality so many times in my life, having made great plans only to see things go awry. Perhaps that is why when people asked me in 2014 what I planned to do when I left private practice I told them that I really do not know, that at that point my focus was not on the outcome, but on the adventure itself. For now the adventure led me back to the practice law; one day it will lead me to something else, but for now I am content to do what I love, help people with their everyday problems.

It is not that observation on life that I want to address here today, though. My father was by trade a shoe salesman. He rose to the level of designing, merchandising, marketing and operating shoe concessions in department stores. In that context he had the opportunity to observe customers, employees, department and store

managers. He had a variety of other life experiences, including growing up a victim of intense bigotry to the point of fending off physical attacks on a daily basis, and service during World War II in a communications unit that was always the first wave in any battle plan. From those experiences he offered an observation which I found amusing when he first said it, but later became for me an invaluable way to understand one aspect of ethical and professional behavior.

Thieves Always Worry that Other People are Stealing From Them

The point of course is that people who in their own lives victimize others are especially sensitive to the possibility that they may be victimized themselves.

I think about this observation in many different kinds of situations when trying to understand what has motivated another lawyer, and sometimes a judge, to act as they do in readily criticizing the conduct of others, often with great emotional intensity. It is especially noteworthy when this comes as a knee jerk reaction to be confronted with the reality of their own misconduct in a situation. This observation has particular application to situations that raise ethical and professionalism issues.

We have all had the experience, and I have had a couple of them very recently, of dealing with lawyers whose conduct is counterproductive in dealing with an issue, potentially destructive and harmful of one's own client's interests, and perhaps even beyond the bounds of ethical and professional practice. When such actions are called to their attention, not with any tag lines about unethical or unprofessional conduct,

but toward the end of resolving the issue and moving in a more productive direction, the quick response includes accusations back of misconduct, including unethical and unprofessional behavior. Such responses are invariably unproductive and can lead to a deterioration of the situation to the point of name-calling, threats and like unproductive behaviors from both sides to the other

Recognition that this may well be a situation of “thieves worrying that other people are stealing from them” may help the lawyer confronted with such situations put the events in a context where a more productive response may be helpful. Rather than engage in the name calling and reciprocating accusations level, the better course may be to ignore the initial volley of threats and stay focused on a constructive outcome that is in the client’s best interests. We all know from our earliest of experiences that bullies thrive on conflict, and that if you do not react to the provocation and either disengage or focus on something productive moving forward, there is the chance for a positive outcome. The bully goes off to look elsewhere to for the pleasure the bully derives from of making trouble.

10. Why Practice Ethically and Professionally?

A student approached me on the last day of my most recently completed ethics class and asked why a lawyer would strive to consistent ethical and professional behavior in practice. I knew the student had something more in mind than avoiding sanctions. I had spent a great deal of time during class talking about all of the things, large and small, subtle and overt, that pull and push at the lawyer to violate ethical rules

and professionalism principles. We had talked at length as well about the challenges Bars face in trying to regulate behavior, both in terms of the resources available to the Bar for lawyer regulation and the difficulty of observing the concerning behaviors in issue, especially where that assessment of the behavior requires consideration of what the lawyer was thinking at the time of the behavior in issue.

The answer I gave the student is rather pollyannaish, but it is what I truly believe. The ethical rules and professionalism principles exist to encourage lawyers to courses of behavior that will maximize the potential for just outcomes while treating those with whom lawyers deal along the way, including clients, counsel, the judiciary, third parties and others, with the respect and dignity to which they are entitled.

SECTION 8

Practical Strategies from Corporate Counsel on the Scope of Intellectual Property Protection



Presented by

Scott Piering

Vice President and Chief Intellectual Property
Counsel, Spectrum Brands, Inc.
Middleton, WI

SECTION 9

The ACPA, UDRP and URS: Navigating the Alphabet Soup of Domain Name Dispute Resolution



Presented by

Paula L. Zecchini
Cozen O'Connor
Seattle, WA

The ACPA, UDRP and URS: Navigating the Alphabet Soup of Domain Name Dispute Resolution

Presented By:

Paula L. Zecchini



“The **rising number** of alleged cybersquatting cases shows the **growing premium placed on domain names** by companies and individuals operating **in the wired environment.**”

- Francis Gurry



Domain Name Basics

- The Internet's global domain system is managed by the **Internet Corporation for Assigned Names and Numbers** (ICANN)
- Available domain names are sold on a **first-come, first-served** basis
- There are no absolute rights to a domain name



Conflict on the Internet

Cybersquatting—the unauthorized registration and use of domain names containing other parties' trademarks—is one of the most frequent sources of conflict on the Internet

Multiple formal and informal options exist to resolve cybersquatting disputes



Conflict on the Internet

ICANN established multiple formal dispute resolution procedures—most notably the **Uniform Domain Name Dispute Resolution Policy (UDRP)** and **Uniform Rapid Suspension (URS) System**

The **Anticybersquatting Consumer Protection Act (ACPA)**, which is part of the Lanham Act, also targets bad faith cybersquatting



Conflict on the Internet

Not every domain name is appropriate for resolution under the URS, UDRP or ACPA

Problems arise where a domain name contains a trademark with multiple other uses, especially in the absence of evidence that the domain name was registered or is being used in bad faith



Uniform Domain Name Dispute Resolution Policy



COZEN
O'CONNOR

UDRP at a Glance

- Contractually-based procedure to address the **most egregious examples** of bad faith registration
- Efficient means to challenge registrations that contain character strings **identical** or **confusingly similar** to trademarks
- Remedies **limited to cancellation or transfer**; damages and injunctions are not available

COZEN
O'CONNOR

Prevailing on a UDRP Claim

Complainant must prove all three of the following by a **balance of probabilities** or **preponderance of the evidence**:

- Domain is **identical** or **confusingly similar** to a trademark or service mark in which the complainant has rights
- Registrant has **no legitimate right** or interest to the domain
- Domain was registered and is being **used in bad faith**

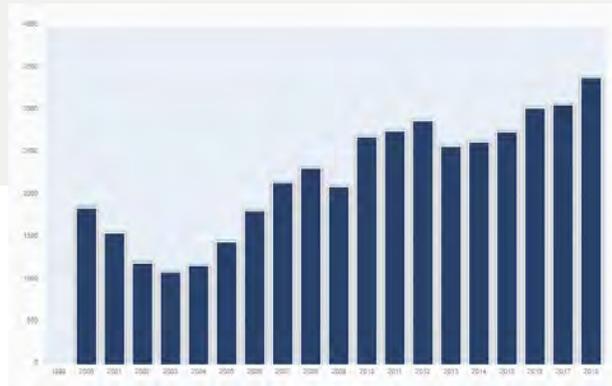


Benefits of the UDRP

- Complaints typically **resolved in less than 60 days** with straightforward filings and no discovery
- Provisions in registration agreements mean **no jurisdictional or service issues**
- Favorable standard of proof for brand owners (approximately **90%** of all UDRPs **decided in favor of brand owners**)
- More cost effective than litigation—average UDRP **resolves for under \$10,000**



UDRP Filings on the Rise



Source: <https://www.wipo.int/amc/en/domains/statistics/cases.jsp>



Disadvantages of the UDRP

- No guarantee that a ruling will be final and availability of **judicial review is limited** by jurisdiction—e.g., U.S. v. U.K.
- Rulings can be **unpredictable** and **inconsistent** due to lack of evidentiary guidelines and precedential authority
- No opportunity for investigation, and **money damages are unavailable**
- Does not apply to all **ccTLDs**



UDRP in Action

- **capitaloneonebank.com** (domain transferred; use of domain name to display links to competitors constituted bad faith)
- **mediurn.com** (domain transferred; replacement of “rn” for “m” insufficient to distinguish the domain from mark where visually perceived as one letter)
- **petlife.com** (transfer denied; trademark registration and first use in commerce post-dated registration of domain)



Decision Point: UDRP

- ✓ Top choice where **speed and cost efficiency** are the most desirable objectives
- ✓ Best suited for **small businesses** and brand owners that are merely attempting to **stop the use of their trademark**
- ✓ Helpful to brand owners challenging domain names registered **prior to the enactment of the ACPA**



Uniform Rapid Suspension (URS) System

YOYO'
e-mail



URS at a Glance

- Only applies to **gTLDs introduced after June 2013** (and handful of earlier gTLDs that adopted it)
- Must present a **clear case of trademark abuse** where evidence is overwhelming
- Sole remedy is **temporary suspension** of domain with one-year option to extend
- Re-examination and **appeals are allowed**



Prevailing on a URS Claim

Complainant must prove by **clear and convincing evidence** all three of the following:

- Domain is **identical** or **confusingly similar** to a word mark for which the complainant holds an **in-use, registered trademark**
- Registrant has **no legitimate right** or interest to the domain
- Domain was **registered and** is being **used in bad faith**



Benefits of the URS

- Online, **streamlined** filing process with **low cost** (filing fee for URS complaint starts at \$375, compared to \$1,300 for the UDRP)
- Built for speed—on average, decision issued in **less than 20 days**
- Can be used **in conjunction with UDRP as a quasi-preliminary injunction** pending resolution of UDRP proceeding



Disadvantages of the URS

The “URS is significantly **more complex** than the UDRP procedurally, offering a **lighter remedy (reversible on appeal)**, for a price target of less than a third of the UDRP.”

- *URS 2.0?, WIPO Discussion Contribution (October 2012)*



URS in Action

- ***goretexgiyim.world*** (suspended; use of website to sell counterfeit products demonstrated bad faith)
- ***saintlaurent.club*** (suspended; URS and UDRP used against same registrant with respect to same domains)
- ***supercluster.space*** (claim denied; URS cannot be used to suspend registration of domain with common terms absent bad faith)



Decision Point: URS

- ✓ Top choice where domain uses **famous mark** in clear infringing manner
- ✓ Primary interest is a **quick turnaround** in shutting down cyber outlets for **counterfeit goods**
- ✓ Better alternative for brand owners **concerned with expense** of growing domain portfolios—suspension allows owners to **balance the cost of enforcement** and monitoring



URS Policy Development

ICANN's URS policy development is ongoing

Initial Report of URS policy proposals is likely to be **released at the end of Q1 2019**—don't miss an opportunity to provide input!



Anticybersquatting Consumer Protection Act (ACPA)



ACPA at a Glance

- The **Anticybersquatting Consumer Protection Act** (ACPA), 15 U.S.C. § 1125(d), enacted in 1999, established a cause of action for **registering, trafficking in, or using** a domain name that is identical, confusingly similar to, or dilutive of, a **trademark** or **personal name**
- Remedies include **injunctive relief**, monetary **damages (actual or statutory)**, as well as domain forfeiture, cancellation or transfer



Bad Faith Under the ACPA

- ACPA enumerates nine non-exclusive factors to consider; **none are dispositive**
- Factors concern evidence of good faith (**registrant's own trademark rights** and use) and bad faith (**registrant's conduct in relation to domain** and extent to which domain is distinctive or famous)
- Despite enumerated factors, most important grounds for finding bad faith are the **unique circumstances** of the case



Benefits of the ACPA

- Availability of **injunctive relief** and **statutory damages** between \$1K-100K per domain
- ACPA provides **express protection for personal names** and authorizes **in rem actions** against domains containing a registered trademark
- In contrast to UDRP, **disjunctive bad faith requirement** (“registers, traffics in, or uses a domain name” rather than “register and use”)



Disadvantages of the ACPA

- Litigation is an **expensive, lengthy process** with no guarantee of a well-reasoned outcome
- Potential **jurisdictional issues** if foreign nationals involved
- Prevailing party entitled to **attorneys' fees in exceptional cases**—danger for brand owners that overreach



ACPA in Action

- ***Sporty's Farm LLC v. Sportsman's Market, Inc.***, 202 F.3d 489 (2d Cir. 2000)
(cybersquatting where domain registered with primary purpose to prevent competitor from using domain name)
- ***Mayflower Transit, LLC v. Prince***, 314 F. Supp. 2d 362 (D.N.J. 2004) (domain registration to provide critical commentary not cybersquatting)



ACPA in Action

- *Petroliam Nasional Berhad v. GoDaddy.com, Inc.*, 737 F.3d 546 (9th Cir. 2013) (no cause of action for contributory cybersquatting)
- *Go Daddy Operating Group LLC v. Usman Ghaznavi, et al.*, 2018 WL 1091257 (N.D. Cal. Feb. 28, 2018) (granting preliminary injunction where infringing domains were used to perpetuate international spam campaign)



Decision Point: ACPA

- ✓ Best for dealing with **serial cybersquatters** where immediate relief is needed to prevent **true, irreparable harm**
- ✓ Effective process for handling **complex disputes** dealing with novel legal issues
- ✓ Most suitable for resolving claims where **bad faith is circumstantial** or based on **pattern and practice** of infringing behavior



SECTION 10

Developments in European IP Law, and the Expected Impact of Brexit



Presented by

Nick Aries
Bird & Bird LLP
London, UK

2019 National CLE Conference, Intellectual Property

Developments in European IP Law & Expected Impact of Brexit

Nick Aries, Partner, Bird & Bird (San Francisco Representative Office) – nick.aries@twobirds.com – (415) 231-6568

1. Trademarks Online – who has jurisdiction over websites?

Checklist for assessing EU targeting of an advertisement for goods offered for sale on a website:

1. In determining whether an advertisement of goods bearing a trade mark on the website of a foreign trader constitutes use of the trade mark in the EU, it is necessary to assess whether the advertisement is targeted at consumers in the EU and in that way constitutes use of the mark in relation to goods in the course of trade in the EU.
2. The mere fact that a website is accessible from the EU is not a sufficient basis for concluding that an advertisement displayed there is targeted at consumers in the EU.
3. The issue of targeting is to be considered objectively from the perspective of average consumers in the EU. The question is whether those average consumers would consider that the advertisement is targeted at them. Conversely, however, evidence that a trader does in fact intend to target consumers in the EU may be relevant in assessing whether its advertisement has that effect. Evidence of subjective intention is a relevant, and possibly (where the objective position is unclear or finely balanced) a determinative consideration in deciding whether the trader's activities, viewed objectively from the perspective of the average consumer, are targeted at the EU. Subjective intention cannot, however, make a website or page (or part of a page) which is plainly, when objectively considered, not intended for the EU, into a page which is so intended.
4. The court must carry out an evaluation of all the relevant circumstances. These may include any clear expressions of an intention to solicit custom in the EU by, for example, in the case of a website promoting trade-marked products, including the EU in a list or map of the geographic areas to which the trader is willing to dispatch its products. But a finding that an advertisement is directed at consumers in the EU does not depend upon there being any such clear evidence. The court may decide that an advertisement is directed at the EU in light of some of the non-exhaustive list of matters referred to by the Court of Justice in Pammer at [93] (see below). The appearance and content of the website will be of particular significance, including whether it is possible to buy goods or services from it. However, the relevant circumstances may extend beyond the website itself and include, for example, the nature and size of the trader's business, the characteristics of the goods or services in issue and the number of visits made to the website by consumers in the EU.

Extract from *Pammer*:

- 93 The following matters, the list of which is not exhaustive, are capable of constituting evidence from which it may be concluded that the trader's activity is directed to the Member State of the consumer's domicile, namely the international nature of the activity, mention of itineraries from other Member States for going to the place where the trader is established, use of a language or a currency other than the language or currency generally used in the Member State in which the trader is established with the possibility of making and confirming the reservation in that other language, mention of telephone*

numbers with an international code, outlay of expenditure on an internet referencing service in order to facilitate access to the trader's site or that of its intermediary by consumers domiciled in other Member States, use of a top-level domain name other than that of the Member State in which the trader is established, and mention of an international clientele composed of customers domiciled in various Member States. It is for the national courts to ascertain whether such evidence exists.

- 94** *On the other hand, the mere accessibility of the trader's or the intermediary's website in the Member State in which the consumer is domiciled is insufficient. The same is true of mention of an email address and of other contact details, or of use of a language or a currency which are the language and/or currency generally used in the Member State in which the trader is established.*

Merck KGaA, Darmstadt, Germany v Merck Sharp & Dohme Corp, Merck & Co Inc

On 24 November 2017, the English Court of Appeal handed down its decision in the dispute between pharmaceutical companies, Merck KGaA, Darmstadt, Germany (KGaA), and US-based Merck Sharp & Dohme Corp (MSD) for breach of contract and trade mark infringement in respect of the use of "Merck". A copy of the decision can be found [here](#).

The Court of Appeal confirmed the High Court's decision of 15 January 2016 that use in the UK by MSD of "Merck" alone either as a trade mark or company name breached a 1970 agreement with KGaA.

The dispute centred on KGaA's claim that MSD's online use of "Merck" in the UK breached a co-existence agreement between the parties and infringed trade mark rights in the UK. At the heart of the litigation was how an agreement originally negotiated in 1955 applied to use on the internet and social media.

Background

KGaA is an international pharmaceutical company whose origins date back to 1668. In 1891 it set up a US branch. After World War I the US branch became independent, eventually becoming MSD.

The two organisations entered into a worldwide co-existence agreement in 1955 regarding the use of the term "Merck". The agreement was amended in 1970.

High Court ruling

The High Court ruled in favour of the Claimant, with Mr Justice Norris deciding that MSD's use of "Merck" alone in the UK whether online or offline was a breach of the Agreement. He held that KGaA was entitled to an order restraining MSD from describing itself in any printed or digital material addressed to the UK as 'Merck', and restraining MSD's use in the UK of the trade mark 'MERCK' alone.

The Judge also ruled that uses of MERCK as part of MSDs branding on its global websites were directed to the UK and infringed the German group's UK trade mark rights.

Court of Appeal Judgment

Breach of Contract

The Court of Appeal decision confirms the Judge's finding that use by MSD of "Merck" alone in the UK whether as a trade mark or a company name amounted to breach of contract.

Targeting the UK

MSD also appealed the finding that the uses on the "Merck" branded websites and social media pages were uses in the UK. They claimed they were directed at US and Canadian citizens, jurisdictions where MSD was permitted to use MERCK alone under the Agreement.

The Court of Appeal took the opportunity to review the law on whether use on websites and social media was targeted at the UK. It summarised the general principles which emerged from CJEU and UK first instance decisions. In particular they noted that the mere fact a website is accessible in the UK is not sufficient basis for concluding that an advertisement is targeted at the UK, and that the issue of targeting is to be considered objectively from the perspective of average consumers in the UK. The Judgment goes on to say that the intention of the trader to target consumers in the UK may be relevant as may other circumstances beyond the website itself, for example, the nature and size of the trader's business and the number of visits made to the website by consumers in the UK.

When applying these principles to this case, Lord Justice Kitchin held that MSD conducted its healthcare business in many countries around the world, including the UK and that business was at all material times supported and promoted by the websites in issue. They constituted an integrated group of sites which were accessible by and directed at users in the UK and other countries in which MSD trades. A person seeking information about MSD on a particular topic would be directed or linked to one of the websites from which that information could be derived. This allowed MSD to target inventors and scientists in the UK, to recruit people in the UK, to solicit suppliers, to seek licensing opportunities in the UK and to provide purchase order terms and conditions applicable to the UK. The social media activities of MSD were also directed at persons and businesses in the UK in just the same way as the websites.

There were also appeals in relation to trade mark infringement, revocation and relief, which do not relate to the question of the principles of "targeting" or their application, so are not discussed here.

2. Trademark Recitations – open questions

Sky Plc & Ots v SkyKick UK Ltd & Anr (Arnold J; [2018] EWHC 155 (Ch); 06.02.18;
With thanks to my colleagues Hilary Atherton and Katharine Stephens)

Reprinted with permission.

Summary

In a case where Sky alleged that use of Skykick infringed its SKY marks, Arnold J referred the following questions to the CJEU: (i) can a registered EU trade mark be declared invalid on the ground that it is registered for goods and services that are not specified with sufficient clarity and precision (and does "computer software" lack sufficient clarity or precision); and (ii) can it constitute bad faith to apply to register a trade mark without any intention to use it in relation to the specified goods or services.

Facts

Sky alleged that Skykick had infringed four of its EU trade marks and one UK trade mark comprising the word SKY by use of the sign 'SkyKick' and variants thereof, and that it had committed passing off. SkyKick used the sign 'SkyKick' in relation to a product which automated the process of migrating a business's email accounts from Microsoft Office to Microsoft Office 365. It provided this product to Microsoft 'partners' who were specialised IT providers and acted as resellers of Microsoft products. SkyKick denied infringement and passing off and counterclaimed for a declaration that the SKY marks were wholly or partially invalid because their specifications lacked clarity and precision and that the marks were registered in bad faith.

Can lack of clarity and precision of the specification be asserted as a ground of invalidity?

The Judge noted that the CJEU's decision in IP TRANSLATOR (Case C-307/10) required that an applicant for a trade mark must specify the goods and services in respect of which registration was sought with sufficient clarity and precision to enable the competent authorities and third parties to determine the extent of the protection conferred by the mark. However, it did not necessarily follow that, if the applicant failed to do so and the office failed to ensure that the applicant rectified the lack of clarity or precision during the course of examination, the mark could be declared invalid on that ground after registration. He therefore referred this question to the CJEU.

The Judge was of the view that "computer software" for which Sky's marks were registered was too broad and conferred too broad a monopoly on a proprietor. However, he said that it did not necessarily follow that the term was lacking in clarity and precision, and he therefore also referred this question to the CJEU.

Validity of the SKY marks: bad faith

SkyKick contended that the SKY marks were registered in bad faith because Sky did not intend to use the marks in relation to all of the goods and services specified in their specifications. The Judge therefore referred to the CJEU the questions: (i) can it constitute bad faith to apply to register a trade mark without any intention to use it in relation to the specified goods or services?; (ii) if the answer is yes, is it possible to conclude that the applicant made the application partly in good faith and partly in bad faith if the applicant had an intention to use the trade mark in relation to some of the specified goods or services, but no intention to use the trade mark in relation to other specified goods or services?; and (iii) is Section 32(3) (which requires a declaration of intention to use a UK trade mark to be made on application) compatible with the Directive?

3. EU Copyright Reform

*So what's the latest? Is Europe really (*still*) moving away from protecting platforms and internet intermediaries? (Nick Aries, October 2018)*

A little while back I wrote a summary of where the debate had got to in Europe on the question of new obligations for online platforms and other internet intermediaries regarding the availability of unlawful content online. This article gives an update, following a highly publicized vote in the European Parliament in September 2018 concerning EU copyright reform.

Some scene-setting

It is worth giving a brief recap of the current regime in Europe. Articles 12-14 of the E-commerce Directive (ECD) contain protection from liability for those acting as "mere conduits", and those who are caching, or performing hosting services. The most relevant for the present debate is the Article 14 hosting defence. This shields information society service providers (such as ISPs, platforms, social media, etc) from liability for content stored at the request of a user of the service as long as they do not have actual knowledge of the illegal activity or information and are not aware of facts and circumstances from which the illegal activity or information is apparent. If the provider obtains such knowledge or awareness they are still protected as long as they act "expeditiously" to remove or disable access to the information (notice and take down).

This goes hand in hand with Article 15 ECD, which prohibits general obligations being imposed on providers to monitor the information transmitted, stored, or actively to seek facts or circumstances indicating illegal activity.

The hosting defence covers not just technical storage providers, but can also apply to sophisticated platforms doing more than mere storage.

Is Europe moving away from the current regime?

There are two aspects to look at: case law, and current EU legislative proposals and policy documents.

- Case law

In my last piece I referred to two European Court of Human Rights cases, *Delfi* and *MTE and Index.hu v Hungary*, in which portals had been found liable in respect of reader comments posted to articles. I pointed out that the correctness of the (questionable) Estonian and Hungarian domestic rulings that no intermediary protection applied to the portals was not under review by the supranational ECtHR, and so they were not necessarily indicative of a wider continental trend towards eroding intermediary protection.

I also referred to two judgments issued by the Northern Ireland High Court (*CG v Facebook Ireland Ltd* and *J20 v Facebook Ireland Ltd*), various aspects of which were subsequently overturned by the Court of Appeal in both cases. The NICA's findings on appeal somewhat reduced some of the concerns platforms would have been feeling based on the first instance findings, at least as regards the question of when "actual knowledge" accrues to a platform.

A question which remains unanswered is the extent to which platforms can be ordered to prevent the reappearance of content previously removed. Since the last piece, there has been a new reference to the Court of Justice of the European Union (CJEU) by the Austrian Supreme Court, on this question of 'notice and stay down' (*Glawischnig-Piesczek* Case C-18/18). In that case, an Austrian politician obtained an order obliging Facebook not only to

remove certain defamatory content but also to delete any future material bearing comments that were identical to the original wording, or if the comments were similar in meaning and Facebook had actual knowledge of these comments. On appeal, the Supreme Court pointed out that a broad injunction including statements differing from the original could conflict with the prohibition against imposing a general monitoring obligation on intermediaries (Art. 15 ECD).

The Supreme Court has therefore asked the CJEU whether Article 15 ECD precludes an order requiring a hosting provider found to have failed to expeditiously remove illegal information not only to remove the specific information but also other information that is not identical in wording, but similar in meaning; and whether that differs once the host provider has actual knowledge of the information. Intermediaries will be watching for the next development in this case for two reasons. First, because of the potential impact on the permissible width of injunctions that could be ordered against them in terms of the nature of the content which is the subject matter of the order. But also second, because the Court has in addition referred questions about the permissible territorial scope of such an order (in the case at hand, should it be global or limited to Austria).

Most recently, on August 8th 2018, the CJEU issued a ruling in the *SNB-React* case (C-521/17). The case concerned the liability of providers of IP address rental and registration service, but the Court made more general comments about the application of the protections from liability in the ECD. The Court recapped that the limitations of liability for mere conduit, caching and hosting services can only apply where the activity is of a mere technical, automatic and passive nature, which implies that that service provider has neither knowledge of nor control over the information which is transmitted or stored. So far, nothing new.

In the *Google France* and *L'Oreal v eBay* cases, the Court ruled that playing an active role of such a kind as to give a service provider knowledge of, or control over the content in question would take a service provider outside the limitation of liability. However, some commentators have drawn attention to wording in the *SNB-React* judgment which is arguably not consistent with these earlier judgments. In particular, the CJEU rather inaccurately paraphrased the 'active role' from *L'Oreal* as "allowing" users to optimise online sales activity, rather than "providing assistance" as it was put in *L'Oreal*. Further, the ambiguous nature of some of the CJEU's wording in its answer to the second question referred has led some to question if the CJEU was deliberately decoupling 'knowledge /control' from 'active role' (albeit, the CJEU was still requiring both before the exemption from liability would be disappplied). Given this would be a departure from previous rulings, and that the CJEU chose not to have the benefit of an Advocate General's Opinion in this case, it is perhaps more likely to be merely the result of some loose language.

- Proposed Copyright Directive

By way of brief recap, in September 2016 the Commission published draft text for a proposed new Copyright Directive. Draft Article 13 would oblige service providers that store and provide access to large amounts of works uploaded by users to: (1) take measures to ensure the functioning of agreements concluded with rights holders for the use of their works, and (2) prevent the availability on their services of works identified by rights holders through cooperation with the service providers. An example given of such measures is effective content recognition technology.

Both sides of the debate (rights holder vs intermediary) continue to be vociferous in their commentary. Many observers have also pointed out the lack of clarity around how this regime (specifically, part (2) above) is supposed to fit with the prohibition on monitoring in Art. 15 ECD, and other EU legal instruments.

What's the state of play right now?

The European Parliament held a vote on September 12th 2018 regarding the next steps for the proposed Directive. The Parliament voted in favour of providing a mandate for three-way ("trilogue") negotiations to begin on the draft Directive, on the basis of an amended version of the text originally proposed by the Commission.

The Parliament endorsed a version of Article 13, applying to 'online content sharing service providers', defined as those who store and give access to significant amount of copyright protected works or other protected subject-matter uploaded by its users, which the service optimises and promotes for profit making purposes. The measure provides that such OCSSPs do perform an act of communication to the public (which is a question currently before the CJEU in two cases referred by the German supreme court), and so need a licence from right holders covering UGC. If they don't take a licence, they must cooperate in good faith with right holders to prevent availability of protected works on their services. Unlike the original proposal, this version contains no longer any express reference to the use of content recognition technologies.

Three-way negotiations between the Commission, Parliament and Council began in October 2018 to find final agreement on the legislative proposal. While the Commission has expressed a wish to complete this process by the end of 2018, it is likely to take considerably longer to iron out the differences in the positions of the co-legislators. The new elements added by the Parliament will have to be discussed fully over the coming months. However, the EU institutions will be very conscious that the European Parliament elections are looming in May 2019, so negotiators will be under intense pressure to reach a political agreement before the Parliament's term ends on April 18th 2019.

Commission Recommendation on Measures to Effectively Tackle Illegal Content Online

The publication on September 28th 2017 by the Commission of a Communication about tackling illegal content online generated plenty of controversy. The thrust of the Communication was apparent from its sub-title: "*Towards an enhanced responsibility of online platforms*". The Communication laid down a set of guidelines and principles for online platforms to "step up the fight against illegal content online". From an intermediary perspective, there were concerns over, for example, over-reliance on so-called trusted flaggers; whether sufficient heed was being paid either to variation between laws of different EU countries about what content is illegal or to context; and proactive measures by online platforms (including automated filtering technology) in the context of the Article 15 prohibition on general monitoring duties.

The Communication provided guidance and recognised it did not change the legal framework or contain legally binding rules. However, it was described as a first step.

In March 2018, the second step was taken, when the Commission issued a Recommendation on Measures to Effectively Tackle Illegal Content Online. This largely followed the Communication, apart from certain additional provisions regarding terrorist content (where stronger measures apply). This includes assessment and, where appropriate, removal within one hour of receiving notification from competent national authorities or Europol.

The Communication set up the possibility of legislative action in this area. Consistent with this, the intention is to monitor the Recommendation within three months as regards terrorist content and after six months as regards other illegal content. On September 12th the Commission announced a proposed new Regulation regarding the rapid removal of online terrorist content (but not at this stage other forms of unlawful content).

Conclusion

This time last year, the combination of the Commission's September 2017 Communication and the proposed Article 13 of the draft Copyright Directive led some to conclude that Europe was indeed moving away from protecting internet intermediaries. The Communication has now been backed up by the March 2018 Commission Recommendation and proposed new Regulation (with its focus on terrorist content). Whether Article 13 is ever enacted and in what form is still to be decided, but it is closer to adoption now than before the vote in September 2018. Meanwhile, we await answers from the CJEU regarding the permissible subject-matter breadth and territorial width of injunctions made against intermediaries.

4. Patents

Unwired Planet v Huawei (with thanks to my partners Richard Vary and Jane Mutimear)

The Court of Appeal judgment in the *Unwired Planet v Huawei* case was handed down on 23 October 2018. We previously reported on [the first instance judgment from April 2017\[1\]](#) and the subsequent decision dealing with [confidentiality in that judgment\[2\]](#). The Court of Appeal (the bench consisting of Lord Justice Kitchin (now Lord Kitchin since his elevation last month to the Supreme Court), Lord Justice Floyd, Lady Justice Asplin) handed down a 291 paragraph, 66 page judgment dealing with Huawei's appeal and Unwired Planet's cross-appeal against Birss J's findings Huawei would be subject to an injunction in the UK unless they entered into a global licence on the terms the Court had determined to be FRAND (which was stayed pending appeal). This has been coined a "FRAND injunction".

Lord Kitchin gave the judgment, which he explained was contributed to by the other two judges, in which the appeals were dismissed upholding the first instance Judge on all substantive points on appeal.

Global licence v national and one FRAND rate

Birss J had found that there was only one set of FRAND terms and that a global licence was FRAND. The rates that the Judge had determined were not challenged on appeal, but the global nature of the FRAND licence was challenged.

Huawei claimed that the imposition of a global licence on terms set by a national court based on a national finding of infringement is wrong in principle. For example, in this case it led to a licence where 64% of the money to be paid relates to Chinese patents owned by the second Defendant, UP LLC. UP LLC is a company which owns no UK patents. The English court had, in effect, set rates for a portfolio for which a large part had no enforceable English patent.

Huawei also argued that the judge had settled this licence notwithstanding the facts that (a) there was ongoing patent litigation in relation to corresponding patents in Germany and in China, and (b) there were some countries where UP had no relevant patents at all.

The Court of Appeal recognised that it may be wholly impractical for a SEP owner to seek to negotiate a licence of its patent rights country by country, just as it may be prohibitively expensive for it to seek to enforce those rights by litigating in each country in which they subsist. This suggests that a global licence between a SEP owner and an implementer may be FRAND. The Court of Appeal considered the various cases internationally which have touched on this issue. Huawei relied upon the European Commission's decision in *Motorola*[3], in which the Commission decided that Apple's offer of a German-only licence was FRAND. The Court also considered two German cases (*Pioneer v Acer*[4] and *St Lawrence v Vodafone*[5]), where the German courts had found that a global licence was FRAND. The Court also reviewed cases from the US, China and Japan, which it found did not assist it in relation to this issue.

The Court of Appeal agreed with the Judge's finding that a global licence was FRAND. It commented that this did not mean that the Judge had been adjudicating on issues of infringement or validity concerning any foreign SEPs: he was simply determining the terms of the licence that UP was required to offer to Huawei pursuant to its undertaking to ETSI. It was then up to Huawei whether to take the licence. It could not be compelled to do so and if it chose not to, the only relief available to UP would be relief for infringement of the two UK SEPs the first instance Judge had found to be valid and essential.

The Court of Appeal came to a different conclusion to the Judge regarding there being only one set of FRAND terms for any given set of circumstances, but found that this had no material effect on the Judge's conclusion. They considered it unreal to suggest that two parties, acting fairly and reasonably, will necessarily arrive at precisely the same set of licence terms as two other parties. This is likely to be welcomed as most people had struggled to interpret the Judge's one set of terms position in a way which fitted in with commercial arms' length negotiations of complex licences. In its discussion of this topic the Court of Appeal appears to have answered another often ventilated concern – if the SEP owners' offer is FRAND but the potential licensee's lower counteroffer is also FRAND, which prevails? The Court of Appeal commented that if both a global and national licence were FRAND, it would be open to the SEP owner to offer a global licence and then it would be a matter for the prospective licensee whether to accept it, suggesting that it is for the SEP owner to choose between the range of FRAND terms available to it.

Hard-edged FRAND?

Huawei argued that the Non-Discriminatory part of FRAND meant that the rates for similarly positioned licensees should be the same across the industry. Co-defendant Samsung had settled shortly before trial, when Unwired Planet was cash-strapped. It had paid a lower rate. Huawei argued that it would be discriminatory if they had to pay more than Samsung.

At first instance, Birss J found that the non-discrimination limb of FRAND does not consist of what he termed a “hard edged” component. A licensee may not demand a lower rate than the benchmark “fair and reasonable” rate solely because that lower rate had once been given to a different but similarly situated licensee. He also held that if FRAND does include such a component, then that obligation would only apply if the difference would distort competition between the two licensees, and there was no evidence that Huawei was suffering from a distortion in the market in handsets as against Samsung.

The Court of Appeal agreed with Birss J that the “Non-discrimination” aspect of FRAND was not hard-edged. It accepted Unwired Planet's submission that differential pricing is not per se objectionable, and felt that an effects-based approach to non-discrimination was appropriate. But, once the “hold-up” problem inherent in standardisation had been addressed by ensuring that the licence is available at a rate which does not exceed a fair and reasonable rate, it is difficult to see any purpose in preventing the patentee from charging less than the licence is worth if it chooses to do so.

In contrast, the Court of Appeal held that a hard-edged non-discrimination rule has the potential to harm the technological development of standards if it has the effect of compelling the SEP owner to accept a level of compensation for the use of its invention which does not reflect the value of the licensed technology. The Court accepted that whilst a patent owner may prefer to license its technology for a return which is commensurate with the value of the portfolio, such an approach is not always commercially possible. It felt that the undertaking should be construed in a way which strikes a proper balance between a fair return to the SEP owner and universal access to the technology without threat of injunction. It found that a hard-edged approach is excessively strict, and fails to achieve that balance.

It also noted that the “hard-edged” interpretation would be akin to the re-insertion of a “most favoured licensee” clause in the FRAND undertaking. This had been considered and rejected by ETSI.

Huawei had argued that this would limit the impact of the non-discrimination limb of the undertaking: if it is enough that the rate is fair and reasonable, why would the policy need to specify “non-discriminatory”? But the court found that a hard-edged approach would give

unwarranted primacy to that limb, in that a licence granted at a lower rate, no matter how low, would always trump the benchmark fair and reasonable rate.

The Court did not go on to consider whether the "non-discrimination obligation" would only apply if the difference would distort competition between the two licensees. This would only have been necessary if it had found that the non-discrimination requirement was hard-edged.

The court did not consider the cases of other courts in great detail because none were found to exactly address the issue it had to decide. It noted that Judge Selva in *TCL v Ericsson*[6] rejected the notion that a requirement for competitive harm should be grafted on to the non-discrimination obligation, but the Californian court was not asked to address the "hard-edged" argument presented to the English appeal court.

Did Unwired Planet need to first comply with the *Huawei v ZTE*[7] steps?

Unwired Planet challenged Birss J's assumption that it held a dominant position (which would be necessary for *Huawei v ZTE*[8] to apply). The Court of Appeal dismissed that challenge.

However, the Court found that in *Huawei v ZTE* the CJEU was not laying down specific mandatory conditions which must be satisfied before proceedings seeking injunctive relief are issued. The CJEU's decision expresses the steps outlined as providing a safe harbour for the SEP owner. But it does not follow that being outside the safe harbour is automatically an abuse. In Unwired Planet's case, although it had not followed those steps, there was contact between the parties before the proceedings were issued. At the moment before proceedings were issued, Huawei had sufficient notice that UP held particular SEPs and it knew or ought to have known that if these SEPs were truly essential and valid then a licence was required. It also knew that UP wished to agree a licence with it. This was sufficient to avoid an abuse of dominance: Unwired Planet was not refusing to license its SEPs.

The Court of Appeal noted that the German courts had also not regarded the *Huawei v ZTE* steps as being mandatory before commencing litigation, noting in particular *Pioneer v Acer*[9], *Sisvel v Haier*[10] and *St Lawrence v Vodafone*[11]. (The *IP Bridge v HTC*[12] decision had not been handed down before the hearing in this appeal and is not addressed).

The case is also a "transitional case": the litigation started before the CJEU gave its decision in *Huawei v ZTE*. It would be unfair if UP were to be found to have conducted itself abusively in failing to comply with requirements identified by the CJEU only at a later date.

The Court of Appeal therefore agreed with Birss J that this did not give Huawei an automatic defence and was not an abuse of Unwired Planet's dominant position.

In relation to costs, the Court of Appeal awarded Unwired Planet 90% of its costs of the appeal, to be assessed if not agreed. It ordered that Huawei make an interim payment of £612,612 within 14 days of the sealed Order and refused permission to appeal to the Supreme Court.

Comment:

This decision will be warmly welcomed by SEP owners. The Court of Appeal noted: "*Just as implementers need protection, so too do the SEP owners. They are entitled to an appropriate reward for carrying out their research and development activities and for engaging with the standardisation process, and they must be able to prevent technology users from free-riding on their innovations. It is therefore important that implementers*

engage constructively in any FRAND negotiation and, where necessary, agree to submit to the outcome of an appropriate FRAND determination". This part of the FRAND contract is often considered by SEP owners to have been overlooked in some of the other recent Court and regulatory decisions.

The Court of Appeal's judgment fully establishes the English Court as a jurisdiction which is willing to tackle FRAND disputes and get involved in the nitty gritty of royalty calculations. Their approval of the "FRAND injunction" approach gives patentees a chance of resolving global disputes where the defendant has sufficient sales in the UK to not want to pull out of the market rather than enter into a licence on terms set by the Court.

This case has taken 4.5 years to reach this conclusion and many millions of pounds worth of legal fees. The *TCL v Ericsson* case has taken a similar amount of time, and is still facing appeal. For the courts to be a viable option for most patentees and potential licensees, they need to find a much quicker and cheaper way to resolve disputes of this nature. A typical licence in the SEP field often has a 5 year term. A solution which takes nearly 5 years to determine the licence fee is unworkable. With the precedent set by this case, we believe that the English Courts will now be in a position to push cases forward in a streamlined manner so that trials can take place within a year, with reasonable costs levels. In two recent arbitrations the ICC has determined SEP portfolio rates inside two years. The English courts have also demonstrated that they can move quickly in the Copyright Tribunal, and when determining rents in business tenancies, both of which can include equally complex issues and large numbers of comparables. It should be possible now to achieve this in relation to patent licensing.

[1] <https://www.twobirds.com/en/news/articles/2017/uk/unwired-planet-v-huawei-english-high-court-sets-frand-royalty-rate>

[2] <https://www.twobirds.com/en/news/articles/2017/uk/uk-high-court-releases-final-public-version-of-the-unwired-planet-v-huawei-judgment>

[3] Case AT.39985

[4] 7 O 96/14

[5] 4a 073/14

[6] https://www.twobirds.com/~/_media/pdfs/supersize-this-unwired-planet-american-style.pdf?la=en

[7] Case C-170/13 *Huawei v ZTE* [2015] Bus LR 1261

[8] <https://www.twobirds.com/en/news/articles/2015/global/cjeu-rules-on-huawei-zte>

[9] 2016 6 U 55/16

[10] 66/15 OLG Dusseldorf, 15 March 2017

[11] 1-15 U 36/16

[12] <https://www.juve.de/nachrichten/verfahren/2018/10/sep-streit-ip-bridge-und-htc-gehen-mit-remis-in-die-naechste-runde>

***Actavis v Eli Lilly* – Summary of Supreme Court Decision of 12 July 2017** (with thanks to my partner Mark Hilton)

In July 2017 the United Kingdom Supreme Court (UKSC) handed down its judgment in the case of *Actavis UK Limited and others v Eli Lilly and Company* ([2017] UKSC 48) that has significantly changed the law of patent infringement in the UK.

Background

Lilly is the proprietor of a patent that claims the use of pemetrexed disodium in the manufacture of a medicament for use in combination with vitamin B12 (and, optionally, folic acid) for the treatment of cancer. Actavis sought declarations of non-infringement for its proposed products which used (i) pemetrexed diacid, (ii) pemetrexed ditromethamine, or (iii) pemetrexed dipotassium in place of pemetrexed disodium. Actavis sought such declaration in respect of the UK, French, Spanish and Italian designations of Lilly's patent. The ability of the English courts to grant such declarations in respect of the foreign designations had been confirmed earlier in this action.

The High Court held that none of the Actavis products would directly or indirectly infringe the patent in the UK, France, Italy and Spain. The Court of Appeal allowed Lilly's appeal in respect of there being indirect infringement of the patent in each jurisdiction. Both parties were given permission to appeal to the UKSC.

Judgment

The UKSC concluded that as a matter of ordinary language, it is clear that the only type of pemetrexed compound to which the patent claims expressly extends is pemetrexed disodium. The question that the UKSC then had to consider was how far one can go outside the wording of a claim.

The UKSC reviewed the relevant case law of the UK and other Convention states. In relation to the UK, those cases were the well-known cases of *Catnic*, *Improver* and *Kirin-Amgen* and the *Improver/Protocol* questions that arose from those cases. The UKSC has stated that the problem of infringement is best approached by addressing the following two issues:

1. Does the variant infringe any of the claims as a matter of normal interpretation; and, if not,
2. Does the variant nonetheless infringe because it varies from the invention in a way or ways which is or are immaterial?

If the answer to either of those questions is "yes" then there is infringement, otherwise there is not. The decision states that issue 1 self-evidently raises a question of interpretation, whereas issue 2 raises a question which would normally have to be answered by reference to the facts and expert evidence. The UKSC then criticises the approach taken in *Catnic*, *Improver* and *Kirin-Amgen* for effectively conflating the two issues and indicates that characterising the issue as a single question of interpretation is wrong in principle.

The UKSC went on to explain that treating issue 2 as one of interpretation will lead to a risk of wrong results in patent infringement cases and it will also lead to a risk of confusing the law relating to interpretation of documents. Accordingly, issue 2 is said to involve not merely identifying what the words in the claim would mean in their context to the notional addressee, but also considering the extent, if any, to which the scope of protection afforded by the claim should extend beyond that meaning.

Applying this new approach to the facts of this case, the UKSC confirmed that, in relation to the first issue, there was no doubt that the Actavis products do not infringe the patent as in no sensible way can pemetrexed diacid, pemetrexed ditromethamine or pemetrexed dipotassium be said to fall within the expression "pemetrexed disodium". However, it is the second issue that posed more difficulties of principle to the UKSC namely, what is it that makes a variation "immaterial"? While acknowledging that the Improver questions provided helpful assistance in answering that question, the UKSC has undertaken a critical explanation of questions 1 and 3 but has also reformulated question 2.

In relation to the first *Improver* question, the UKSC has now said that the emphasis of that question on how "the invention" works should involve the court focussing on "the problem underlying the invention", "the inventive core" or "the inventive concept". Terms such as this will be familiar to practitioners in other jurisdictions.

The UKSC found the second *Improver* question more problematic. Its view is that it places too high a burden on the patentee to ask whether it would have been obvious that the variant had no material effect on the way the invention works, given that it requires the addressee to figure out for himself whether the variant would work. To overcome this problem, the UKSC has determined that this question should be asked on the assumption that the notional addressee knows that the variant works. This new question should also apply to variants which rely on, or are based on, developments which have occurred since the priority date, even though the notional addressee is treated as considering the second question as at the priority date.

In relation to the third *Improver* question, the UKSC was satisfied with that question as long as it was properly applied. The court makes four points in relation to that. First, the "language of the claim" does not exclude the specification and all the knowledge and expertise which the notional addressee is assumed to have. Second, the fact that the language of the claim does not on any sensible reading cover the variant is not enough to justify holding that the patentee does not satisfy the third question. Third, it is appropriate to ask whether the component at issue is an "essential" part of the invention, but that is not the same thing as asking if it is an "essential" part of the overall product or process of which the inventive concept is a part. Fourth, when considering a variant which would have been obvious at the date of infringement rather than at the priority date, it is necessary to imbue the notional addressee with rather more information than he might have had at the priority date.

In an attempt to assist with interpreting their judgment, the UKSC expressed their new questions as follows:

- Notwithstanding that it is not within the literal meaning of the relevant claim(s) of the patent, does the variant achieve substantially the same result in substantially the same way as the invention, i.e. the inventive concept revealed by the patent?
- Would it be obvious to the person skilled in the art, reading the patent at the priority date, but knowing that the variant achieves substantially the same result as the invention, that it does so in substantially the same way as the invention?
- Would such a reader of the patent have concluded that the patentee nonetheless intended that strict compliance with the literal meaning of the relevant claim(s) of the patent was an essential requirement of the invention?

The impact of these new questions and the new approach to assessing infringement of patents in the UK (and the consequences for the validity of those patents) will take time to become fully appreciated.

Prosecution History

The UKSC was also asked to consider the use of the prosecution file when considering the question of interpretation or infringement. It concluded that its current view was that such reference to the file would only be appropriate where (a) the point at issue is truly unclear if one confines oneself to the specification and claims of the patent, and the contents of the file unambiguously resolve the point, or (b) it would be contrary to the public interest for the contents of the file to be ignored.

In the present case, the UKSC did not consider that the file justified departing from its conclusion that the Actavis products infringed Lilly's patent.

Further reading: International Comparative Legal Guide to Patents 2019: Actavis v Lilly - A year after the revolution (with thanks to my partner Katharine Stephens)

<https://www.twobirds.com/~media/pdfs/news/articles/2018/actavis-v-lilly--a-year-after-the-revolution.pdf?la=en>

5. Expected Impact of Brexit

(HEALTH WARNING: THESE MATERIALS WERE PRODUCED IN EARLY NOVEMBER 2018 TO MEET PRINT DEADLINES. THE POSITION WILL HAVE MOVED ON BY JANUARY 2019. I WILL GIVE AN OVERVIEW OF THE LATEST POSITION IN THE ORAL SESSION)

Brexit: English Intellectual Property law implications (with thanks to my partner Sally Shorthose)

The UK Government served formal notice under Article 50 of The Treaty on European Union to terminate the UK's membership of the EU on 29 March 2017 (following the June 2016 UK referendum on EU membership). The EU Treaties will accordingly cease to apply to the UK and the UK exit will take effect on 29th March 2019. If a Withdrawal Agreement is agreed by the UK and EU and is approved by the UK Parliament, this will include provisions for a transitional or "implementation" period to the end of 2020, during which EU law will continue to apply in the UK. Any Withdrawal Agreement is expected to include an outline of a future UK/EU relationship agreement, in the form of a political declaration, to be negotiated during the transitional period. If no Withdrawal Agreement is concluded, i.e. in a "no deal" or "hard Brexit" scenario, EU law will cease to apply in and to the UK on 29 March 2019.

This briefing note advises readers on the immediate considerations and anticipates how a Brexit will impact on the IP/IT market which has been governed by so many EU Regulations and Directives in the past (albeit not exclusively) that intricately bound the UK to the EU. For the purposes of this note, we are assuming that following Brexit the "Norway model" (i.e. EEA membership) will not be applied to the UK and that the UK will be outside the single market.

- [Relationship with EU law](#)
- [Implications of the Brexit](#)
- [The unitary patent system](#)
- [Community rights](#)
- [Life Science regulation](#)
- [European Digital Single Market](#)
- [Conclusion](#)

Relationship with EU law

IP laws are harmonised to a large extent across Europe, and much of the UK legislative framework in this field is currently composed of directly effective EU Regulations and transposed EU Directives. Unless those EU Regulations relevant to IP and life sciences (especially pharmaceuticals) are transposed into English or Scottish law, a regulatory vacuum may be created.

The European Union Withdrawal Act 2018 ("the EU Withdrawal Act") will repeal the European Communities Act 1972 ("ECA 1972") as from Brexit (or from the end of the transitional agreement if a Withdrawal Agreement is concluded) and will also include provisions to convert the existing body of currently directly applicable EU law into domestic UK law, by means of statutory instruments. This will mainly apply to EU Regulations which

would otherwise cease to apply on Brexit, and also to statutory instruments implementing EU Directives, where the statutory instruments were adopted pursuant to the ECA 1972 and would otherwise fall away on repeal of that Act.

MPs would then go through each law on a piecemeal basis and amend or repeal them as necessary based upon national interests. This would facilitate a smooth transition with all EU laws, including the relevant IP Regulations and Directives remaining in force. However, the UK would no longer be a member of the EU, which would affect the unitary character afforded to IP rights. The UK will have to negotiate an agreement with the EU to address this, but for now, until the UK actually leaves the EU, UK rights holders can continue to enforce their IP in the EU.

In a speech on the Brexit process in January 2017, Prime Minister Theresa May indicated that:

- The UK will not remain a member of the EU single market or Customs Union but would instead seek to negotiate separate trade and customs agreements with the EU, including the greatest possible access to the single market on a reciprocal basis.
- The UK would look to negotiate new trade deals with other international countries that are not EU member states.
- Guaranteeing the rights of EU nationals living in the UK is a priority, but that not every other EU member state favours such an agreement.
- Controls will be introduced on immigration from the EU (removing the existing freedom of movement for EU nationals).

However, in light of the above, the implications of Brexit are still very uncertain and will, to a large extent, be determined by the terms of any international agreements negotiated and by the amendments and repeals of EU laws following the EU Withdrawal Act.

Implications of the Brexit

Some implications of Brexit will apply to organisations in the same way whether they are based in the UK, in the EU or elsewhere in the world. For example, the changes to unitary patents are pertinent to any company seeking pan-European patent coverage, whereas the now likely exclusion of the UK from the European Digital Single Market, will be more acutely felt in the UK. Below is a summary of some of the main implications.

UPC

The new EU patent regime is intended to provide patentees with the option to apply for a single pan-EU Unitary Patent (UP) covering most of the EU. It would also create the Unified Patent Court (UPC) to hear and determine patent disputes on an EU-wide basis.

The introduction of the new regime, whose future was already uncertain after the Brexit vote in June 2016, is now further delayed and complicated by the challenges to the regime going through the German courts. The announcement by the UK on 28 November 2016 that it will proceed to the ratification of the UPC Agreement is of questionable relevance given the effluxion of time. Further analysis on this is found [here](#).

Community rights

There is a potential that community rights, such as registered and unregistered community designs and EU trade marks (previously community trade marks), will no longer have effect

in the UK. In order to address this, the current draft of the withdrawal agreement currently being negotiated between the UK and the EU aims to ensure community rights will automatically convert into analogous UK rights upon Brexit. In addition, regardless of whether a final agreement is reached, the UK Government has confirmed that its aim is to "ensure the continuity of protection" and to "avoid the loss" of existing rights.

Concurrently, it has also been confirmed that the UK intends to create and grant 1.7 million automatic and free-of-charge intellectual property rights (including trade marks) corresponding to existing EU-wide rights. Note however that this is subject to the agreement of the Withdrawal Agreement, and as such the government has stopped short of providing a guarantee of free-of-charge IP rights without an agreement with the EU.

Ultimately the scope of any community rights applied for post Brexit will not include the UK, and it remains to be seen precisely what will happen to the "UK portion" of such rights if they were obtained before Brexit. If agreement is not reached, or if the UK Government does not follow through on its promise to ensure continuity of protection, the rights in question will be automatically reduced in geographical scope and their value will diminish, especially given the economic significance of the UK, which could result in the right-holder losing out commercially. Any organisations which rely on community rights will now need swiftly to respond to changes in this area.

Life Science regulation

The UK's various Life Sciences regulatory regimes are currently intimately connected with the EU; the European Medicines Agency was based in London and a sophisticated and comprehensive pharmacovigilance system has been established around this regime. Whilst change will, no doubt, be managed to enable a smooth transition, organisations working in this sector will need to be ready to adapt now that the regulatory framework is likely to be reshaped; a "soft Brexit" involving continued affiliation with the current system was rejected by the government so this area is particularly uncertain. The Netherlands won the competition to host the EMA post-Brexit. In October MHRA published its proposals for a life sciences regulatory framework after Brexit. The proposals can be found at <https://consultations.dh.gov.uk/mhra/mhra-no-deal-contingency-legislation-for-the-regul/>

European Digital Single Market

There is a real risk that the UK will be shut off from operating in the European Digital Single Market. The drive behind the single digital market was to promote common data protection laws, provide better access to products and services at reduced costs, and generally increase adoption and acceptance of digital services. There are significant differences in the attitudes of different European countries towards the use of social and digital media marketing and, in the absence of the UK within the EU, these differences are now likely to widen and the influence of the UK will be minimal.

Conclusion

Brexit is not going to be a simple divorce. Now any UK legislation, which has hitherto been dependent on EU legislation, will have to be unpicked (see above for reference to the Withdrawal Bill). Beyond this, the key development in the IP field is the likely exclusion of the UK from pan-European rights systems (notwithstanding the government statement that the UK will ratify the UPC). Separation presents the opportunity for the UK's laws to diverge from those of Europe, and such separation may be embraced in some areas. However, in IP, this is unlikely to happen to any significant extent given the interconnection of trade and the universal recognition that harmonisation is beneficial. Going forwards, the UK is no longer going to be able to assert the same influence on EU policy, which may undermine the

position of UK-based IP and IT companies both within Europe and on the world stage (especially vis-à-vis the USA as the UK may be seen as second class without a voice in Europe) and make it a little more difficult to compete.

Given the uncertainty about what the exact Brexit environment will comprise, the long term future is still unclear. Thereafter, IP owners should identify which of their rights are now likely to be affected and may need further application/registration in order to achieve maximum protection over that right.

Brexit: Trade mark licensing implications

This bulletin discusses the implications of Brexit on licensing EU Trade Marks (EUTMs). The bulletin very briefly considers what will happen to EUTMs in the UK after Brexit, before turning to implications for EUTM licences.

Once Brexit takes effect, how will unitary EU-wide registered IP rights, such as EUTMs, be addressed with regard to the UK, and what implications are there for EUTM licences? For the purposes of this note, we are assuming that following Brexit the "Norway model" (i.e. EEA membership) will not be applied to the UK and that the UK will be outside the single market.

Will my EUTM still cover the UK?

The answer is no. However, a new UK trade mark will be created out of the existing EUTM, to cover the UK territory. This appears to be going to happen whether or not a Brexit deal is done. The UK Government recently set out its position regarding a "no deal" Brexit, stating that its aim is to ensure continuity of protection for EUTM owners and to avoid the loss of currently held rights. Accordingly all existing EUTM holders will be granted an equivalent trade mark registered in the UK. In respect of pending EUTM applications, applicants will have a grace period of 9 months to apply in the UK for the same mark to retain the priority date of the original EUTM application.

What about EUTM licences?

Of equal concern to licensors and licensees is what will happen to existing EUTM licences after Brexit, where the licensed territory includes the UK. Will the UK continue to be covered by the licence?

The question will be easy enough to answer where wording is used such as "*the EU as constituted from time to time*" (on the one hand), or "*as constituted at the date of this Agreement*" (on the other). Where no such wording is used, the answer is likely to depend on the factual background to the licence (assuming it is governed by English law), meaning it requires case by case analysis. Was the "EU" simply being used as convenient shorthand for a list of countries, so the UK would continue to be in scope? Or was the terminology used because it had certain factual or legislative implications on the subject matter of the contract?

Relevant factors might include whether, for example:

- any national rights (registered or unregistered) are included in the licence alongside the EUTMs;
- the EU territory was chosen because it is a single market, with ability to protect against unauthorised imports from outside but not to prevent parallel trade of authorised goods within;

- there are legal or regulatory reasons why the licensee needs to be located in an EU Member State.

Assuming parties are in agreement, they would be advised to amend existing licences to ensure it is clear whether the UK will remain part of the licensed territory after Brexit, and at the same time to clarify the position with regard to future EU joiners/leavers. The same is true for licences currently under (re-)negotiation.

If the correct interpretation is that the UK remains part of the licensed territory, there is a second question about whether the new UKTM right deriving from the EUTM is automatically included in the existing licence without the need to amend the licence. This is a matter which might be provided for in any transitional legislation which sets out how the Brexit "gap filling" UKTMs are created in the first place. Failing that, the answer is again likely to depend on the factual background to the licence (assuming it is governed by English law), meaning it again requires case by case analysis.

Assume that the UK 'portion' of an EUTM will be converted into a UKTM registration (e.g. with the same filing, publication and registration dates as the EUTM). The right being licensed in the scenario contemplated above is likely then to either: (1) change altogether from an EUTM to a UKTM (where the territory is the UK only), or (2) be expanded to include a UKTM (for the UK part of the licensed territory), alongside the existing EUTM (for the EU part of the licensed territory).

This means that the legal rules governing the UK portion of the licence will change. This is because the licensing of UKTMs is governed by sections 28 to 31 of the Trade Marks Act 1994, whereas the licensing of EUTMs is governed by Articles 22 and 23 of the EUTM Regulation. Until recently, this risked creating material divergences between a licensee's rights under the EUTM and under the UKTM portions of the licence (described fully in an earlier version of this bulletin). However, the recently enacted UK legislation implementing the new Trade Mark Directive (Directive 2015/2436) will now align the regimes, so that is no longer relevant.

However, licensees in particular should note that a licence of a UKTM is only effective against a third party acquiring a conflicting interest (such as a party buying the UKTM, or a subsequent licensee whose rights conflict) if it has been registered at the UK IPO. The rights of an exclusive licensee to enforce the UKTM in its own name are also contingent on the licence having first been registered at the UK IPO.

As a result, absent specific transitional provisions directed at this, a licensee of an EUTM licence whose territory includes the UK should seek to register the licence at the UK IPO as soon as the new UKTM deriving from the EUTM comes into existence. This will be the case even if the EUTM licence has previously been registered at the EU IPO. It costs £50 to register the licence against the relevant UKTM with the UK IPO, and this can be done without the licensor's involvement if the licensee supplies a copy of the licence. Of course, there remains a question over how the UK IPO will respond after Brexit to requests to register what is on the face of it an EUTM licence against a UKTM which is not expressly listed as one of the licensed marks, something on which the "no deal" technical notice concerning trade mark registrations is silent.

Bird & Bird & Developments in European IP Law & Expected Impact of Brexit

Nick Aries
Partner
Bird & Bird (San Francisco Representative Office)



Slide 2

Bird & Bird

Developments in European IP Law & Expected Impact of Brexit

Overview

1. Trademarks online: Who has jurisdiction over websites?
2. Trademark recitations – open questions
3. EU copyright reform and platform liability
4. Patents: *very* briefly
5. Expected Impact of Brexit

Slide 3

Bird & Bird

Trademarks online: Jurisdiction over websites

Slide 4

Bird & Bird

Where can TM owner sue (PART 1)

- Q: When is trademark use online actionable in a given country in Europe?
- A: When the use "targets" consumers in that country. Accessibility not enough.
- *Merck KGaA, Darmstadt, Germany v Merck Sharp & Dohme Corp, Merck & Co Inc*
- Factors: language/currency, delivery countries, testimonials, use of local paid search, use of cctld, appearance and content of site
- Site traffic and structure of website
- Factors beyond website: nature/size of business, type of goods/services
- Role of intention

Slide 5

Bird & Bird

Where can TM owner sue (PART 2)

- Q: Which court has jurisdiction over EUTM claim?
 - Member State where Defendant domiciled or established, *failing which*
 - MS where Plaintiff domiciled or established, *failing which*
 - Spain, *BUT ALSO*
 - MS where infringing act committed (can only get relief in that MS)
- Where did the infringer perform the active conduct?
- How does that work with websites offering and selling goods? DE BGH and UK HC say location of website operator.
- *AMS v Heritage Audio* – Waiting for CJEU to decide.

Slide 6

Bird & Bird

Trademark recitations – open questions

Slide 7

Bird & Bird

Trademark recitations – permissible breadth

Sky v Skykick

- Can an EUTM be partially invalidated on the basis parts of its recitation lacked clarity or precision?
- E.g. computer software; telecommunications services; etc
- Can it constitute bad faith to apply to register a trade mark without any intention to use it in relation to the specified goods or services?
- What is the effect of having an intention to use in respect of some but not other goods/services?

Slide 8

Bird & Bird

EU Copyright Reform and platform liability

Slide 9

Bird & Bird

Article 11

- Facilitating enforcement by EU publishers v ISPs
- 'Link tax'?
- Big questions:
 - How to define 'press publication'?
 - How much use = infringement?
- Missed opportunity to harmonise



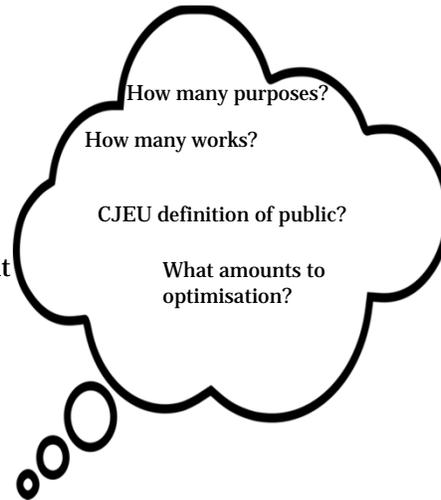
Slide 10

Bird & Bird

Article 13

"Online content sharing service provider"

- *One of* main purposes
- Store and give access
- To the public
- A significant amount of works
- Uploaded by users
- Optimised and promoted for profit



Slide 11

Bird & Bird

Some things beyond doubt?

- OCSSPs *perform* acts of communication
- They *shall*:
 - conclude licensing agreements
 - not make unauthorised works available
 - put in place effective and expeditious redress mechanisms
- *Not* OCSSPs:
 - Micro and SSEs
 - Online marketplaces of physical goods

Slide 12

Bird & Bird

What next?



Slide 13

Bird & Bird

What is the state of play?

Q4 2018/Q1 2019

- Trilogue negotiations to finalise text (aiming for pre-xmas)

Q2 2019

- Directive passed and published

2019/2020

- Consultation/negotiations in Member States re implementation

Q2 2021

- Deadline for implementation

Brexit?

Slide 14

Bird & Bird

Patents

Slide 15

Bird & Bird

FRAND/SEP disputes, new UK test and the UPC

- **FRAND/SEP disputes**
 - *Unwired Planet v Huawei*
 - "FRAND injunction": Huawei subject to injunction in the UK unless they entered into a global licence on the terms the Court had determined to be FRAND
- **New, broader infringement test in UK**
 - *Actavis v Lilly*
- **UPC** (Unitary Patent and Unified Patent Court)
 - *Hmmmm.*

Slide 16

Bird & Bird

Expected Impact of Brexit

Slide 17

Bird & Bird

Brexit and IP



Patents

- No impact (outside UPC issue)

Trade Secrets

- No impact

Copyright

- Reciprocity gaps?

Registered EU Trademarks and Designs

- Registrations, Applications, Licensing, Litigation, Exhaustion, Customs, Representation

Slide 18

Bird & Bird

Brexit and trademarks: protection



- UK registrations – not affected in any way
- But EUTMs will cease to cover the UK on Brexit
- The UK government won't allow that protection to be lost, so existing EUTM protection will be maintained in the UK
- All EUTMs are automatically converted into UK registrations at the point of Brexit
- Nine month period to file UK claiming filing date of EUTM that is pending at point of Brexit

Page 19

Bird & Bird

Brexit and trademarks: losing rights?



- Need to use trademarks to maintain registrations
- If only operate in UK, won't be able to defend EUTM rights – when will this take effect?
- If only operate outside UK, won't be able to defend UK rights – again, when this will take effect?
- Will use up to Brexit (or end of transitional period) count, so effectively the 5 year periods start from then for both UK and EUTM rights?

Page 20

Bird & Bird

Brexit and trademarks: licensing



Territory

- Does licence cover the EU "*as constituted from time to time*" or "*as at the date of the agreement*"?
- If the former, need to amend licence to cover UK – chance to renegotiate terms

Licensed rights

- Are extended UK rights included in the licence?
- Assuming yes, implications for enforcement (exclusive licensee can sue – if licence recorded) and maintenance of rights (what if no use in the UK?)

Page 21

Bird & Bird

Brexit and trademarks: enforcement implications



- UK Court will cease to be an EUTM Court
- What will happen to on-going trade mark infringement proceedings seeking EU-wide relief at Brexit?
 - In UK Courts?
 - In EUTM Courts in other Member States?
- What about existing injunctions granted by UK Courts?
- And EU-wide injunctions granted by non-UK Courts?
- Need to bring UK-specific actions – so increase in litigation?

Page 22

Bird & Bird

Brexit and trademarks: exhaustion, customs, representation



Exhaustion

- At present EU-wide exhaustion
- Will we have national, regional or international exhaustion post Brexit?

Customs enforcement of IPRs

- Commission notice 4 June 2018
- Notices (1) based on EU rights and (2) filed through UK Customs will cease to have effect not just in UK, but in EU 27
- Companies will need to refile in UK and in an EU member state

Representation

- Need to be admitted and have a place of business in EEA member state

Page 23

Bird & Bird

Brexit and trademarks: so what do we do now?



- Filing strategy
 - Register valuable trade marks in the UK?
 - File both EUTM and UK for new marks?
- File new Customs notices in UK and another EU member state
- Licensing audit and strategy
 - Consider amending existing licences
 - Draft new licences carefully
 - Review co-existence agreements

Page 24

Bird & Bird

Thank you & Bird & Bird

Nick Aries

e: nick.aries@twobirds.com

m: 415 231-6568



twobirds.com

Bird & Bird is an international legal practice comprising Bird & Bird LLP and its affiliated and associated businesses.

Bird & Bird LLP is a limited liability partnership, registered in England and Wales with registered number OC340318 and is authorised and regulated by the Solicitors Regulation Authority. Its registered office and principal place of business is at 12 New Fetter Lane, London EC4A 1JP. A list of members of Bird & Bird LLP and of any non-members who are designated as partners, and of their respective professional qualifications, is open to inspection at that address.

SECTION 11

BONUS PLENARY SESSION

**CTE and Mild Traumatic
Brain Injury: An Update and a
Litigator's Protocol**



Presented by

Larry J. Cohen, Ph.D., J.D.

Cohen's Counsel

Bethel, VT

SECTION 12

The Top Ten Patent Issues to Know About the U.S. Patent and Trademark Office



Presented by

Drew Hirshfeld
Commissioner for Patents
US Patent and Trademark Office
Washington, DC

UNITED STATES
PATENT AND TRADEMARK OFFICE



Drew Hirshfeld
Commissioner for Patents

January 4, 2019
National CLE Conference
Snowmass, Colorado



USPTO Mission

Fostering innovation, competitiveness and job growth in the United States by conducting high quality and timely patent and trademark examination and review proceedings in order to produce reliable and predictable intellectual property rights; guiding intellectual property policy, and improving intellectual property rights protection; and delivering intellectual property information and education worldwide.



3

“ [T]he focus for discussion, and the focus for IP policy, must be on the positive. We must create a new narrative that defines the patent system by the brilliance of inventors, the excitement of invention, and the incredible benefits they bring to society. And it is these benefits that must drive our patent policies.”

A handwritten signature in black ink that reads "Andrei Iancu".

Remarks by USPTO Director Andrei Iancu at U.S. Chamber of Commerce Patent Policy Conference – April 11, 2018



4

USPTO at a Glance (as of Nov 30)

- 12,587 USPTO Employees
- 8,217 Patent Examiners



5

USPTO at a Glance

- Total Patent Pendency: 24 months
(as of Nov. 30)
- Total new serialized filings = 426,943 in
FY '18 (+1.7% over FY'17)



6

USPTO Top Priorities

- Subject Matter Eligibility
- Examiner Search
- PTAB reform

uspto

7

Subject Matter Eligibility

- *Berkheimer* and *Vanda Memos*
(April 19 and June 7)
- Revised Guidance?

uspto

8

Search

- Access to Relevant Prior Art
- Expanded Collaborative Search Pilot (CSP)
- Artificial Intelligence?
- Process changes?

At times, there is a gap between the prior art found during initial examination and the prior art found during litigation. There are many reasons for this, but the main culprits are the ever-accelerating publication and accessibility explosions. These are issues that face every patent office around the world. Indeed, we are ahead of most others on this front. But if we could further narrow this gap in prior art between examination and litigation, then the accuracy of the patent grant – and therefore, its reliability – would increase.

--Director Iancu describes vision for agency at U.S. Chamber of Commerce, April 11, 2018

9

PTAB Reform

- Claim construction standard
- Precedential Opinion Panel (POP)
- Amendment practice

10

On the Horizon

- **Fee Setting (2020–2021)**
 - Proposed Across-the-Board Increase of ~5%
 - Some Exceptions
- **Fee Setting Authority extended to 2026**

uspto

11

On the Horizon

- **Examiner Performance Measures**
 - Examination Time
 - Application Routing
 - Performance Appraisal Plan

uspto

12

Authentication Change: EFS-Web and PAIR

- Switching from PKI certificates to two-factor USPTO.gov account authentication
- Saves time, compliance w/Federal requirements, safer, more compatible with browser
 - More Information:
 - <https://www.uspto.gov/patent/authentication-changes-efs-web-and-pair?MURL=AuthenticationChange>



13

Statistics and Fun Facts

14

Colorado Stats/Facts

- In FY18, 4,145 patents were granted which included at least one inventor from Colorado
 - Comparison of neighboring states for (FY18):
 - Arizona 3,473
 - Nebraska 427
 - Utah 1,851

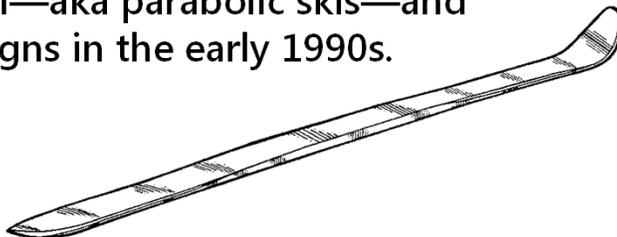
uspto

15

Interesting Stats/Facts

Modern Skis

Skis are ancient inventions; But contemporary skis were pioneered by Elan, which invented the "deep sidecut" ski—aka parabolic skis—and patented several designs in the early 1990s.
USPN D325062



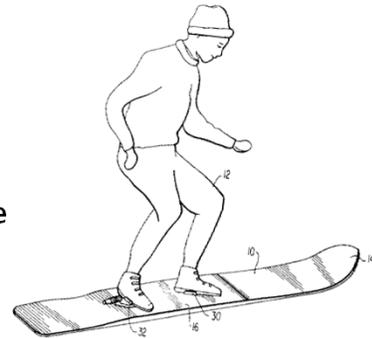
uspto

16

Interesting Stats/Facts

Snowboard

Many point to USPN 3,900,204 for a "mono-ski," awarded to Robert Weber in 1975, as the first registered board. However, there's some dispute about that—in the form of a fascinating 1939 patent from two Illinois swedes named Burgeson, filed long before the advent of the modern snowboard. It's now widely considered the first snowboard patent: USPN 2,181,391.

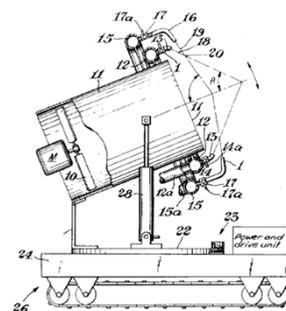


uspto

17

Interesting Stats/Facts

The history of snow makers is surprisingly long, dating back to the late 1920s. However, USPN 4,004,732 —a Method for making and distributing snow—awarded to a Michigan man in 1977, is closer to the tech we use today.

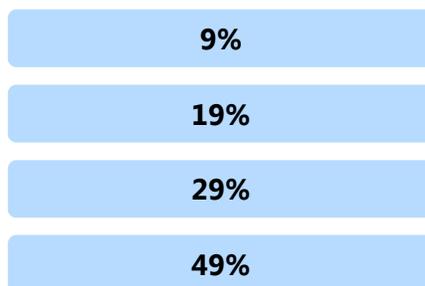


uspto

18

USPTO Stats/Facts

- What percentage of applications had an interview?

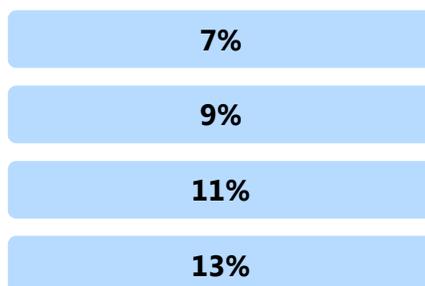


uspto

19

USPTO Stats/Facts

- If an interview takes place, the chance of allowance increases by?



uspto

20

Questions



21

SECTION 13

Building a Strong Patent Portfolio: Views from In-House



Presented by

Steve Mackenzie

Senior Counsel, Intellectual Property and Intellectual
Property Litigation, Koch Companies Public Sector LLC
Wichita, KS

David McKenzie

Associate General Counsel, IP Legal, WD,
a Western Digital Company
San Jose, CA

Cynthia S. Mitchell

Senior Corporate IP Counsel, Zimmer Biomet
Denver, CO

Building a Strong Patent Portfolio – Views from In-House

1

National CLE Conference January 2-6, 2019

- **Panel Moderator**
 - Scott Alter, Partner; Michael Best & Friedrich, LLP
- **Panel Members**
 - Stephen Mackenzie, Sr. IP Counsel; Koch Companies Public Sector LLC
 - David McKenzie, Associate General Counsel, IP; Western Digital Company
 - Cynthia Mitchell, Sr. IP Counsel; Zimmer Biomet, Inc.

Building a Strong Patent Portfolio

2

Existing Portfolio

- Classify the existing patent portfolio
 - Use key words to identify what technologies and/or products each patent covers
 - Helps to efficiently identify patent families for
 - Out or cross licensing
 - Divesting Business Unit, products or technology
 - Offensive/Defensive litigation
 - Rank portfolio
 - highest patents cover strategic products
 - Medium/high patents cover less strategic products
 - Medium/high patents cover what important competitors are doing or need to do to compete
 - Medium patents create picket fence around strategic products
 - Low/medium patents cover less strategic products or company specific solution to problem
- Review the existing patent portfolio to determine if there are patents which do not have offensive or defensive use.
 - Look for sale / license opportunities. If not, abandon.

New Inventions

3

- Embed IP Counsel in R&D for each Business Unit, preferably co-located with the largest group of product design engineers/scientists
- Assign IP member to attend regular strategy meetings and Product Development Phase Gate meetings with Business Unit
- Ensure IP reviews for freedom to operate, invention mining, and trademark assessments are embedded in Product Development Phase Gates
- Hold regular Patent Training Coffee Talks
 - New employee orientation
 - Annual for Business Unit R&D
- Consider Inventor Incentive Awards
 - Helps jump start a small portfolio and overcome antipathy to patents (e.g., software)
- Hold invention harvesting/mining sessions at regular intervals
 - project initiation
 - design freeze
 - pre-commercialization
- Hold brainstorming sessions to pursue strategic inventions covering
 - barriers to entry and picket fences for strategic products
 - important innovations to existing products

Controlling on going Patent Portfolio Costs

4

- Review the existing portfolio to determine if there are patents which do not have offensive or defensive use
 - Look for sale / license opportunities. If not, abandon.
- Consolidate multiple cases or inventions into one case where appropriate
 - Watch out for Divisional or Unity of Invention issues
- Filing process optimizations (these can be tied to invention ranking)
 - Reduce the length of the specifications
 - Reduce the number of claims (e.g., US – 3 indep & 20 total)
 - Reduce number drawings presented
 - Optimize filing countries
 - ✦ business input on key markets for products/inventions covered by patent family
 - ✦ number of countries filed in can be tied to invention ranking
 - ✦ File strategically based upon country approach to invention type (e.g., business method, medical, software, etc.)
 - Look for patent office incentives (e.g. Brazil) or accelerated examination (e.g. PPH).

Controlling on going Patent Portfolio Costs

5

- Review Patent Annuity Payments regularly
 - Stop paying patent annuity fees sometime between years 15-19 or when fees exceed a predetermined amount per country (e.g., \$1000)
 - ✦ Consider making this a default
 - ✦ This can be optimized based upon patent family rankings
 - ✦ Flag any patent families that have ongoing royalties or other reasons/obligations to maintain – to prevent inadvertent lapse of important patent families

Connecting the Business to the Patent Value – Connecting the IP Group to the Business Strategy

6

- Make patent costs transparent to the business leaders and include on their P&L.
 - Don't let the patent costs fall into a "generic" R&D cost center.
- Work with business to match patents to products / processes.
 - Then have business report revenue, NIAT, and/or cost-of-capital-consumed for those products / processes.
- Have members of the IP group attend regular business strategy meetings.
 - The patent strategy should be dynamic and match the business strategy.
 - Look for ways to rely on trademarks or trade secrets to protect the business.
- Challenge the status quo.

Thank You



QUESTIONS?

SECTION 14

The Fast-Changing World of Software-Related Patents: Critical Issues You Need to Know



Presented by

Scott Alter

Michael Best & Friedrich LLP
Denver, CO

Edward R. Tempesta

Vice President – Senior Counsel –
Intellectual Property, Mastercard
New York, NY



Software Patents – Critical Issues from 2018 You Need To Know

For: National CLE Conference - Snowmass
January 4, 2019

Edward Tempesta
edward.tempesta@mastercard.com
T. 914-249-2989

Scott M. Alter
smalter@michaelbest.com
T. 720-745-4869



Agenda (Software Patents)

- Background
- *Berkheimer v. HP*
 - The Decision
 - The Memo (USPTO)
- Revised MPEP Section 2106 (Patent Subject Matter Eligibility)
- Other Pertinent 2018 Court Decisions
 - What Do They Mean For You?
- Observations from the Trenches

Background

Alice v. CLS Bank (S. Ct., June, 2014)

- Recited two-part test from *Mayo v. Prometheus* (from *Parker v. Flook*):
 - 1) Determine whether the claims at issue are “directed” to a patent-ineligible concept, e.g., an “abstract idea”
 - Note: *Alice* Court had just previously stated that, at some level, everything “embodied,” “used,” etc., an abstract idea. . . So apply to every patent?
 - “Directed” different from “embodied, used,” etc.?
 - Claim “smells” like it might preempt an abstract idea? If “yes,” proceed to step 2.
 - 2) Is there an “**inventive concept**”
 - [Sounds like some kind of novelty/non-obviousness requirement, but without the prior art...]

Alice v. CLS Bank (S. Ct., June, 2014)

- “The *Mayo* test” as applied to the claims in *Alice*:
 - Step 1: Are the claims directed to an abstract idea?
 - Cited prior S. Ct cases where the claims were held to be directed to abstract ideas; court then summarily stated that “[i]t follows from our prior cases [] that the claims at issue here are directed to an abstract idea,” i.e., “the concept of intermediated settlement.”
 - No indication was given regarding why it “follows”....
 - **Subject to lots of interpretation!**

***Alice v. CLS Bank* (S. Ct., June, 2014)**

- The claims at issue in *Alice* (Cont.):
 - Step 2: Does the claim “contain[] an ‘**inventive**’ concept’ sufficient to ‘transform’ the claimed abstract idea into a patent-eligible application”?
 - No. the claimed functions at each step, separately, are “purely conventional,” and not “inventive.” Citing *Mayo*, the court particularly found with regard to the computer functions, that “all of these computer functions are ‘**well-understood, routine, conventional activit[ies]**’ previously known to the industry.”
 - Claims do not amount to “significantly more” than the abstract idea.
 - Much can thus depend on how the abstract idea is defined....
 - Then “**viewed as a whole**,” the claims still recite an abstract idea (i.e., they do not amount to “significantly more”)
 - [Didn’t really analyze the claim as a whole, though, to consider whether the combination was unconventional, not routine, etc.]
 - Claims deemed not patent eligible

***Berkheimer v. HP* (Federal Circuit, February 8, 2018)**

- Background
 - Judges Moore (author) Taranto and Stoll
 - Technology: Patent relates to a digital asset management system / database
 - Increases efficiency and reduces redundancy by using “rules” to prevent duplicative storage of common text and graphics
 - Allows a change in one element to carry over to all archived elements containing the same stored object (“one-to-many” editing / changing)
 - District Ct.
 - Granted **summary judgement** that claims 1-7 and 9 were patent-ineligible under § 101
 - All claims at issue (1-7 and 9) failed Alice Step 2 “because they describe steps that employ only ‘well understood, routine, and conventional’ computer functions” and are claimed “at a relatively high level of generality.”

Berkheimer v. HP (Federal Circuit, February 8, 2018)

- Federal Circuit
 - First addressed whether plaintiff could argue the dependent claims are separately patent eligible from the independent claim and each other
 - Court: As here, where limitations of dependent claims bear on patent eligibility and in the absence of agreement by patentee to the contrary, arguments going specifically to dependent claims are properly preserved on appeal.
 - *Alice* Step 1: All claims at issue directed to an “abstract idea”
 - E.g., independent claim 1 directed to the abstract idea of parsing and comparing data, and dependent claim 4 further being directed to the abstract idea of storing.
 - However, dependent claim 4, but not claim 1, was deemed to contain an “inventive” concept under *Alice* step 2 as will be discussed below

Berkheimer v. HP (Federal Circuit, February 8, 2018)

- Federal Circuit (Cont.)
 - *Alice* Step 2: This step is “satisfied when the claim limitations ‘involve more than performance of ‘well-understood, routine, [and] conventional activities previously known to the industry.’”
 - “The question of whether a claim element or combination of elements is well-understood, routine, and conventional to a skilled artisan in the relevant field is a question of fact.”
[Emphasis added]
 - Though “whether a claim recites patent eligible subject matter is a question of law which may contain underlying facts.”
 - Whether something “is well-understood, routine, and conventional goes beyond what was simply known in the prior art. The mere fact that something is disclosed in a piece of prior art, for example, does not mean it was well-understood, routine, and conventional.”

Berkheimer v. HP (Federal Circuit, February 8, 2018)

• Federal Circuit (Cont.)

- Court approvingly noted that “the specification explains that the claimed improvement increases efficiency and computer functionality over the prior art systems,” quoting the following from the specification:
 - “By eliminating redundancy in the archive 14, system operating efficiency will be improved, storage costs will be reduced and a one-to-many editing process can be implemented...”
 - **Hint:** Consider putting language in your specification that asserts what the invention does, e.g., “elimination of redundancy” and that it therefore benefits operation of the computer.
 - “The improvements in the specification, to the extent they are captured in the claims, create a factual dispute regarding whether the invention describes well-understood, routine, and conventional activities...”
 - **Q:** Were they captured in the claims sufficiently to affect the district Ct’s summary judgment motion?

Berkheimer v. HP (Federal Circuit, February 8, 2018)

• Federal Circuit (Cont.)

- Independent claim 1 fails Step 2 of Alice: “Does not include limitations which incorporate eliminating redundancy [] or effecting a one-to-many change of linked documents within an archive.”
 - Recited only conventional limitations, e.g., a “parser.”
- But some dependent claims “arguably” pass Step 2, e.g., “[c]laim 4 recites ‘storing a reconciled object structure in the archive without substantial redundancy.’ The specification states that storing object structures in the archive without substantial redundancy improves system operating efficiency and reduces storage costs.” This is directed to an “arguably unconventional inventive concept described in the specification.”
 - **Hint:** Tie claims into stated operating efficiencies or other such beneficial effects (in this case, the so-called “improvement”) relating to a computer or other electronics/“technology” mentioned in the specification, where possible.

***Berkheimer v. HP* (Federal Circuit, February 8, 2018)**

- Federal Circuit (Cont.)
 - Court conceded that the claimed language is not determinative of patent eligibility, but it at least raised “a genuine issue of material fact.”
 - “Whether [the dependent] claims [] perform well-understood, routine, and conventional activities to a skilled artisan is a genuine issue of material fact making summary judgment inappropriate with respect to these claims.”
 - Grant of summary judgment vacated and case remanded to presumably determine what a skilled artisan would think
 - Claims at least saved from invalidity on summary judgment.
 - Note: given that claim 4 “improves system operating efficiency,” etc., it’s not entirely clear why it didn’t pass Alice step 1 for those same reasons as articulated in *Enfish*.

USPTO “*Berkheimer* “ Memorandum (April 19, 2018)

- “Addresses the limited question of whether an additional [claim] element **(or combination of additional elements)** represents well-understood, routine, conventional activity.
 - Found to be an issue of fact, as reaffirmed by two subsequent Federal Circuit decisions
 - *Aatrix v. Green Shades* (Fed. Cir., Feb. 14, 2018) (reversed a judgment on the pleadings of patent ineligibility)
 - Moore, Taranto. Reyna dissenting (“Our precedent is clear that the § 101 inquiry is a legal question.”)
 - *Exergen v. Kaz* [Non-precedential] (March 8, 2018) (Upholding district court conclusion/fact finding that the claims were drawn to a patent eligible invention; Inquiry was factual)
 - Moore, Bryson. Hughes dissenting
- “This memorandum revises the procedures set forth in MPEP § 2106.07”
 - “The MPEP will be updated in due course to incorporate the changes put into effect by this memorandum.”

USPTO “*Berkheimer*” Memorandum (Cont.)

- “**Formulating Rejections**: In [Step 2/2b of an Alice/Mayo analysis], an additional element (**or combination of elements**) is **not** well-understood, routine or conventional **unless** the examiner finds, and expressly supports a rejection in writing with, one or more of the following:”
[Emphasis added]
 - There are four enumerated items where, if none of them test positive with regard to a claim element “or combination of elements,” the claim passes the second step of Alice/Mayo and would be patent-eligible:

USPTO “*Berkheimer*” Memorandum Formulating Rejections (Cont.)

- **1)** “A citation to an express statement in the specification or to a statement made by an applicant during prosecution that demonstrates the well-understood, routine, conventional nature of the additional element(s).”
 - Hint: Be thoughtful/careful about saying, in the specification or prosecution history, that something is well known for, e.g., purposes of enablement
- “A finding that an element is well-understood, [etc.] cannot be based only on the fact that the specification is silent with respect to describing such element.”
 - Thus, there has to be some affirmative statement

USPTO “*Berkheimer*” Memorandum Formulating Rejections (Cont.)

- 2) “A citation to one or more of the court decisions discussed in MPEP § 2106.05(d)(II) as noting the well-understood, routine, conventional nature of the additional element(s).”
 - As when element(s) are claimed, e.g., “in a merely generic manner (e.g., at a high level of generality)...”
- Examples:
 - Receiving or transmitting data over a network, e.g., using the Internet to gather data, sending messages over a network, etc.
 - Storing and retrieving information in memory
 - Freezing and thawing cells

USPTO “*Berkheimer*” Memorandum Formulating Rejections (Cont.)

- 2) (Cont.)
- Hint: Where possible, strenuously argue your claim is more than “generic” or “high level” and point out distinctions between your claim and those in any cited court decision
 - Note: Also from MPEP § 2106.05(d): “Courts have held computer-implemented processes to be significantly more than an abstract idea (and thus eligible), where generic computer components are able **in combination** to perform functions that are not merely generic.”
 - Thus, again, make arguments with a combination of elements (as a whole) in mind.

USPTO “*Berkheimer*” Memorandum Formulating Rejections (Cont.)

- **3)** “A citation to a publication that demonstrates the well-understood, routine, conventional nature of the additional element(s).” [Emphasis added]
 - Does not include all items that might otherwise qualify as a “printed publication” as used in 35 U.S.C. § 102
 - E.g., a single copy of a thesis written in German and located in a German university library is a “printed publication” but not something considered “well-understood, routine, and conventional by scientists who work in the field.”
 - U.S. patents and published applications are publications, but “merely finding the additional element in a **single patent** or published application would not be sufficient to demonstrate that the additional element is well-understood, routine, conventional, **unless the patent or published application demonstrates that the additional element [is] widely prevalent or in common use in the relevant field.**”
 - Hint: E.g., Where only § 101 rejections exist in an application and in the absence of other indicia from this Memo, this indicia #3 might be used to help strengthen an argument that the invention must not be routine or conventional, since the examiner can’t find any prior art, let alone something like the treatise example above which itself is not even adequate for ineligibility.
 - I.e., you couldn’t find any prior art, so how could these elements be “widely prevalent or in common use in the relevant field”

USPTO “*Berkheimer*” Memorandum Formulating Rejections (Cont.)

- **4)** A statement that the examiner is taking official notice of the well-understood, routine, conventional nature of the additional element(s).
 - Should be used “**only** when the examiner is certain, based upon his or her personal knowledge, that the additional element(s) represents well-understood, routine, conventional activity engaged in by those in the relevant art...” [Emphasis in original]
 - If examiner asserts this ground and applicant challenges it, “the examiner **must** then provide one of the items discussed in paragraphs (1) through (3) [] above, or an affidavit or declaration [] setting forth specific factual statements and explanation to support his or her position. [Emphasis added]
- If applicant challenges an assertion under paragraphs (1) –(3), the examiner should merely “reevaluate” his or her position

USPTO “Berkheimer” Memorandum

- Additional thoughts:
 - Memorandum seems to have some good, affirmative guidance as compared to some previous USPTO §101 memos
 - While previous USPTO §101 memos have not always resonated with examiners, the office anecdotally seems to have 101 fatigue. This one might stick.
 - Many examiners (...) are spending a lot of time on the 101 issue.
 - Examiners in AU 3600 have been telling us recently how excited they are about this memo
 - Examiners can play games and, e.g., assert virtually all features (or at least the “inventive” ones) are part of the abstract idea, leaving fewer features to use as “something more”
 - But then it may be harder for the examiner to maintain that the claim is directed to an abstract idea under the various tests under Alice Step 1.

January 2018 Revision of MPEP Section 2106 Patent Subject Matter Eligibility

- Gives applicants (and examiners...) much to cite to
- Some tidbits for consideration:
 - Emphasizes that claims that **recite** an eligibility exception (requiring further analysis) should be carefully distinguished from those that “merely **involve** an exception” (which are patent eligible and do not require further analysis)
 - A machine comprising elements that operate in accordance with $F=ma$ requires further analysis, while a teeter-totter with various components does not, since it merely “involves” mechanical principles.

January 2018 Revision of MPEP Section 2106 Patent Subject Matter Eligibility

- Some tidbits for consideration (Cont.):
 - “The initial burden is on the examiner to explain why a claim or claims are ineligible for patenting clearly and specifically, so that applicant has sufficient notice and is able to effectively respond.”
 - “For example, the rejection should identify the judicial exception by referring to what is recited [] in the claim and explain why it is considered an exception, [] and explain the reason(s) that the additional elements [] taken as a combination, do not result in the claim as a whole amounting to significantly more than the judicial exception.” [Emphasis added]
 - Thus, if examiner’s didn’t completely fulfill this (e.g., “as a whole”) can assert that did not make a prima facie case of eligibility.

Core Wireless v. LG (Federal Circuit, January 25, 2018)

Background

- Judges Moore (author) O’Malley and Wallach
- Technology:
 - A computing device having a display screen displaying a main menu listing one or more applications
 - An application summary window, directly reachable from the main menu, displays a limited list of common functions and data for each application.
 - The data being selectable to launch its respective application
 - The application summary window is displayed while the applications are in an un-launched state
 - According to one of the patents at issue:
 - The improved interfaces allow users to more quickly access data and functions of electronic devices with small screens
 - “The disclosed application summary window ‘is far faster and easier than conventional navigation approaches,’ particularly for devices with small screens.”

Core Wireless v. LG (Federal Circuit, January 25, 2018)

Background (Cont.)

- District Ct.
 - D's motion for summary judgement of invalidity denied
 - According to the district court, the claims are not directed to an abstract idea because "the concepts of 'application,' 'summary window,' and 'unlaunched state' are specific to devices like computers and cell phones [, and] 'LG identifie[d] no analog to these concepts outside the context of such devices.'"
 - The jury found all asserted claims infringed and not invalid.

Core Wireless v. LG (Federal Circuit, January 25, 2018)

Federal Circuit

- The claims "are directed to a particular manner of summarizing and presenting information in electronic devices." [Emphasis added] E.g., claim 1 requires:
 - "an application summary that can be reached directly from the menu,"
 - Thus, the claim specifies "a particular manner by which the summary window must be accessed."
 - "the application summary window list a limited set of data, 'each of the data in the list being selectable to launch [a] respective application and enable the selected data to be seen within the respective application.'" [Emphasis added]
 - the application summary window "is displayed while the one or more applications are in an un-launched state" [Emphasis added]
 - Thus, device applications exist in a particular state
- Thus, "like [] *Enfish*, *Thales*, *Visual Memory*, and *Finjan*, these claims recite a specific improvement over prior systems, resulting in an improved user interface for electronic devices. [Emphasis added]

Core Wireless v. LG (Federal Circuit, January 25, 2018)

Federal Circuit

- “The Specification confirms that these claims disclose an improved user interface for electronic devices, particularly those with small screens”
 - “It teaches that the prior art interfaces had many deficits relating to the efficient functioning of the computer, requiring a user ‘to scroll around and switch views many times to find the right data/functionality.’”
 - “That process could ‘seem slow, complex and difficult to learn, particularly to novice users.’”

Core Wireless v. LG (Federal Circuit, January 25, 2018)

Federal Circuit

- Improvements/Benefits of the invention, as per the specification
 - It “improves the efficiency of using the electronic device by bringing together ‘a limited list of common functions and commonly accessed stored data,’ which can be accessed directly from the main menu...Displaying selected data or functions of interest in the summary window allows the user to see the most relevant data or functions “without actually opening the application up.”
 - Thus, efficiency of using an electronic device can also serve as an improvement /advantage to the “functioning of computers” (see also, “In sum” bullet below).
 - “The speed of a user’s navigation through various views and windows can be improved because it ‘saves the user from navigating to the required application, opening it up, and then navigating within that application to enable the data of interest to be seen or a function of interest to be activated.’ [Emphasis added]
- In sum, the above-language “clearly indicates that the claims are directed to an improvement in the functioning of computers, particularly those with small screens. [Emphasis added]



***Core Wireless v. LG* (Federal Circuit, January 25, 2018)**

Federal Circuit

- Holding
 - "Because we hold that the asserted claims are not directed to an abstract idea, we do not proceed to the second step of the inquiry."
 - "The claims are patent eligible under § 101."



***SAP v. InvestPic* (Federal Circuit, May 15, 2018)**

- Background
 - Judges Lourie, O'Malley and Taranto (Author)
 - Technology: Performance of "certain statistical analyses of investment information." According to the application, unlike the prior art, the invention utilizes methods "which do not assume a normal [rudimentary] probability distribution." Instead, non-symmetrical outliers are advantageously and unconventionally taken into account.
 - District Ct.: Defendant's motion for judgment on the pleadings for invalidity under § 101 was granted.

SAP v. InvestPic (Federal Circuit, May 15, 2018)

- Federal Circuit
 - Began almost immediately by affirming the district court and stating “[w]e may assume that the techniques claimed are ‘[g]roundbreaking, innovative, or even brilliant, but that is not enough for eligibility. Nor is it enough for subject-matter eligibility that claimed techniques be novel and nonobvious in light of prior art, passing muster under 35 U.S.C. §§ 102 and 103.”
 - Might this be a swipe at the Berkheimer memo, indicating that there could still be patent-ineligible subject matter that the memo would otherwise indicate is patent-eligible because it does not run afoul of any of the four indicia in the memo?
 - “No matter how much of an advance in the finance field the claims recite, the advance lies entirely in the realm of abstract ideas, with no plausibly alleged innovation in the non-abstract application realm.”

29

**SAP v. InvestPic (Federal Circuit, May 15, 2018)
Fed. Cir. (Cont.)**

- Claim 1:
 - A method for calculating, analyzing and displaying investment data []
 - (a) selecting a sample space,[including] at least one investment []
 - (b) generating a [somewhat described] distribution function []; and
 - (c) generating a plot of the distribution function.
 - “We have explained that claims focused on ‘collecting information, analyzing it, and displaying certain results of the collection and analysis’ are directed to an abstract idea,” citing the often-used Elec. *Power v. Alstom* case.
 - In this situation, it’s of no consequence that “the information here is information about real investments.”
 - Claims found to be directed to abstract ideas and thus failed Step 1 of Alice.

30

SAP v. InvestPic (Federal Circuit, May 15, 2018)
Fed. Cir. (Cont.)

- Distinguished *McRO* decision (where claims were found patent-eligible) since those claims “were directed to the creation of something physical—namely, the display of ‘lip synchronization’ and facial expressions” of animated characters on screens for viewing by human eyes.”
- “The claimed improvement was to how the physical display operated (to produce better quality images), unlike (what is present here) a claimed improvement in a mathematical technique with no improved display mechanism.”
 - Arguably it’s a bit of a stretch to say *McRO* was about how the physical display operated
 - **BUT note:** Claims directed to graphical output (including the display of informational menus) where, e.g., it can be shown it improves efficiency of a device in at least some manner, seem to fare well.
 - See, e.g., *Core Wireless v. LG* (Fed. Cir. 2018)

SAP v. InvestPic (Federal Circuit, May 15, 2018)
Fed. Cir. (Cont.)

- Alice Step 2
 - All claim details are either “themselves abstract; or there are no factual allegations from which one could plausibly infer that they are inventive.”
 - In other words, the claim elements were either subsumed by the “abstract idea,” or they were deemed “conventional”/“routine”/“not something more”/etc.
 - The court did not discretely map out which elements fell into which category, but did mention at least some claims required various databases and processors which are in the “physical realm”
 - Court stated that “these limitations require no improved computer resources [], just already available computers, with their already available basic functions, to use as tools in executing the claimed process.”
 - No mention of anything happening faster, more efficiently, etc. with the computer
 - Interestingly, *Berkheimer* was never mentioned in the discussion of Step 2, even in a context to distinguish it from the current decision
 - Note, Toronto, the author of the SAP decision, was on the *Berkheimer* panel



BSG Tech v. Buyseasons, Inc. (Federal Circuit, August 15, 2018)

Background

- Judges Hughes (author) Reyna and Wallach
- Technology:
 - Directed to a "self-evolving generic index" for organizing information stored in a database.
 - Problem with prior art is that, where "specialty indices" exist that assist with, e.g., real estate, they are not useful for handling information about other items such as cars
 - Present invention: Enables users to "add new parameters for use in describing items." Particularly allows a user who wants to enter information about a car to be "presented with historical usage information showing that prior users commonly described car items using year, model, and price parameters. The usage information would include information about the relative frequency at which various parameters or values were used."



BSG Tech v. Buyseasons, Inc. (Federal Circuit, August 15, 2018)

Background (Cont.)

- District Court: Defendant's motion to dismiss was "converted" into a motion for summary judgment and then granted.
 - "The district court concluded that the asserted claims 'are directed to the abstract idea of considering historical usage information while inputting data' and lack an inventive concept sufficient to transform them into patent-eligible subject matter."

***BSG Tech v. Buyseasons, Inc.* (Federal Circuit, August 15, 2018)**

Federal Circuit:

- Acknowledged under *Enfish* that software “can make non-abstract improvements to computer technology just as hardware improvements can,” and that “[w]e must, therefore, consider whether the ‘focus of the claims’ is on a ‘specific asserted improvement in computer capabilities . . . , or, instead, on a process that qualifies as an ‘abstract idea’ for which computers are invoked merely as a tool.”
- Agreed with the district court that “the asserted claims are directed to the abstract idea of considering historical usage information while inputting data.”

***BSG Tech v. Buyseasons, Inc.* (Federal Circuit, August 15, 2018)**

Federal Circuit (Cont.):

- According to the court, plaintiff “does not purport to have invented database structures that allow database users to input item data as a series of parameters and values. The [] specification makes clear that such databases predate the claimed invention. [] Rather, the claim’s ‘focus’ is guiding database users by presenting summary comparison information to users before they input data. [] It amounts to having users consider previous item descriptions before they describe items to achieve more consistent item descriptions.”



BSG Tech v. Buyseasons, Inc. (Federal Circuit, August 15, 2018)

Federal Circuit (Cont.):

- Plaintiff made the following three arguments for why the claims are not directed to an abstract idea, none of which were persuasive:
 - 1) The claims “require [the use of] a specific database structure”
 - Court countered that “claims are not saved from abstraction merely because they recite components more specific than a generic computer.”
 - 2) The claims “require users to specifically consider ‘summary comparison usage information’ rather than any type of historical usage information.”
 - Court countered that, “regardless of how narrow ‘summary comparison usage information’ may be relative to the category of ‘historical usage information,’ [] we have never suggested that such [] narrowing, by itself, satisfies Alice’s test.”
 - “In *Content Extraction*, for example, we determined that the claimed methods were directed, in part, to the abstract idea of ‘collecting data,’ even though the claims specifically concerned data from ‘hard copy documents’ collected by an “automated digitizing unit.”
 - For an application of an abstract idea to satisfy step one, the claim’s focus must be something other than the abstract idea itself.”

37



BSG Tech v. Buyseasons, Inc. (Federal Circuit, August 15, 2018)

Federal Circuit (Cont.):

- 3) The claims “focus on a nonabstract improvement in database functionality. [Plaintiff] argues that the claimed invention improves the quality of information added to the database and the organization of information in the database. These improvements result from guiding users’ selection of classifications, parameters, and values through displays of summary comparison usage information.” [] “As a result, the claimed invention ‘allows users to quickly and efficiently access hundreds of thousands or even millions of records, and still find only those few records that are relevant.’
 - Court countered that “[t]hese benefits [] are not improvements to database functionality. Instead, they are benefits that flow from performing an abstract idea in conjunction with a well-known database structure.”
 - Unlike *Enfish* and *Visual Memory* that “focused on improved ways in which systems store and access data,” in this situation, the claims are “unrelated to how databases function.” Here, the claims “do not recite any improvement to the way in which [] databases store or organize information analogous to” *Enfish* or *Visual Memory*.
 - “[A]n improvement to the information stored by a database is not equivalent to an improvement in the database’s functionality”

38



BSG Tech v. Buyseasons, Inc. (Federal Circuit, August 15, 2018)

Federal Circuit (Cont.):

- Alice Step 2:
 - Court cited to Berkheimer where “certain claims recited non-abstract features [] that the specification described as unconventional improvements over conventional systems” and noted that a genuine issue of material fact existed, making summary judgment inappropriate in that case.
 - Court then stated “This case is different. [Plaintiff] points to the [] patent specifications to argue that the asserted claims recite unconventional features that provide benefits over conventional prior art databases. But the relevant inquiry is not whether the claimed invention as a whole is unconventional or non-routine. At step two, we ‘search for an ‘inventive concept’ . . . that is ‘sufficient to ensure that the patent in practice amounts to significantly more than a patent upon the [ineligible concept] itself.’”
 - “It has been clear since *Alice* that a claimed invention’s use of the ineligible concept to which it is directed cannot supply the inventive concept that renders the invention ‘significantly more’ than that ineligible concept.”



BSG Tech v. Buyseasons, Inc. (Federal Circuit, August 15, 2018)

Federal Circuit (Cont.):

- Alice Step 2 (Cont.):
 - Thus, according to the court, “At Alice step two, it is irrelevant whether considering historical usage information while inputting data may have been non-routine or unconventional as a factual matter.”
 - This notion appears to go back to *Flook*...
 - The Berkheimer Memo does not address whether certain elements that may be deemed part of the abstract idea are off limits to an analysis of whether they are “conventional,” either by themselves or in combination with other elements that may or may not, themselves, be deemed part of the “abstract idea”

***BSG Tech v. Buyseasons, Inc.* (Federal Circuit, August 15, 2018)**

Federal Circuit (Cont.):

- Alice Step 2 (Cont.):
 - Moreover, in the *Berkheimer* decision itself, the court also did not appear to address this issue. Notably, though, claim 4 (where a substantial issue was deemed raised on SJ) was held to be “directed to the abstract idea of parsing, comparing, and storing data.” In the Step 2 analysis, what saved the claim on summary judgment as possibly being “conventional” was that the “storing” was done “without substantial redundancy.”
 - Would the judges in this *BSG* decision have found this to be part of the abstract idea and held that it was off limits to such “non-conventional” consideration?
- Bottom line: Claims held directed to patent-ineligible subject matter

***Data Engine Tech v. Google* (Federal Circuit, October 9, 2018)**

Background

- Judges Stoll (author), Reyna, Bryson
- Technology:
 - Three of the patents (the “Tab” patents) relate to “making complex electronic spreadsheets [e.g., multi-dimensional spreadsheets] more accessible by providing familiar, user-friendly interface objects—specifically, notebook tabs—to navigate through spreadsheets while circumventing the arduous process of searching for, memorizing, and entering complex commands.”
 - “The Tab Patents explain that [conventionally] the complex commands required to manipulate each additional spread of the three-dimensional spreadsheet diminished the utility and ease of use of this technology.”
 - In contrast, the present invention “includes user-familiar objects [] which the user already knows how to use’ such as notebook tabs.”



Data Engine Tech v. Google (Federal Circuit, October 9, 2018)

Background

- Tab Patent Technology, cont.
 - "Although these tabs are labeled A, B, and C, etc., they are typically given descriptive names assigned by the user. [] To move to different spreadsheet pages, the user selects the corresponding tab for that page.

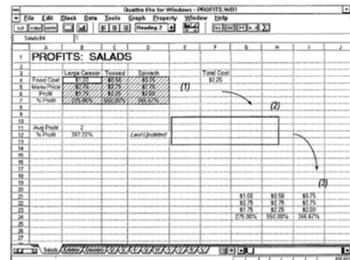


FIG. 4G

Figure 2D below shows more closely an individual spreadsheet page with notebook tabs located along the bottom edge of the page.



FIG. 2D



Data Engine Tech v. Google (Federal Circuit, October 9, 2018)

Background

- Tab Patent Technology, cont.
 - "Quattro Pro, the first commercial embodiment of the claimed invention, was highly acclaimed as having revolutionized three-dimensional electronic spreadsheets."
 - "During prosecution, DET [actually Borland] submitted contemporaneous articles showing the state of the art at the time of the invention and evidencing the significance of the claimed methods to spreadsheet technology." Federal circuit cited approvingly to several of these articles.
 - Does this mean "commercial success" is now an indicia of patent eligibility under Section 101? More likely the articles were submitted for obviousness than for patent eligibility (though file histories difficult to obtain)
 - Note: Quattro Pro was purchased by and continues to be sold by Corel, but it appears the patent was purchased by DET.



Data Engine Tech v. Google (Federal Circuit, October 9, 2018)

Background

- Tab Patent Technology, cont.
 - Representative claim 12 of one of the Tab Patents recited “displaying a row of spreadsheet page identifiers along one side of said first spreadsheet page, each said spreadsheet page identifier being displayed as an image of a notebook tab on said screen display and indicating a single respective spreadsheet page,” “receiving user input for requesting display of a second spreadsheet page in response to selection [] of a spreadsheet page identifier,” and “in response to [] receiving [the] user input step, displaying said second spreadsheet page on [a] screen display”

45



Data Engine Tech v. Google (Federal Circuit, October 9, 2018)

Background

- Technology (‘146 Patent)
 - Not one of the “Tab” patents
 - Appears to essentially be a way to implement “track changes” on a spreadsheet
 - Allows a user to avoid implementing this function manually by making copies of the various versions, etc.
 - One of the claim elements of claim 1 of the ‘146 patent even recites “specifying a base set of information cells for the system to track changes...” [Emphasis in original]
 - Claims did not incorporate or otherwise relate to the aforementioned “tabs.”

46



Data Engine Tech v. Google (Federal Circuit, October 9, 2018)

Background

- District Ct.:
 - Granted defendant's motion on the pleadings finding the Tab Patents directed to an abstract idea "of using notebook-type tabs to label and organize spreadsheets."
 - Also stated the patents are "directed to an abstract idea that humans have commonly performed entirely in their minds, with the aid of columnar pads and writing instruments."
 - Regarding the '146 patent, the court also found this patent directed to an abstract idea and invalid under Section 101.

47



Data Engine Tech v. Google (Federal Circuit, October 9, 2018)

Federal Circuit – The Tab Patents (All but claim 1 of the '551 patent)

- Representative claim 12 "provides a specific solution to then-existing technological problems in computers and prior art electronic spreadsheets."
 - "The specification teaches that prior art computer spreadsheets were not user friendly. [] This was particularly true for three-dimensional spreadsheets"
- "The improvement allowed computers, for the first time, to provide rapid access to and processing of information in different spreadsheets, as well as easy navigation in three dimensional spreadsheets. The invention was applauded by the industry for improving computers' functionality as a tool able to instantly access all parts of complex three dimensional electronic spreadsheets."
 - Query, what if the industry had been silent regarding the invention? Would that have somehow turned the invention into something that didn't solve a technical problem?

48

***Data Engine Tech v. Google* (Federal Circuit, October 9, 2018)**

Federal Circuit – The Tab Patents (All but claim 1 of the ‘551 patent)

- The claim “precisely” recites the salient aforementioned solution and improvement, i.e., “[t]he claim recites specific steps detailing the method of navigating through spreadsheet pages within a three-dimensional spreadsheet environment using notebook tabs.”
- “The claimed method does not recite the idea of navigating through spreadsheet pages using buttons or a generic method of labeling and organizing spreadsheets. Rather, the claims require a specific interface and implementation for navigating complex three-dimensional spreadsheets using techniques unique to computers.”

***Data Engine Tech v. Google* (Federal Circuit, October 9, 2018)**

Federal Circuit – The Tab Patents (All but claim 1 of the ‘551 patent)

- The claim was compared with claims in *Core Wireless*, where the claims “were directed to an improved display interface that allowed users to more quickly access stored data and programs in small-screen electronics, thereby improving the efficient functioning of the computer.”
- Importantly, “akin to the claims in *Core Wireless*, claim 12 recites a ‘specific’ and ‘particular’ manner of navigating a three dimensional spreadsheet that improves the efficient functioning of computers.”



Data Engine Tech v. Google (Federal Circuit, October 9, 2018)

Federal Circuit – The Tab Patents (All but claim 1 of the ‘551 patent)

- Court distinguished cases finding patents patent-ineligible
 - Distinguished *Affinity Labs* since the claims relating to “streaming regional broadcast signals to cellular telephones located outside the region” were “entirely functional in nature,” and “we found nothing in the claims ‘directed to how to implement out-of-region broadcasting.” [Emphasis in original]
 - Though the claims in that case also recited a GUI, that limitation was deemed “conventional.”
 - Unlike *Affinity Labs* and other similar decisions, the present claims are “not simply directed to displaying a graphical user interface or collecting, manipulating, or organizing information to improve navigation through three-dimensional spreadsheets. Instead, the claim recites a specific structure (i.e., notebook tabs) within a particular spreadsheet display that performs a specific function (i.e., navigating within a three dimensional spreadsheet).” [Emphasis added]
 - Also distinguished decisions such as *Intellectual Ventures I LLC v. Capital One*, *Intellectual Ventures I LLC v. Erie Indemnity* and *Electric Power Group v. Alstom*

51



Data Engine Tech v. Google (Federal Circuit, October 9, 2018)

Federal Circuit – The Tab Patents (All but claim 1 of the ‘551 patent)

- “Google avers that humans have long used tabs to organize information. It cites tabbed notebooks, binder dividers, file folders,...”
 - But Court replied “It is not enough, however, to merely trace the invention to some real-world analogy. The eligibility question is not whether anyone has ever used tabs to organize information. That question is reserved for §§ 102 and 103. The question of abstraction is whether the claim is ‘directed to’ the abstract idea itself. [] We must consider the claim as a whole to determine whether the claim is directed to an abstract idea or something more.” [Emphasis added]
 - “The tabs are not merely labeled buttons or other generic icons. [] Rather, the notebook tabs are specific structures within the three-dimensional spreadsheet environment that allow a user to avoid the burdensome task of navigating through spreadsheets in separate windows using arbitrary commands.”
- Because the Court found the claims not abstract under Alice Step 1, they did not reach Step 2

52

Data Engine Tech v. Google (Federal Circuit, October 9, 2018)

Federal Circuit – The Tab Patents (Claim 1 of the '551 patent)

- Among other things, claim 1 “generically recites ‘associating each of the cell matrices [i.e., each page] with a user-settable page identifier’ and does not recite the specific implementation of a notebook tab interface.”
- “Claim 1 of the '551 patent is therefore not limited to the specific technical solution and improvement in electronic spreadsheet functionality that rendered representative claim 12 of the '259 patent eligible. Instead, claim 1 of the '551 patent covers any means for identifying electronic spreadsheet pages.”
 - Claim was directed to an abstract idea, and did not pass Alice Step 2 either.
 - Seems like the specificity of using the “tabs” made a difference between claim 1 and the other claims.
 - Is this like a prior art rejection without the prior art? Did the judges “know it when they saw it”?

53

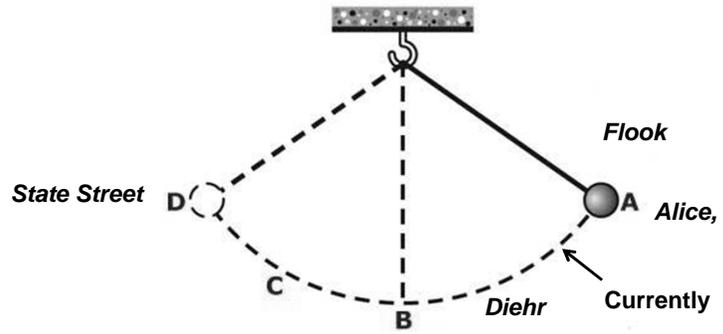
Data Engine Tech v. Google (Federal Circuit, October 9, 2018)

Federal Circuit – The '146 patent

- As indicated, this is “directed to a method of tracking changes in three-dimensional spreadsheets.”
- “The concept of manually tracking modifications across multiple sheets is an abstract idea. The mere automation of this process does not negate its abstraction.”
- “Unlike [the Tab Patents], nothing in the '146 patent’s claims viewed in light of the specification convinces us that the claimed method improves spreadsheet functionality in a specific way sufficient to render the claims not abstract.” [Emphasis added]
- Patent held patent-ineligible

54

Alice in Perspective . . .



SECTION 15

Patent Law Update – 2018 in Review



Presented by

Dennis D. Crouch
Associate Professor of Law
University of Missouri Law School
Columbia, MO

SECTION 16

Beyond the Looking Glass: Getting in Front of the Next Generation of Patent Prosecution Cases



Presented by

Derek C. Stettner

Michael Best & Friedrich LLP
Waukesha, WI, and Chicago, IL



Beyond the Looking Glass: Getting in Front of the Next Generation of Patent Prosecution Cases

Derek C. Stettner

January 2019



Patent Preparation and Prosecution Tips

1. Patent Preparation in View of Alice and Other Trends

- Invention Disclosure/Record
- Inventor Interviews

2. Prosecution Strategies

- Data-Driven, Statistical Approach
- Amendment Strategies
- Examiner Interviews
- Changing the Conversation

3. Post Allowance



Patent Preparation – Back to the Future

- *The specification and claims of a patent, particularly if the invention be at all complicated, constitute one of the most difficult legal instruments to draw with accuracy, and in view of the fact that valuable inventions are often placed in the hands of inexperienced persons to prepare such specifications and claims, it is no matter of surprise that the latter frequently fail to describe with requisite certainty the exact invention of the patentee, and err either in claiming that which the patentee had not in fact invented, or in omitting some element which was a valuable or essential part of his actual invention. Topliff v. Topliff, 145 U.S. 156, 171 (1892).*



Invention Disclosure/Record

- Application quality depends on the quality of the invention disclosure
 - A few sentences or a paragraph of text
 - 150 page PowerPoint presentation
 - Disclosure with written description of problem invention solves, description of how the invention works (the “technical details”), and illustrations of architecture and logic (flow charts, messaging diagrams (UML model), etc.)
- Inventor Interview
 - Collecting a disclosure
 - Understand how the invention works
 - Drafting a claim



Invention Record/Disclosure

- Understand the Invention
 - Drafter taking time to understand the technology
 - Work with inventors to obtain a complete disclosure
 - Illustration of platform
 - Flowchart for software
 - Microprocessor/computer provides sufficient structure only to basic functions of a microprocessor/computer
 - Other computer-implemented functions require disclosure of an algorithm
 - Single block in flow chart included exact functional term/claim element probably not sufficient to explain how the function is achieved



Preparation of Claims

- Written with objective view of prior art
 - Broad is great, unrealistically broad is just an extra round of prosecution
- Cover intended commercial product and potential competitor products – interaction with stakeholders
 - Check during prosecution, no later than Notice of Allowance
- Avoid divided infringement and extraterritoriality
- Different types and varying scope
- Dependent claims with substance



Contents of the Specification

- Concise and without fear
 - Explain what the embodiments are and how they work
 - Don't fear technical detail or explaining a particular example
 - Avoid excess boilerplate before describing what is new
 - Describe generic implementations and multiple embodiments, but don't hide the invention in a sea of possibility
 - Every verb includes "may"
 - Lengthy lists of alternatives and options
- Technical problem and technical solution
- Full support and enablement for claims
- European requirements in mind – added matter if generic instance not described, verbatim support



Specification

- Disclosed, but unclaimed subject matter
- Disclosed, but non-enabled subject matter
- Avoid patent profanity
 - Absolutes – “all,” “every,” “must,” “maximum,” etc.
 - Emphatics – “key,” “critical,” “essential,” etc.
 - Limiters – “The present invention is”
 - Admitted prior art – short background and removed from specification
 - Risks or dangers – “Reduces cancer caused by RF radiation”



Prosecution Strategies

- Check the stats on the art unit and examiner
- Understand the rejections
 - Interview to avoid misunderstanding the Examiner, talking past him or her, or making irrelevant arguments
- Amendments and arguments targeted to the points necessary to distinguish from the prior art
- Rewrite allowable claims in independent form to avoid unnecessary narrowing through dependency
- Pull back prior amendments if not successful
- Keep remarks concise
- Separately argue claims



Prosecution Strategies

- Inverse Approach
 - Narrow first, broader continuation?
- Examiner Interview
 - Provide proposed claim set? Proposed Argument? (See, Avoiding Disclaimer and Estoppel)
- Changing the Conversation
 - PPH Continuation Using Claims Allowed in Foreign Counterpart
 - Appeal
- Post Allowance
 - Continuation to Maintaining Pendency



Avoiding Disclaimer and Estoppel

- Disclaimer – clear and unmistakable surrender of claimed subject matter
 - Specification or during prosecution
 - The self-referential database is the storage repository for all embodiments contemplated.
- Prosecution History Estoppel
 - Limits scope of DOE
 - Amendment or argument, prior art or non-prior art



Avoiding Disclosure and Estoppel

- No Argument Approach
 - “The cited art does not disclose [repeat claim language].”
- Argument explaining differences between references and claimed subject matter
 - Amendments and arguments targeted to the points necessary to distinguish from the prior art



Offices

Austin

Terrace 7 Building
2801 Via Fortuna, Suite 300
Austin, TX 78746

Chicago

River Point
444 West Lake Street, Suite 3200
Chicago, IL 60606

Madison

One South Pinckney Street
Suite 700
Madison, WI 53703

Raleigh

Atrium at Blue Ridge
2501 Blue Ridge Road, Suite 390
Raleigh, NC 27607

Washington, D.C.

801 Pennsylvania Avenue NW
Suite 415
Washington, D.C. 20004

Boulder

1919 14th Street
Suite 700
Boulder, CO 80302

Cottonwood Heights

2750 East Cottonwood Parkway
Suite 560
Cottonwood Heights, UT 84121

Manitowoc

1000 Maritime Drive
Manitowoc, WI 54220

Salt Lake City

170 South Main Street
Suite 1000
Salt Lake City, UT 84101

Waukesha

Two Riverwood Place
N19 W24133 Riverwood Drive, Suite 200
Waukesha, WI 53188

Broomfield

8300 Arista Place
Suite 300
Broomfield, CO 80021

Denver

1776 Lincoln Street
Suite 1100
Denver, CO 80203

Milwaukee

100 East Wisconsin Avenue
Suite 3300
Milwaukee, WI 53202

Washington, D.C.

601 Pennsylvania Avenue NW
Suite 700 South
Washington, D.C. 20004

Michael Best & Friedrich LLP



Michael Best & Friedrich LLP

SECTION 17

The Interplay Between IPRs and Other PTAB Trial Proceedings and Litigation — Strategy and Lessons



Presented by

Honorable Kara Stoll

Circuit Judge, Court of Appeals for the Federal Circuit,
Washington, DC

Erika Arner

Finnegan, Henderson, Farabow, Garrett & Dunner LLP,
Washington, DC

SECTION 18

Corporate Counsel Panel: What's Keeping Corporate Counsel Awake at Night



Presented by

Monica Adjemian

Attorney, Microsoft Corporate, External and Legal Affairs,
Seattle, WA

Toni Y. Hickey

Chief Intellectual Property Counsel,
Cummins, Inc., Indianapolis, IN

Heath Hoglund

Chief Patent Counsel, Dolby
San Francisco, CA

Shelley Mixon

Agilent Technologies, Inc.
Colorado Springs, CO

Brian Platt

Director of IP Litigation, Nagra,
Wenatchee, WA

PANEL: What's Keeping In-house Counsel Awake at Night?

1. Protection of IP in China
2. How to get it all done on a limited budget – doing more with less
 - a. Making the business case for Legal
3. Ownership and protection for new technologies (AR, AI/ML, etc), particularly given state of §101 law
4. Maintaining privilege in a large organization and dealing with the “stupid things” people say in emails
5. Getting Legal involved early enough in the business decisions

SECTION 19

A Dialogue Between Bench and Bar



Presented by

Honorable Kimberly Ann Moore
Circuit Judge
Court of Appeals for the Federal Circuit
Washington, DC

Honorable Leonard P. Stark
Chief Judge,
United States District Court
District of Delaware
Wilmington, DE

John M. Whealan
Intellectual Property Advisory Board
Associate Dean for Intellectual Property
Law Studies, GW | Law, The George
Washington University
Washington, DC

Honorable Kara Stoll
Circuit Judge
Court of Appeals for the Federal Circuit
Washington, DC

Ian Gershengorn
Jenner & Block, Former Acting Solicitor
General and Deputy Solicitor
Washington, DC

Deanne E. Maynard
Morrison Foerster
Washington, DC

**MORRISON
FOERSTER**

36th Annual National CLE Conference

**A Dialogue Between Bench and Bar
Supplemental Materials**

January 5, 2019

Deanne Maynard

SELECT MORRISON & FOERSTER PUBLICATIONS

<u>Page</u>	<u>Article Info</u>	<u>Case Name</u>
1	IP Highlights from Recent Supreme Court Terms (as of Nov. 1, 2018)	--
5	TC Heartland – one year on Eric Acker, John Lanham, Reid Gardner October 2018	<i>TC Heartland LLC v. Kraft Foods Group Brands LLC</i> No. 16-341, Opinion May 22, 2017
9	Sending Out an SAS: Analyzing the SAS Institute Inc. v. Iancu Decision Richard Hung, Rachel Dolphin June 2018	<i>SAS Institute v. Iancu</i> No. 17-130, Opinion Jun 21, 2018
12	All or Nothing: Supreme Court Prohibits PTAB From Partially Instituting AIA Petitions Challenging Patents Matthew Kreeger, Mehran Arjomand, Brian Matsui, Shouvik Biswas April 25, 2018	

IP HIGHLIGHTS FROM RECENT SUPREME COURT TERMS (AS OF NOV. 1, 2018)

OCTOBER TERM 2018: CERTIORARI GRANTS AND CVSGS

- ***Helsinn Healthcare S.A. v. Teva Pharmaceuticals USA Inc.*, No. 17-1229**
 - Petition granted June 25, 2018; scheduled for oral argument December 4, 2018.
 - Whether, under the Leahy-Smith America Invents Act, an inventor's sale of an invention to a third party that is obligated to keep the invention confidential qualifies as prior art for purposes of determining the patentability of the invention.

- ***Fourth Estate Public Benefit Corp. v. Wall-Street.com*, No. 17-571**
 - Petition granted June 28, 2018; not yet scheduled for argument.
 - Whether the registration of a copyright claim has been made within the meaning of 17 U.S.C. § 411(a) when the copyright holder delivers the required application, deposit, and fee to the Copyright office, or only once the Copyright Office acts on the application.

- ***Rimini Street Inc. v. Oracle USA Inc.*, No. 17-1625**
 - Petition granted September 27, 2018; not yet scheduled for argument.
 - Whether the Copyright Act's allowance of "full costs" to a prevailing party is limited to taxable costs under 28 U.S.C. §§ 1821 and 1920, or whether it also allows non-taxable costs.

- ***Return Mail, Inc. v. United States Postal Service*, No. 17-1594**
 - Petition granted October 26, 2018; argument not yet scheduled.
 - Whether the government is a 'person' who may petition to institute review proceedings under the Leahy-Smith America Invents Act."

- ***RPX Corp. c. ChanBond LLC*, No. 17-1686**
 - CVSG October 1, 2018
 - Whether the U.S. Court of Appeals for the Federal Circuit can refuse to hear an appeal by a petitioner from an adverse final decision in a Patent Office inter partes review on the basis of lack of a patent-inflicted injury-in-fact when Congress has (i) statutorily created the right to have the Director of the Patent Office cancel patent claims when the petitioner has met its burden to show unpatentability of those claims, (ii) statutorily created the right for parties dissatisfied with a final decision of the Patent Office to appeal to the U.S. Court of Appeals for the Federal Circuit, and (iii) statutorily created an estoppel prohibiting the petitioner from again challenging the patent claims

- ***Ariosa Diagnostics, Inc. v. Illumina, Inc.*, No. 18-109**
 - CVSG October 29, 2018
 - Whether unclaimed disclosures in a published patent application and an earlier application it relies on for priority enter the public domain and thus become prior art as of the earlier application's filing date.

OCTOBER TERM 2017: SIGNIFICANT DECISIONS

- ***WesternGeco LLC v. ION Geophysical Corp.*, No. 16-1011**
 - Decided June 2018
 - Whether the U.S. Court of Appeals for the Federal Circuit erred in holding that lost profits arising from prohibited combinations occurring outside of the United States are categorically unavailable in cases where patent infringement is proven under 35 U.S.C. § 271(f).
 - The Court reversed the decision of the Federal Circuit and held that WesternGeco’s damages award for lost profits was a permissible domestic application of 35 U.S.C. §284.

- ***Oil States Energy Services, LLC v. Greene’s Energy Group, LLC*, No. 16-712**
 - Decided April 2018
 - Whether the Leahy-Smith America Invents Act in establishing inter partes review violates Article III or the Seventh Amendment of the Constitution.
 - The Court held that inter partes review does not violate either Article III or the Seventh Amendment of the Constitution.

- ***SAS Institute Inc. v. Iancu*, No. 16-969**
 - Decided April 2018
 - Whether 35 U.S.C. § 318(a), which provides that the Patent Trial and Appeal Board in an inter partes review “shall issue a final written decision with respect to the patentability of any patent claim challenged by the petitioner,” requires that Board to issue a final written decision as to every claim challenged by the petitioner, or whether it allows that Board to issue a final written decision with respect to the patentability of only some of the patent claims challenged by the petitioner, as the U.S. Court of Appeals for the Federal Circuit held.
 - In a 5-4 decision, the Court reversed the decision of the Federal Circuit and held that when the United States Patent and Trademark Office institutes an inter partes review to reconsider an already-issued patent claim, under 35 U. S. C. §§311–319, it must decide the patentability of every claim the petitioner has challenged.

OCTOBER 2016 TERM: SIGNIFICANT DECISIONS

- ***Sandoz Inc. v. Amgen Inc.*, No. 15-1039**
 - Decided June 2017
 - Whether the requirement that an applicant provide its application and manufacturing information to the manufacturer of the biologic is enforceable by injunction.
 - Whether the applicant must give notice to the manufacture after, rather than before, obtaining a license from the FDA for its biosimilar.
 - The Court unanimously held that an injunction was not available under federal law, but the Federal Circuit on remand should decide whether an injunction is

available under state law, and that an applicant may provide notice before obtaining a license.

- ***Impression Products, Inc. v. Lexmark International, Inc.* No. 15-1189**
 - Decided May 2017
 - Whether the “patent exhaustion doctrine” applies to conditional sales where the patent holder places post-sale restrictions on the article’s use or resale, and therefore permits the enforcement of these restrictions through the patent law’s infringement remedy.
 - Whether a patentee exhausts its patent rights by selling its product outside of the United States.
 - The Court held that both restrictions set by the patent holder and location were irrelevant and that the “patent exhaustion doctrine” was dependent on the patentee’s decision to make a sale.

- ***TC Heartland LLC v. Kraft Foods Group Brands LLC*, No. 16-341**
 - Decided May 2017
 - Whether the patent venue statute, 28 U.S.C. § 1400(b), is the sole and exclusive provision governing venue in patent infringement actions and is not to be supplemented by the broader definition of corporate “residence” contained in the general venue statute 28 U.S.C. § 1391(c).
 - The Court unanimously held that the amendments to Section 1391 did not modify the meaning of Section 1400(b) and therefore a domestic corporation “resides” only in its state of incorporation for purposes of the patent venue statute.

- ***SCA Hygiene Products Aktiebolag v. First Quality Baby Products, LLC*, No. 15-927**
 - Decided March 2017
 - Whether and to what extent the defense of laches may bar a claim for patent infringement brought within the Patent Act’s six-year statutory limitations period set out in 35 U.S.C. §286.
 - The Court held that laches cannot be invoked as a defense against damages where the infringement occurred within the period described by Section 286.

- ***Athletica, LLC v. Varsity Brands Inc.*, No. 15-866**
 - Decided March 2017
 - Whether the artistic design that is part of a “useful article” qualifies for copyright protection in its own right.
 - The Court held that an artistic feature of the design of a useful article was eligible for copyright protection since the feature satisfied the following test: (1) that it could be perceived as a two- or three-dimensional work of art separate from the useful article, and (2) it would qualify as a protectable work of art in its own right if imagine separately from the useful article.

- ***Life Technologies Corporation v. Promega Corporation*, No. 14-1538**
 - Decided February 2017

- Whether the statutory phrase “all or a substantial portion of the components of a patented invention” in 35 U.S.C. § 271(f)(1) can refer to a single component of a multicomponent invention.
- In a unanimous decision, the Court held that the phrase “substantial portion” in 35 U.S.C. §271(f)(1) has a quantitative meaning, not a qualitative one, and thus §271(f)(1) did not cover the supply of a single component of a multicomponent invention.

dc-1015060



TC Heartland – one year on

With the one-year anniversary of *TC Heartland v Kraft Foods*, the impact of the Supreme Court of the US' landmark patent venue decision becomes clearer. **Eric M Acker, John R Lanham and Reid R Gardner** explain

One year on from the Supreme Court of the US' decision, it comes as no surprise that, the patent docket in the Eastern District of Texas has shrunk, though it still remains a leading forum for newly-filed suits. The District of Delaware supplanted the Eastern District of Texas as the top forum for new patent litigation, and it is likely to remain a top venue choice at the same time that vacancies from the Delaware bench strain the district's resources. We review the specific number of cases being filed in the key patent litigation districts and the impact of those numbers on how quickly cases are being resolved. We also examine several trends emerging in the application of *TC Heartland* by district courts and the Federal Circuit.

By now, the general implications of *TC Heartland* among patent litigators are well known. In a unanimous decision, the Supreme Court found that the patent venue statute, 28 USC § 1400(b) – not the general venue statute, 28 USC § 1391(c) – supplies the venue rules for patent infringement cases. Under the general venue statute, residence for defendant legal entities is coextensive with personal jurisdiction. The patent venue statute, in comparison, provides that an action may be brought only in the judicial district where (1) the

“Under the place of incorporation test, the Federal Circuit recently held that venue is only appropriate in the district of incorporation, rather than in any district in the state.”

defendant resides or (2) where the defendant has committed acts of infringement *and* has a regular and established place of business. A subsequent Federal Circuit decision, *In re Cray*, defined the “regular and established place of business” test to require “a physical place, of business, of the defendant.”

Patent litigation trends post-TC Heartland

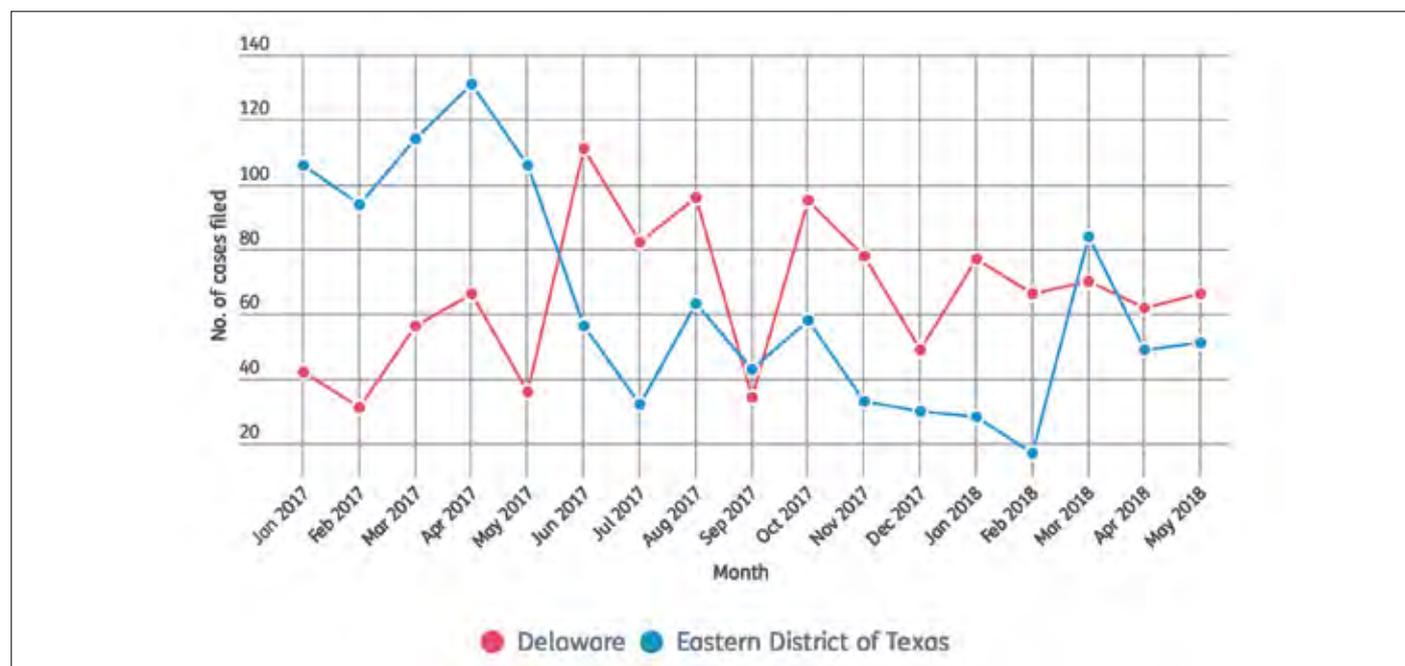
Before the *TC Heartland* decision, the leading patent litigation venues were, in order, the Eastern District of Texas, the District of Delaware, the Central District of California, and the Northern District of California. While each of those districts remains a top choice for patent plaintiffs, their order has changed in ways that will impact the litigation landscape for years to come. Just prior to *TC Heartland*, the Eastern District of Texas saw an average of over 100 patent cases filed per month. Immediately after *TC Heartland*, the docket dropped below 60 new cases per month. After the *In re Cray* decision, new patent cases in the Eastern District of Texas dropped even further to below 40 per month. Although recently there has been an uptick in Eastern District case filings, the overall trend appears decidedly lower for the Eastern District (see figure 1).

Delaware

Meanwhile, the District of Delaware has seen nearly the inverse impact. Since more than 1.2m legal entities – and nearly 67% of Fortune 500 companies¹ – are incorporated in Delaware, many defendants are subject to venue there under the place of incorporation test. New

Figure 1: Patent case filings, by month

Source: LegalMetric



patent cases in the District of Delaware jumped from under 40 filings in May 2017 to over 100 filings in June 2017, immediately after the *TC Heartland* decision, though recent months have seen a downward trend in new filings. The Delaware patent docket has grown sufficiently to have an impact on the national statistics for patent litigation. In the year prior to *TC Heartland*, Delaware handled 12.3% of the patent cases in the country. In the year after, Delaware's docket increased to 23.5% of the country's patent cases.²

The shift of caseload to the District of Delaware will have a real-world impact on litigants. The Eastern District of Texas has resolved patent cases faster than any other popular forum, attributable in part to tighter case schedules and a faster timetable at each major step of the patent litigation process, although this pace has slowed in recent years as the caseload in the Eastern District of Texas impacted case schedules. Delaware's patent litigation process has historically been slower than the Eastern District of Texas. Moreover, Delaware has lost two of its four district court judges: Judge Robinson retired in the summer of 2017, and Judge Sleet has reassigned much of his docket in advance of his retirement later this year. Maryellen Noreika and Colm Connolly have been nominated to fill the Delaware vacancies and have completed their confirmation hearings but, as of the time of this article, the confirmation process for those nominees is ongoing. To help manage its caseload in light of these changes, the District of Delaware is relying more heavily on its magistrate judges and has enrolled a group of

“TC Heartland may not be merely shuffling caseloads between venues but may actually be driving down the overall volume of patent litigation.”

district and appellate judges from other federal districts to sit by designation. At least for the short term, then, parties to Delaware litigation are faced with the potential of slower and less consistent case progress.

California

California venues have likewise seen changes, though less dramatic than the shift between Texas and Delaware. Prior to *TC Heartland*, the Central District held a consistent lead in patent filings over the Northern District (perceived by some as less friendly to patent plaintiffs).

Following the Supreme Court's decision, both Northern District and Central District filings have seen a marked increase, with the Northern District starting to close the gap with the Central District. Comparing the year before *TC Heartland* with the year after, the Central District docket increased from 6.1% to 9.0% of the country's patent cases filed. The Northern District docket increased from 3.4% of patent filings to 7.4%.³

LegalMetric data on time to various case milestones is largely consistent with the shift in filing volume. For example, the time to summary judgment in Delaware patent cases has gone from an average of 30.5 months pre-*TC Heartland* to over 45 months following the decision. The Central District of California has seen a more modest increase in the timetable from an average of 18.1 months to an average of 23.4 months, while the Eastern District of Texas and Northern District of California have experienced slightly faster paths to summary judgment – 24.7 down to 20.7 months and 24.1 down to 19.5 months, respectively.

In another notable result from analysis of patent litigation trends, *TC Heartland* may not be merely shuffling caseloads between venues but may actually be driving down the overall volume of patent litigation. The more restrictive venue rules will often force patent-holding companies and non-practising entities to pursue multiple defendants in districts across the country, rather than suing batches of defendants in a single district. Lex Machina's statistics reflect a nearly 80% drop in filings by “high volume” plaintiffs post-*TC Heartland* (23 May 2017 to 11 April 2018)

as compared to the same period prior to *TC Heartland*.⁴ While it is too early to make a final determination, and while the Supreme Court's decision is unlikely to be the sole cause for this drop, the data nonetheless suggests that aggressive patent plaintiffs may be less active in a post-*TC Heartland* world.

The more restrictive venue test required under *TC Heartland* has also led to increased focus on the established place of business test, with a developing body of case law. We examine some emerging trends below.

Foreign corporate entities

The Supreme Court's *TC Heartland* opinion expressly declined to reach the issue of venue for foreign corporations or the court's prior holding on foreign corporation venue under *Brunette Machine Works Ltd v Kockum Industries, Inc* (S Ct 1972), leading to some uncertainty over where foreign companies could be sued. The Federal Circuit has now provided guidance. Denying a writ of *mandamus* in *In re HTC Corporation* (Fed Cir 2018), the Federal Circuit held that foreign corporations sued for patent infringement are subject to the nationwide venue provisions of Section 1391(c)(3), rather than the patent-specific venue statute Section 1400(b). *In re HTC* raises similar questions of Supreme Court precedent and statutory interpretation as *TC Heartland*, and it is possible that the issue of patent venue may once again appear before the Supreme Court. For the time being, however, foreign corporations should assume that they may be subject to a patent suit in any district that has personal jurisdiction with respect to the action.

Developing venue case law

In general, district court decisions since *In re Cray* have narrowly interpreted the "established place of business" test for venue in a patent suit. For example, in *Post Consumer Brands, LLC v General Mills, Inc* (ED Mo 2017) and *Unity Opto Tech Co v Lowe's Home Centers LLC* (WD Wis. 2018), courts rejected plaintiffs' arguments that defendants were subject to venue based on the presence of a corporate affiliate. In *General Mills*, the court found no venue based on the presence of an affiliate's factory, even where the defendant had its name on the factory and associated itself with the factory in regulatory filings. In *Lowe's*, the court found no venue over one of the defendants even where it was a corporate affiliate of another defendant (which was subject to venue) and worked closely with that defendant. Similarly, in *Precision Fabrics Group, Inc v Tietex Int'l Ltd* (MDNC 2017), the court applied *Cray* and found no venue based on a home office of defendant's employee in

the district. It appears that courts will continue to strictly construe Section 1400(b) to require physical presence of the defendant entity itself.

Indeed, since *TC Heartland*, courts have ruled in favour of plaintiffs in very few patent cases contesting venue. In two exceptions, the Eastern District of Texas denied motions to dismiss for venue in *American GNC Corp v ZTE Corp* (ED Tex 2017) and *GEODynamics, Inc v DynaEnergetics US, Inc* (ED Tex 2017). But the Federal Circuit vacated the *American GNC Corp* decision, holding that the district court failed to fully consider the factors related to venue. In *GEODynamics*, the Eastern District denied the defendant's motion to dismiss based on a narrow circumstance in which the corporation's president seemingly indicated in a prior case between the two parties that the defendant corporation has or is planning a presence in the district.

“More case law, and possibly Federal Circuit intervention, will be necessary to resolve this split.”

For the most part, courts have carefully avoided a "liberal construction" of Section 1400(b) and dismissed cases where venue is in question. Courts have found that venue is not established by a local phone number printed on an employee's business cards,⁵ limited quantities of promotional literature in employees' home offices,⁶ online services using a third party-controlled server,⁷ a remotely controlled billboard,⁸ and leased shelf space in the district.⁹ Note, however, that the defendant's physical presence in the district may not necessarily need to be connected with the acts of infringement for venue to apply. In *Plexikon Inc v Novartis Pharm Corp* (ND Cal 2017), defendant was alleged to lease and operate two facilities within the district, though defendants argued that there was

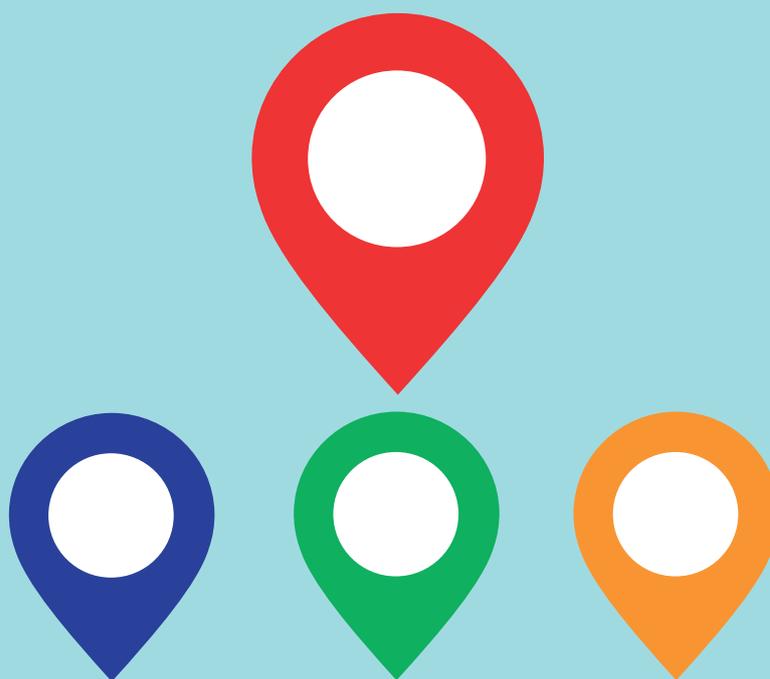
no connection between the alleged acts of infringement and those facilities. The court declined to read a "nexus" requirement into Section 1400(b) and denied defendants' venue challenge.

Furthermore, under the place of incorporation test, the Federal Circuit recently held that venue is only appropriate in the district of incorporation, rather than in any district in the state.¹⁰ If the company has a physical headquarters within the state, that will identify the district of incorporation. But, if it does not, the Federal Circuit has instructed courts to look to the location of the company's registered office for purposes of incorporation. This ruling provides another basis for defendants seeking to transfer a case out of the Eastern District of Texas and will also have significant impacts on venue selection for California companies.

Finally, federal courts will be faced with new venue challenges for declaratory judgment actions. *Under VE Holding Corp v Johnson Gas Appliance Co* (Fed Cir 1990), which was overruled in part by *TC Heartland*, "[i]t has long been held that a declaratory judgment action alleging that a patent is invalid and not infringed – the mirror image of a suit for patent infringement – is governed by the general venue statutes, not by § 1400(b)." Similarly, Section 1400(b) applies to "civil action[s] for patent infringement," rather than actions for declaratory judgment. Should this standard continue to apply, an accused infringer could seek an appropriate (and favourable) venue under the broader general venue rules by seeking declaratory judgment before being sued for infringement. A patent holder could likewise attempt to structure its suit as a declaratory judgment action to alter the venue rules. While declaratory judgment actions bring their own standing and jurisdictional challenges, they may provide a different venue path for creative litigants.

The Hatch-Waxman dilemma

TC Heartland has triggered a split of authority for venue in generic drug patent litigation. The Hatch-Waxman Act provides a process through which generic drug companies can file an Abbreviated New Drug Application (ANDA) to secure approval to market a generic version of a brand-name drug. The Act creates an artificial act of infringement for generic companies that use the ANDA process to certify that patents associated with the brand-name drug are invalid, not enforceable, or not infringed by the drug at issue. The brand-name drug sponsor may then sue the generic company for patent infringement, prior to any manufacture or sale of the generic product taking place. However, Section 1400(b)



provides for venue only where “defendant *has committed* acts of infringement and has a regular and established place of business.” The incongruity between the pre-manufacture posture of ANDA litigation and the past-tense verb in the patent venue statute has led to split authority over where the lawsuit may be filed.

Recent cases from the District of Delaware and District of New Jersey hold that the “has committed” test is satisfied when the ANDA applicant plans to market the generic drug within the district. In *Bristol-Myers Squibb Co v Mylan Pharm Inc* (D Del 2017), Judge Stark of the District of Delaware characterised the inconsistency between the ANDA procedure and the language of the patent venue statute as “an almost impenetrable problem”. After comparing the purpose of the two laws, and relevant Federal Circuit authority, Judge Stark determined that the ANDA filer’s “future, intended acts must be included as part of the ‘acts of infringement’ analysis for purposes of determining if venue is proper under the patent venue statute.” Thus, the court may consider the ANDA filer’s non-speculative plans to market the subject drug within the district. Judge Stark has since incorporated this reasoning in several other venue decisions. In *Celgene Corp v Hetero Labs Ltd* (DNJ 2018), Judge Salas in the District of New Jersey also recently adopted Judge Stark’s reasoning.

The Northern District of Texas implemented a different approach. In *Galderma Labs, LP v Teva Pharm USA, Inc* (ND Tex 2017), Chief

Judge Lynn considered the standard adopted in the District of Delaware but focused on Congress’s past tense use of “has committed”. Applying this language, the court concluded that future marketing plans should not be considered for venue, which instead should be determined by looking to where the ANDA submission itself was prepared and submitted. As of the time of this article, the narrower *Galderma* venue standard has not been applied in other courts but has been cited in briefings on pending venue motions in other districts. If adopted more broadly, the *Galderma* standard could effectively limit Hatch-Waxman litigation venues to the generic company’s place of incorporation or place of ANDA filing preparation. More case law, and possibly Federal Circuit intervention, will be necessary to resolve this split.

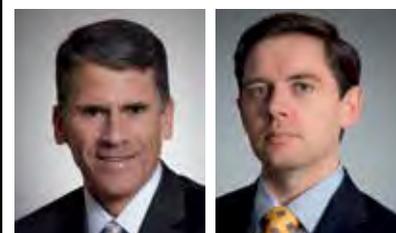
Footnotes

1. Delaware Division of Corporations 2016 Annual Report, available at <https://corp.delaware.gov/2016AnnualReport.pdf>
2. Data courtesy of LegalMetric.
3. *Id.*
4. Lex Machina defines a “high-volume plaintiff” as a party has filed at least 10 patent cases (excluding ANDA cases) within a 365-day period.
5. *Nike, Inc v Skechers USA, Inc*, No 3:16-CV-007-PK, 2017 US Dist LEXIS 217302, at *20-21 (D Or 14 November 2017).
6. *Regents of Univ of Minnesota v Gilead Scis, Inc*, No 16-CV-2915 (SRN/HB), 2017 US Dist LEXIS

174093, at *23 (D Minn 20 October 2017).

7. *Pers Audio, LLC v Google, Inc*, 280 F Supp 3d 922, 934-35 (ED Tex 2017).
8. *Lites Out, LLC v OutdoorLink, Inc*, No 4:17-CV-00192, 2017 US Dist LEXIS 181917, at *11 (ED Tex 2 November 2017).
9. *Peerless Network, Inc v Blitz Telecom Consulting, LLC*, No 17-CV-1725 (JPO), 2018 US Dist LEXIS 49628, at *11 (SDNY 26 March 2018).
10. *In re BigCommerce, Inc*, 890 F.3d 978, 986 (Fed Cir 2018).

Authors



Eric M Acker (top left) is a partner and trial lawyer in Morrison & Foerster’s IP group and John R Lanham (top right) is an associate in the firm’s IP group and Reid R Gardner (bottom left) is an associate in the litigation department.

Sending Out an SAS: Analyzing the *SAS Institute Inc. v. Iancu* Decision

By Richard Hung and Rachel Silverman Dolphin

In a 5-4 decision, with four justices dissenting, the U.S. Supreme Court struck down the Patent Trial and Appeal Board (PTAB)'s practice of instituting review on only a subset of an *inter partes* review (IPR) petitioner's validity challenges. *SAS Inst., Inc. v. Iancu*, --U.S.--, 200 L.Ed.2d 695, 700 (2018) (*SAS*) (<http://bit.ly/2IzikiF>).

The case turned on the statutory interpretation of the Leahy-Smith America Invents Act. The specific statute at issue, 35 U.S.C. §318(a), provides: "If an inter partes review is instituted and not dismissed under this chapter, the Patent Trial and Appeal Board shall issue a final written decision with respect to the patentability of any patent claim challenged by the petitioner and any new claim added under section 316(d)."

Rich Hung is a Litigation partner and the co-chair of the Intellectual Property Group at Morrison & Foerster. **Rachel Dolphin** is an associate in the Intellectual Property Group at Morrison & Foerster. Her practice focuses on IP Litigation and post-grant patent proceedings.

The question in *SAS* was whether the PTAB's final written decision must address all patent claims in a petition or whether the PTAB has discretion to only institute review on certain claims (meaning the final written decision would address only those.)

In an opinion authored by Justice Neil Gorsuch, the majority found the statute clear and unambiguous, while the dissent found it ambiguous. The majority determined that the word "any" meant "every," such that the PTAB did not have discretion to only review a subset of claims. Because the Court found the statute unambiguous, it did not defer to the United States Patent and Trademark Office (PTO)'s interpretation under the *Chevron* doctrine. See, *Chevron U.S.A. Inc. v. Natural Resources Defense Council, Inc.*, 467 U. S. 837 (1984) (<http://bit.ly/2IzzJ1a>).

Despite finding the language unambiguous, the majority looked to a neighboring provision governing *ex parte* reexaminations and compared it with the language governing IPRs. Under the former regime, the PTO director is granted explicit discretion to initiate a particular *ex*

parte reexamination. The majority reasoned that, if Congress wanted to grant the PTAB this discretion for IPRs, it could have used the same language. The absence of such language supported the majority's view (albeit dicta) that Congress did not intend to provide the PTAB with this discretion.

The Court rejected the PTO's policy argument that its reading of the statute undermined the statutory intent, *viz.*, to promote efficiency at the PTAB and expedite the patent review system. Were the PTO required to analyze weak claims or challenges, the argument went, that would undermine the efficiency of the system. The Court rejected this argument as an issue for Congress.

THE DISSENTS

Justices Ruth Bader Ginsburg and Stephen Breyer both wrote dissents discussing the majority opinion's impractical results.

Justice Ginsburg noted that the PTAB now could deny petitions with claims likely to be unpatentable but simultaneously signal its views, thus encouraging piecemeal petitions on certain claims

or grounds. This process would be more expensive and time-consuming for the parties than the PTAB's prior process of partial institutions. As she succinctly observed: "Why should the statute be read to preclude the Board's more rational way to weed out insubstantial challenges?" *SAS*, 200 L.Ed.2d at 708.

Finding the statute ambiguous, Justice Breyer would have deferred to the PTO's "reasonable" interpretation. *Id.* at 709. He also found the practical results inefficient, in part because the Federal Circuit would have to review a decision on all petitioned claims. Justice Breyer deemed the majority's opinion "anomalous," as the PTAB's decision to institute review is discretionary and nonreviewable, but the Board now must issue a final written decision on all petitioned claims — even ones that are "near frivolous." *Id.* at 713.

SAS'S IMPACT: MUST THE PTAB INSTITUTE ON ALL GROUNDS?

While *SAS* clarified that the PTAB must either not institute at all or institute on all petitioned claims, an immediate question is what this decision means for challenged claims. Before this case, the PTAB often only instituted on certain grounds raised in the petition. For example, if the petitioner asserted that claim 4 was invalid as anticipated by reference A and was also invalid as obvious by B in light of C, the PTAB might choose only to institute on the obviousness ground. After *SAS*, practitioners wondered

where this practice stood, in large part because of its impact on estoppel.

Some language in *SAS* certainly suggests that the PTAB must institute on all challenged grounds (if any). For example, the majority opinion compared an IPR petition to a civil complaint, saying "the petitioner is master of its complaint and normally entitled to judgment on all of the claims it raises, not just those the decision maker might wish to address." 200 L.Ed.2d at 703. This suggests that the petition controls what grounds the PTAB must consider. But it is important to remember that the statute itself is silent as to grounds; instead, the statute discusses what must happen with "any patent *claim* challenged." 35 U.S.C. §318(a) (emphasis added). Especially given the majority's emphasis on the statute's plain language, *SAS* arguably should be read as limited to claims.

The PTO's initial reaction, however, was more conservative. According to its recent guidance on *SAS*, if it grants review, it will now institute on all claims and all challenged grounds. *See*, "Guidance on the Impact of *SAS* on AIA Trial Proceedings" (Apr. 26, 2018) (<http://bit.ly/2IzAkC5>). In a webinar titled "Chat with the Chief" on April 30 (<http://bit.ly/2IzF154>), the PTO confirmed that this means it will institute on and consider all challenges in a petition, at least for now. But the PTO was ambivalent as to whether *SAS* compelled this approach, noting instead that the PTO believed it was the best one.

HOW DOES THIS DECISION AFFECT ESTOPPEL AND STAY MOTIONS?

The practical considerations regarding estoppel and stays are many. For example, if a defendant challenges all claims, will it essentially be waiving its invalidity case in the district court? Should a defendant challenge fewer claims to limit its estoppel perspectives in district court? If a defendant does so, will that weaken its argument for a stay pending IPR? On the flip side, as the PTAB now must institute on all requested claims (if at all), can defendants strengthen the arguments for a stay if defendants challenge all claims asserted in the district court?

The estoppel effects of the PTAB's final written decision will likely force patent challengers to rethink their IPR strategies. A petitioner is estopped from re-asserting invalidity defenses that were raised, or reasonably could have been raised, in the IPR proceedings. 35 U.S.C. §315(e)(2). While, previously, a petitioner could assert a particular invalidity ground in the district court proceeding if the Board did not institute on it, now the petitioner will be estopped from making such arguments. It may behoove patent challengers not to file questionable IPRs, or at least questionable claims, as putting on an invalidity case is an important part of most defendants' district court strategies.

WILL INSTITUTION DECISIONS CHANGE?

Some practitioners note that PTAB institution decisions may

become less robust due to timing constraints and the requirement to institute on all claims now. Were this to occur, it is unclear whether this would be positive or negative overall. On the one hand, thorough institution decisions provide significant insight into the panel's views on the claims and grounds at issue, which can help both parties strategize and focus their arguments (and may encourage settlement). If the decisions are not as thorough, then the parties will be left to wonder about the relative persuasiveness of their arguments, and thus spend more time and money shoring up each argument. On the other hand, some worry that a thorough institution decision will entrench the panel in its preliminary views. This might not be ideal given the limited evidence and argument before the panel at that stage.

As to whether the practice of robust institution decisions will change, the PTO noted that panels have always had the discretion to decide what to include in their institution decisions. According to the PTO, *SAS* did not change that discretion. The Supreme Court in *SAS* even recognized that lengthy decisions are not necessary, explaining that "the Director need not even consider any other claim before instituting review" once the PTO has decided that the petitioner is likely to succeed on one claim. 200 L.Ed.2d at 704.

WILL PATENT HOLDERS BEGIN TO DISCLAIM?

Another potential outcome of *SAS* is that patent owners may begin to

disclaim claims most susceptible to an invalidity challenge. This currently occurs in covered business method (CBM) petitions, where patent owners sometimes disclaim the claims relating to financial products or services to make their patent ineligible for CBM review. Disclaiming relatively weak claims may make institution less likely, but may also limit the patent owner's infringement positions. Patent owners will need to weigh the disclaimer decision more carefully now in view of the different incentives.

HOW IMPACTFUL WILL THIS CASE REALLY BE?

In its webinar, the PTO estimated that *SAS* affects only about 20% of pending cases (*i.e.*, institutions where the PTAB agreed to review some, but not all, of the challenged claims). Of course, the case reaches far beyond that.

First, it will impact all institution decisions going forward. This has already occurred. In the institution decision in *Western Digital Corp. v. Spex Technologies Inc.*, the panel indicated its belief that petitioner was likely to succeed only on two of the 11 asserted claims. Following *SAS*, it instituted on all 11 claims.

Second, it affects the 20% or so of pending partially instituted cases. Anyone with a pending review where only some claims were instituted should read the PTO's guidance, which explains the procedures for such cases.

Third, as *SAS* did not address retroactivity, the impact on partially

instituted cases that have already gone to a final decision remains to be seen. For the cases that are currently pending at the Federal Circuit, must the petitioner move to vacate the appeal and remand the case back to the PTAB for a final decision on all petitioned claims? Does the Federal Circuit even have jurisdiction over these appeals? For the cases in which the Federal Circuit's opinion has become final and non-reviewable, does the losing party have any options? For the parties that didn't appeal their initial PTAB loss, can they now move for re-institution in light of *SAS*?

CONCLUSION

There are many questions left, but the PTAB continues to work vigorously to issue further guidance on the case's impact. And Congress, of course, could moot *SAS* entirely by expressly granting the PTAB the discretionary power to institute partial reviews. It might do so to further its goal of creating an efficient patent review process and to reduce the burdens on the PTAB and Federal Circuit. All in all, *SAS*'s effects on the PTAB's procedures and workload will require that practitioners carefully assess pending and future IPR petitions.



All or Nothing: Supreme Court Prohibits PTAB From Partially Instituting AIA Petitions Challenging Patents

Matthew I. Kreeger, Mehran Arjomand, Brian R. Matsui, and Shouvik Biswas

04/25/2018

[Appellate + Supreme Court](#), [Intellectual Property Litigation](#), [Inter Partes Review + Post Grant Practice](#), and [Patent Litigation](#)

Client Alert

On the same day that patent challengers breathed a sigh of relief once the Supreme Court upheld the constitutionality of inter partes review (IPR) in *Oil States*, [1] the Court also threw a monkey wrench into the way IPRs will be litigated. In a 5-4 decision, the Court held that when the Patent Trial and Appeal Board (PTAB) institutes an IPR, the PTAB must decide the patentability of *all* of the claims that a Petitioner has challenged in its petition. *SAS Institute Inc., v. Iancu*. The Court held that the United States Patent and Trademark Office (USPTO) Director does not have the statutory authority to partially institute a challenge by picking and choosing the claims that will proceed to a full review. Instead, if the PTAB decides to institute an IPR because at least one claim in the challenge has a reasonable likelihood of being invalidated, the PTAB is required to institute as to *all* of the claims challenged in the original petition, and ultimately issue a final written decision on all of the challenged claims. While the Court's decision on the surface appears to make only a procedural adjustment, the decision could have far-reaching impact on cases before the PTAB, as well as before district courts.

Background

In response to the passage of the Leahy-Smith America Invents Act in September 2011, which created IPRs, the USPTO promulgated a series of rules governing how the PTAB was to conduct the newly created IPR proceedings. One of those rules provided that “the Board may authorize the review to proceed *on all or some of the challenged claims* and on *all or some of the grounds of unpatentability* asserted for each claim.” 37 CFR § 42.108(a) (emphasis added). Using this rule, the PTAB routinely has instituted IPR proceedings only on patent claims that it felt had a “reasonable likelihood of success” of being found unpatentable. As a result, even if an IPR petition challenged all the claims of a patent, the PTAB often used its discretion to institute a proceeding only on some of those claims, while declining to institute review on the remaining claims. Upon conclusion of the proceeding, the PTAB would render a final written decision addressing only the claims for which it had instituted review.

SAS Institute's Challenge

SAS Institute Inc. (SAS) sought an IPR of U.S. Patent 7,110,936 assigned to ComplementSoft LLC. In its petition, SAS challenged all 16 of the patent's claims on various grounds of invalidity. However, the PTAB instituted an IPR only on claims 1 and 3 through 10, while declining to review the rest of the claims. Ultimately, in a final written decision, the Board found claims 1, 3, and 5 through 10 unpatentable, while upholding claim 4. The Board's final written decision did not address the claims for which review was denied.

SAS appealed, arguing that 35 U.S.C. § 318(a) required the PTAB to decide the patentability of every challenged claim in its final written decision. The Court agreed with SAS. Section 318(a) states that “[i]f an inter partes review is instituted and not dismissed . . . the Patent Trial and Appeal Board shall issue a final written decision with respect to the patentability of any patent claim challenged by the petitioner. . . .” In analyzing the text of § 318(a), the Court concluded that by stating that

the Board's final written decision "shall" resolve the patentability of "any patent claim challenged by the petitioner," Congress meant that the Board must address every claim Petitioner challenged in its petition. Thus, the Court held that the PTAB did not have the statutory authority to only institute proceedings on some of the challenged claims. Instead, if the Board found that any claim had a reasonable likelihood of being successfully invalidated based on the petition, the Board was required to institute review for all of the claims challenged in the petition.

Short Term and Long Term Effects on the PTAB

The Court's holding will likely have an immediate impact on pending cases before the PTAB in which the Board only partially instituted on the claims raised in the petition. The Board may be forced to revisit its original institution decisions and add non-instituted claims back into pending proceedings in order to comply with the SAS decision. Furthermore, the Federal Circuit may also remand cases back to the PTAB in which the Board only partially instituted a petition so that the non-instituted claims can be considered. Petitioners who currently have IPRs pending before the PTAB, or appeals pending before the Federal Circuit from the PTAB, should immediately consider whether to request that the PTAB add non-instituted claims to their IPR proceedings and issue a final written decision as to the non-instituted claims. However, Petitioners should be wary of what they wish for. Asking for claims to be reviewed by the PTAB, which had previously declined to review them, may mean that these claims could be found patentable at the final written decision, thereby triggering estoppel for Petitioners as discussed below. Furthermore, the addition of claims in any proceeding will increase costs for all involved.

The longer-term impacts of the Court's decision are less clear. While the SAS decision holds that if the PTAB decides to institute a proceeding, it must institute with respect to all claims challenged by Petitioner, the Court's decision left open the question of whether the PTAB will be required to institute on all *grounds* of invalidation set out in a petition. For instance, if a petition challenges a single claim of a patent on multiple grounds of invalidation (i.e., using different combinations of prior references), it is not clear whether the PTAB is required to institute on all grounds contained within the petition. The statutory basis for the Court's holding, 35 U.S.C. § 318, only addresses claims, and the question presented to the Court was directed only to whether the PTAB must decide all claims. However, the Court's decision is based in part on its view that the "petitioner is master of its complaint and normally entitled to judgment on all of the claims it raises, not just those the decision maker wish to address" and that "the statute envisions that a petitioner will seek an inter partes review of a particular kind – one guided by a petition describing 'each claim challenged' and 'the grounds on which the challenge to each claim is based.'" Thus, the Court's decision might also be read to require that, if the Board institutes a challenge, it must institute as to all grounds raised by Petitioner. If that happens, IPRs will become more expensive for all parties involved and the scope of estoppel will be larger for Petitioners as discussed below.

It is unclear how the PTAB will respond to the Court's decision. The PTAB retains considerable discretion as to whether to institute an IPR proceeding, and institution decisions are largely unreviewable. As a result, the PTAB could elect to control its docket by instituting fewer cases. For example, if a Petitioner files two petitions on the same patent, the Board may opt to institute review only one of the two petitions to reduce its workload while still being true to SAS. The PTAB might also opt to issue less thoughtful and complete institution decisions, perhaps stopping once it found that a single claim was likely invalid. Justice Ginsburg, in a dissent to the Court's majority opinion, contemplated that the PTAB could circumvent the Court's ruling and narrow proceedings by denying petitions that contain multiple challenges, and noting in its institution decision which grounds the Board felt were unworthy of institution. In Justice Ginsburg's hypothetical, Petitioners would then be free to file a new petition that removed the challenges that the Board previously had noted were not worthy of institution. Responding to Justice Ginsburg's hypothetical, the majority suggested a court could invalidate "shenanigans" by the PTAB, but would only consider the issue later.

District Court Impact

Even though the Court's decision applies to IPR proceedings before the PTAB, the case will likely have a significant impact on patent cases before district courts. As a preliminary matter, the Court's decision could mean that a district court would be more likely to grant a stay in a pending patent litigation prior to the PTAB's institution decision, since now only one claim needs to be found likely unpatentable to trigger a final written decision from the Board as to all challenged claims.

The Court's decision will also likely have a significant impact on the estoppel effects triggered by final written decision from the PTAB. Section 315(e)(2) estops a petitioner in an IPR from asserting in district court "that the claim is invalid on any ground that the petitioner raised or reasonably could have raised during that inter partes review." District courts have considered estoppel as to three types of invalidity arguments: (1) grounds that were actually instituted in the IPR ("instituted grounds"); (2) grounds that were included in a petition but not instituted ("non-instituted grounds"); and (3) grounds that not were included in a petition ("non-petitioned grounds"). Many courts had found that estoppel did not apply to category (2) grounds, thus permitting those grounds to be litigated in district court even after a petitioner's unsuccessful IPR.

The Supreme Court's holding in *SAS* may eliminate category (2) entirely if the PTAB no longer is able to institute review only on some of the grounds raised in the petition. Thus, by including a ground in an IPR petition, it may become more likely Petitioner will be estopped from raising the ground in the district court. Therefore, going forward, the estoppel risks associated with filing an IPR petition may increase.

Conclusion

Because of the far-reaching implications that the *SAS* decision may have for IPR proceedings and district court litigation, both Petitioners and Patent Owners will need to reevaluate their strategies in conducting IPRs before the PTAB going forward. Petitioners will need to doubly ensure that the unpatentability analysis, including expert testimony, in their petitions are equally strong for independent and dependent claims. Furthermore, this decision may only allow Petitioners to litigate the invalidity of a patent in one forum (either the PTAB or the district court) due to the new "all or nothing" nature of IPR proceedings and its estoppel impacts. Thus, Petitioners will have to make a strategic decision as to which forum to assert their invalidity challenges. Patent Owners will need to reassess their responses to an IPR petition, taking into account the fact that should the Board decide that even one claim has a reasonable likelihood of being invalidated, the Patent Owner may be required to respond to every claim (and perhaps every ground) that was included in the Petition.

[1] See MoFo Client Alert at <https://www.mofo.com/resources/publications/180424-inter-partes-review.html>

SECTION 20

PLENARY SESSION

Cyber-Rights and Cyber- Wrongs: Legal Ethics in a Digital Age



Presented by

Sherman W. Kahn

Mauriel Kapouytian Woods LLP
New York, NY

Joseph V. DeMarco

DeVore and DeMarco LLP
New York, NY

**THE STATE BAR OF CALIFORNIA
STANDING COMMITTEE ON
PROFESSIONAL RESPONSIBILITY AND CONDUCT
FORMAL OPINION NO. 2010-179**

ISSUE: Does an attorney violate the duties of confidentiality and competence he or she owes to a client by using technology to transmit or store confidential client information when the technology may be susceptible to unauthorized access by third parties?

DIGEST: Whether an attorney violates his or her duties of confidentiality and competence when using technology to transmit or store confidential client information will depend on the particular technology being used and the circumstances surrounding such use. Before using a particular technology in the course of representing a client, an attorney must take appropriate steps to evaluate: 1) the level of security attendant to the use of that technology, including whether reasonable precautions may be taken when using the technology to increase the level of security; 2) the legal ramifications to a third party who intercepts, accesses or exceeds authorized use of the electronic information; 3) the degree of sensitivity of the information; 4) the possible impact on the client of an inadvertent disclosure of privileged or confidential information or work product; 5) the urgency of the situation; and 6) the client's instructions and circumstances, such as access by others to the client's devices and communications.

**AUTHORITIES
INTERPRETED:**

Rules 3-100 and 3-110 of the California Rules of Professional Conduct.

Business and Professions Code section 6068, subdivision (e)(1).

Evidence Code sections 917(a) and 952.

STATEMENT OF FACTS

Attorney is an associate at a law firm that provides a laptop computer for his use on client and firm matters and which includes software necessary to his practice. As the firm informed Attorney when it hired him, the computer is subject to the law firm's access as a matter of course for routine maintenance and also for monitoring to ensure that the computer and software are not used in violation of the law firm's computer and Internet-use policy. Unauthorized access by employees or unauthorized use of the data obtained during the course of such maintenance or monitoring is expressly prohibited. Attorney's supervisor is also permitted access to Attorney's computer to review the substance of his work and related communications.

Client has asked for Attorney's advice on a matter. Attorney takes his laptop computer to the local coffee shop and accesses a public wireless Internet connection to conduct legal research on the matter and email Client. He also takes the laptop computer home to conduct the research and email Client from his personal wireless system.

DISCUSSION

Due to the ever-evolving nature of technology and its integration in virtually every aspect of our daily lives, attorneys are faced with an ongoing responsibility of evaluating the level of security of technology that has increasingly become an indispensable tool in the practice of law. The Committee's own research – including conferring with computer security experts – causes it to understand that, without appropriate safeguards (such as firewalls, secure username/password combinations, and encryption), data transmitted wirelessly can be intercepted and read with increasing ease. Unfortunately, guidance to attorneys in this area has not kept pace with technology. Rather than engage in a technology-by-technology analysis, which would likely become obsolete shortly, this

opinion sets forth the general analysis that an attorney should undertake when considering use of a particular form of technology.

1. The Duty of Confidentiality

In California, attorneys have an express duty “[t]o maintain inviolate the confidence, and at every peril to himself or herself to preserve the secrets, of his or her client.”^{1/} (Bus. & Prof. Code, § 6068, subd. (e)(1).) This duty arises from the relationship of trust between an attorney and a client and, absent the informed consent of the client to reveal such information, the duty of confidentiality has very few exceptions. (Rules Prof. Conduct, rule 3-100 & discussion “[A] member may not reveal such information except with the consent of the client or as authorized or required by the State Bar Act, these rules, or other law.”)^{2/}

Unlike Rule 1.6 of the Model Rules of Professional Conduct (“MRPC”), the exceptions to the duty of confidentiality under rule 3-100 do not expressly include disclosure “impliedly authorized in order to carry out the representation.” (MRPC, Rule 1.6.) Nevertheless, the absence of such language in the California Rules of Professional Conduct does not prohibit an attorney from using postal or courier services, telephone lines, or other modes of communication beyond face-to-face meetings, in order to effectively carry out the representation. There is a distinction between actually disclosing confidential information to a third party for purposes ancillary to the representation,^{3/} on the one hand, and using appropriately secure technology provided by a third party as a method of communicating with the client or researching a client’s matter,^{4/} on the other hand.

Section 952 of the California Evidence Code, defining “confidential communication between client and lawyer” for purposes of application of the attorney-client privilege, includes disclosure of information to third persons “to whom disclosure is reasonably necessary for the transmission of the information or the accomplishment of the purpose for which the lawyer is consulted.” (Evid. Code, § 952.) While the duty to protect confidential client information is broader in scope than the attorney-client privilege (Discussion [2] to rule 3-100; *Goldstein v. Lees* (1975) 46 Cal.App.3d 614, 621, fn. 5 [120 Cal.Rptr. 253]), the underlying principle remains the same, namely, that transmission of information through a third party reasonably necessary for purposes of the representation should not be deemed to have destroyed the confidentiality of the information. (See Cal. State Bar Formal Opn. No. 2003-161 [repeating the Committee’s prior observation “that the duty of confidentiality and the evidentiary privilege share the same basic policy foundation: to encourage clients to disclose all possibly pertinent information to their attorneys so that the attorneys may effectively represent the clients’ interests.”].) Pertinent here, the manner in which an attorney acts to safeguard confidential client information is governed by the duty of competence, and determining whether a third party has the ability to access and use confidential client information in a manner that is unauthorized by the client is a subject that must be considered in conjunction with that duty.

2. The Duty of Competence

Rule 3-110(A) prohibits the intentional, reckless or repeated failure to perform legal services with competence. Pertinent here, “competence” may apply to an attorney’s diligence and learning with respect to handling matters for clients. (Rules Prof. Conduct, rule 3-110(B).) The duty of competence also applies to an attorney’s “duty to supervise the work of subordinate attorney and non-attorney employees or agents.” (Discussion to rule 3-110.)

^{1/} “Secrets” include “[a]ny ‘information gained in the professional relationship that the client has requested be held inviolate or the disclosure of which would be embarrassing or would likely be detrimental to the client.’” (Cal. State Bar Formal Opn. No. 1981-58.)

^{2/} Unless otherwise indicated, all future references to rules in this opinion will be to the Rules of Professional Conduct of the State Bar of California.

^{3/} In this regard, compare Cal. State Bar Formal Opn. No. 1971-25 (use of an outside data processing center without the client’s consent for bookkeeping, billing, accounting and statistical purposes, if such information includes client secrets and confidences, would violate section 6068, subdivision (e)), with Los Angeles County Bar Assn. Formal Opn. No. 374 (1978) (concluding that in most circumstances, if protective conditions are observed, disclosure of client’s secrets and confidences to a central data processor would not violate section 6068(e) and would be the same as disclosures to non-lawyer office employees).

^{4/} Cf. Evid. Code, § 917(b) (“A communication . . . does not lose its privileged character for the sole reason that it is communicated by electronic means or because persons involved in the delivery, facilitation, or storage of electronic communication may have access to the content of the communication.”).

With respect to acting competently to preserve confidential client information, the comments to Rule 1.6 of the MRPC^{5/} provide:

[16] A lawyer must act competently to safeguard information relating to the representation of a client against inadvertent or unauthorized disclosure by the lawyer or other persons who are participating in the representation of the client or who are subject to the lawyer's supervision. See Rules 1.1, 5.1 and 5.3.

[17] When transmitting a communication that includes information relating to the representation of a client, the lawyer must take reasonable precautions to prevent the information from coming into the hands of unintended recipients. This duty, however, does not require that the lawyer use special security measures if the method of communication affords a reasonable expectation of privacy. Special circumstances, however, may warrant special precautions. Factors to be considered in determining the reasonableness of the lawyer's expectation of confidentiality include the sensitivity of the information and the extent to which the privacy of the communication is protected by law or by a confidentiality agreement. A client may require the lawyer to implement special security measures not required by this Rule or may give informed consent to the use of a means of communication that would otherwise be prohibited by this Rule.

(MRPC, cmts. 16 & 17 to Rule 1.6.) In this regard, the duty of competence includes taking appropriate steps to ensure both that secrets and privileged information of a client remain confidential and that the attorney's handling of such information does not result in a waiver of any privileges or protections.

3. Factors to Consider

In accordance with the duties of confidentiality and competence, an attorney should consider the following before using a specific technology:^{6/}

- a) The attorney's ability to assess the level of security afforded by the technology, including without limitation:
 - i) Consideration of how the particular technology differs from other media use. For example, while one court has stated that, "[u]nlike postal mail, simple e-mail generally is not 'sealed' or secure, and can be accessed or viewed on intermediate computers between the sender and recipient (unless the message is encrypted)" (*American Civil Liberties Union v. Reno* (E.D.Pa. 1996) 929 F.Supp. 824, 834, aff'd (1997) 521 U.S. 844 [117 S.Ct. 2329]), most bar associations have taken the position that the risks of a third party's unauthorized review of email (whether by interception or delivery to an unintended recipient) are similar to the risks that confidential client information transmitted by standard mail service will be opened by any of the many hands it passes through on the way to its recipient or will be misdirected^{7/} (see, e.g., ABA Formal Opn. No. 99-413^{8/} [concluding that attorneys have a reasonable expectation of privacy in email communications, even if unencrypted, "despite some risk of interception and disclosure"]; Los Angeles County Bar Assn. Formal Opn. No. 514 (2005) ["Lawyers are not required

^{5/} In the absence of on-point California authority and conflicting state public policy, the MRPC may serve as guidelines. (*City & County of San Francisco v. Cobra Solutions, Inc.* (2006) 38 Cal. 4th 839, 852 [43 Cal.Rptr.3d 771].)

^{6/} These factors should be considered regardless of whether the attorney practices in a law firm, a governmental agency, a non-profit organization, a company, as a sole practitioner or otherwise.

^{7/} Rule 1-100(A) provides that "[e]thics opinions and rules and standards promulgated by other jurisdictions and bar associations may . . . be considered" for professional conduct guidance.

^{8/} In 1999, the ABA Committee on Ethics and Professional Responsibility reviewed state bar ethics opinions across the country and determined that, as attorneys' understanding of technology has improved, the opinions generally have transitioned from concluding that use of Internet email violates confidentiality obligations to concluding that use of unencrypted Internet email is permitted without express client consent. (ABA Formal Opn. No. 99-413 [detailing various positions taken in state ethics opinions from Alaska, Washington D.C., Kentucky, New York, Illinois, North Dakota, South Carolina, Vermont, Pennsylvania, Arizona, Iowa and North Carolina].)

to encrypt e-mail containing confidential client communications because e-mail poses no greater risk of interception and disclosure than regular mail, phones or faxes.”]; Orange County Bar Assn. Formal Opn. No. 97-0002 [concluding use of encrypted email is encouraged, but not required].) (See also *City of Reno v. Reno Police Protective Assn.* (2003) 118 Nev. 889, 897-898 [59 P.3d 1212] [referencing an earlier version of section 952 of the California Evidence Code and concluding “that a document transmitted by e-mail is protected by the attorney-client privilege as long as the requirements of the privilege are met.”].)

- ii) Whether reasonable precautions may be taken when using the technology to increase the level of security.^{9/} As with the above-referenced views expressed on email, the fact that opinions differ on whether a particular technology is secure suggests that attorneys should take reasonable steps as a precautionary measure to protect against disclosure.^{10/} For example, depositing confidential client mail in a secure postal box or handing it directly to the postal carrier or courier is a reasonable step for an attorney to take to protect the confidentiality of such mail, as opposed to leaving the mail unattended in an open basket outside of the office door for pick up by the postal service. Similarly, encrypting email may be a reasonable step for an attorney to take in an effort to ensure the confidentiality of such communications remain so when the circumstance calls for it, particularly if the information at issue is highly sensitive and the use of encryption is not onerous. To place the risks in perspective, it should not be overlooked that the very nature of digital technologies makes it easier for a third party to intercept a much greater amount of confidential information in a much shorter period of time than would be required to transfer the same amount of data in hard copy format. In this regard, if an attorney can readily employ encryption when using public wireless connections and has enabled his or her personal firewall, the risks of unauthorized access may be significantly reduced.^{11/} Both of these tools are readily available and relatively inexpensive, and may already be built into the operating system. Likewise, activating password protection features on mobile devices, such as laptops and PDAs, presently helps protect against access to confidential client information by a third party if the device is lost, stolen or left unattended. (See David Ries & Reid Trautz, *Law Practice Today*, “Securing Your Clients’ Data While On the Road,” October 2008 [noting reports that “as many as 10% of laptops used by American businesses are stolen during their useful lives and 97% of them are never recovered”].)
- iii) Limitations on who is permitted to monitor the use of the technology, to what extent and on what grounds. For example, if a license to use certain software or a technology service imposes a requirement of third party access to information related to the attorney’s use of the technology, the attorney may need to confirm that the terms of the requirement or authorization do not permit the third party to disclose confidential client information to others or use such information for any purpose other than to ensure the functionality of the software or that the technology is not being used for an improper purpose, particularly if the information at issue is highly sensitive.^{12/} “Under Rule 5.3 [of the MRPC], a lawyer retaining such an outside service provider is required to make reasonable efforts to ensure that

^{9/} Attorneys also should employ precautions to protect confidential information when in public, such as ensuring that the person sitting in the adjacent seat on an airplane cannot see the computer screen or moving to a private location before discussing confidential information on a mobile phone.

^{10/} Section 60(1)(b) of the Restatement (Third) of The Law Governing Lawyers provides that “a lawyer must take steps reasonable in the circumstances to protect confidential client information against impermissible use or disclosure by the lawyer’s associates or agents that may adversely affect a material interest of the client or otherwise than as instructed by the client.”

^{11/} Similarly, this Committee has stated that if an attorney is going to maintain client documents in electronic form, he or she must take reasonable steps to strip any metadata containing confidential information of other clients before turning such materials over to a current or former client or his or her new attorney. (See Cal. State Bar Formal Opn. 2007-174.)

^{12/} A similar approach might be appropriate if the attorney is employed by a non-profit or governmental organization where information may be monitored by a person or entity with interests potentially or actually in conflict with the attorney’s client. In such cases, the attorney should not use the technology for the representation, absent informed consent by the client or the ability to employ safeguards to prevent access to confidential client information. The attorney also may need to consider whether he or she can competently represent the client without the technology.

the service provider will not make unauthorized disclosures of client information. Thus when a lawyer considers entering into a relationship with such a service provider he must ensure that the service provider has in place, or will establish, reasonable procedures to protect the confidentiality of information to which it gains access, and moreover, that it fully understands its obligations in this regard. [Citation.] In connection with this inquiry, a lawyer might be well-advised to secure from the service provider in writing, along with or apart from any written contract for services that might exist, a written statement of the service provider's assurance of confidentiality.” (ABA Formal Opn. No. 95-398.)

Many attorneys, as with a large contingent of the general public, do not possess much, if any, technological savvy. Although the Committee does not believe that attorneys must develop a mastery of the security features and deficiencies of each technology available, the duties of confidentiality and competence that attorneys owe to their clients do require a basic understanding of the electronic protections afforded by the technology they use in their practice. If the attorney lacks the necessary competence to assess the security of the technology, he or she must seek additional information or consult with someone who possesses the necessary knowledge, such as an information technology consultant.^{13/} (Cf. Rules Prof. Conduct, rule 3-110(C) [“If a member does not have sufficient learning and skill when the legal service is undertaken, the member may nonetheless perform such services competently by 1) associating with or, where appropriate, professionally consulting another lawyer reasonably believed to be competent, or 2) by acquiring sufficient learning and skill before performance is required.”].)

- b) Legal ramifications to third parties of intercepting, accessing or exceeding authorized use of another person’s electronic information. The fact that a third party could be subject to criminal charges or civil claims for intercepting, accessing or engaging in unauthorized use of confidential client information favors an expectation of privacy with respect to a particular technology. (See, e.g., 18 U.S.C. § 2510 et seq. [Electronic Communications Privacy Act of 1986]; 18 U.S.C. § 1030 et seq. [Computer Fraud and Abuse Act]; Pen. Code, § 502(c) [making certain unauthorized access to computers, computer systems and computer data a criminal offense]; Cal. Pen. Code, § 629.86 [providing a civil cause of action to “[a]ny person whose wire, electronic pager, or electronic cellular telephone communication is intercepted, disclosed, or used in violation of [Chapter 1.4 on Interception of Wire, Electronic Digital Pager, or Electronic Cellular Telephone Communications].”]; *eBay, Inc. v. Bidder’s Edge, Inc.* (N.D.Cal. 2000) 100 F.Supp.2d 1058, 1070 [in case involving use of web crawlers that exceeded plaintiff’s consent, court stated “[c]onduct that does not amount to a substantial interference with possession, but which consists of intermeddling with or use of another’s personal property, is sufficient to establish a cause of action for trespass to chattel.”].^{14/})
- c) The degree of sensitivity of the information. The greater the sensitivity of the information, the less risk an attorney should take with technology. If the information is of a highly sensitive nature and there is a risk of disclosure when using a particular technology, the attorney should consider alternatives unless the client provides informed consent.^{15/} As noted above, if another person may have access to the communications transmitted between the attorney and the client (or others necessary to the representation), and may have an interest in the information being disclosed that is in conflict with the client’s interest, the attorney should take precautions to ensure that the person will not be able to access the information or should avoid using the technology. These types of situations increase the likelihood for intrusion.

^{13/} Some potential security issues may be more apparent than others. For example, users of unsecured public wireless connections may receive a warning when accessing the connection. However, in most instances, users must take affirmative steps to determine whether the technology is secure.

^{14/} Attorneys also have corresponding legal and ethical obligations not to invade the confidential and privileged information of others.

^{15/} For the client’s consent to be informed, the attorney should fully advise the client about the nature of the information to be transmitted with the technology, the purpose of the transmission and use of the information, the benefits and detriments that may result from transmission (both legal and nonlegal), and any other facts that may be important to the client’s decision. (Los Angeles County Bar Assn. Formal Opn. No. 456 (1989).) It is particularly important for an attorney to discuss the risks and potential harmful consequences of using the technology when seeking informed consent.

- d) Possible impact on the client of an inadvertent disclosure of privileged or confidential information or work product, including possible waiver of the privileges.^{16/} Section 917(a) of the California Evidence Code provides that “a communication made in confidence in the course of the lawyer-client, physician-patient, psychotherapist-patient, clergy-penitent, husband-wife, sexual assault counselor-victim, or domestic violence counselor-victim relationship ... is presumed to have been made in confidence and the opponent of the claim of privilege has the burden of proof to establish that the communication was not confidential.” (Evid. Code, § 917(a).) Significantly, subsection (b) of section 917 states that such a communication “does not lose its privileged character for the sole reason that it is communicated by electronic means or because persons involved in the delivery, facilitation, or storage of electronic communication may have access to the content of the communication.” (Evid. Code, § 917(b). See also Penal Code, § 629.80 [“No otherwise privileged communication intercepted in accordance with, or in violation of, the provisions of [Chapter 1.4] shall lose its privileged character.”]; 18 U.S.C. § 2517(4) [“No otherwise privileged wire, oral, or electronic communication intercepted in accordance with, or in violation of, the provisions of [18 U.S.C. § 2510 et seq.] shall lose its privileged character.”].) While these provisions seem to provide a certain level of comfort in using technology for such communications, they are not a complete safeguard. For example, it is possible that, if a particular technology lacks essential security features, use of such a technology could be deemed to have waived these protections. Where the attorney-client privilege is at issue, failure to use sufficient precautions may be considered in determining waiver.^{17/} Further, the analysis differs with regard to an attorney’s duty of confidentiality. Harm from waiver of attorney-client privilege is possible depending on if and how the information is used, but harm from disclosure of confidential client information may be immediate as it does not necessarily depend on use or admissibility of the information, including as it does matters which would be embarrassing or would likely be detrimental to the client if disclosed.
- e) The urgency of the situation. If use of the technology is necessary to address an imminent situation or exigent circumstances and other alternatives are not reasonably available, it may be reasonable in limited cases for the attorney to do so without taking additional precautions.
- f) Client instructions and circumstances. If a client has instructed an attorney not to use certain technology due to confidentiality or other concerns or an attorney is aware that others have access to the client’s electronic devices or accounts and may intercept or be exposed to confidential client information, then such technology should not be used in the course of the representation.^{18/}

4. **Application to Fact Pattern**^{19/}

In applying these factors to Attorney’s situation, the Committee does not believe that Attorney would violate his duties of confidentiality or competence to Client by using the laptop computer because access is limited to authorized individuals to perform required tasks. However, Attorney should confirm that personnel have been appropriately instructed regarding client confidentiality and are supervised in accordance with rule 3-110. (See *Crane v. State Bar* (1981) 30 Cal.3d 117, 123 [177 Cal.Rptr. 670] [“An attorney is responsible for the work product of his employees which is performed pursuant to his direction and authority.”]; *In re Complex Asbestos Litig.* (1991) 232 Cal.App.3d 572, 588 [283 Cal.Rptr. 732] [discussing law firm’s ability to supervise employees and ensure they protect client confidences]; Cal. State Bar Formal Opn. No. 1979-50 [discussing lawyer’s duty to explain to

^{16/} Consideration of evidentiary issues is beyond the scope of this opinion, which addresses only the ethical implications of using certain technologies.

^{17/} For example, with respect to the impact of inadvertent disclosure on the attorney-client privilege or work-product protection, rule 502(b) of the Federal Rules of Evidence states: “When made in a Federal proceeding or to a Federal office or agency, the disclosure does not operate as a waiver in a Federal or State proceeding if: 1. the disclosure is inadvertent; 2. the holder of the privilege or protection took reasonable steps to prevent disclosure; and 3. the holder promptly took reasonable steps to rectify the error, including (if applicable) following Federal Rule of Civil Procedure 26(b)(5)(B).” As a practical matter, attorneys also should use appropriate confidentiality labels and notices when transmitting confidential or privileged client information.

^{18/} In certain circumstances, it may be appropriate to obtain a client’s informed consent to the use of a particular technology.

^{19/} In this opinion, we are applying the factors to the use of computers and wireless connections to assist the reader in understanding how such factors function in practice. Use of other electronic devices would require similar considerations.

employee what obligations exist with respect to confidentiality[.]) In addition, access to the laptop by Attorney's supervisor would be appropriate in light of her duty to supervise Attorney in accordance with rule 3-110 and her own fiduciary duty to Client to keep such information confidential.

With regard to the use of a public wireless connection, the Committee believes that, due to the lack of security features provided in most public wireless access locations, Attorney risks violating his duties of confidentiality and competence in using the wireless connection at the coffee shop to work on Client's matter unless he takes appropriate precautions, such as using a combination of file encryption, encryption of wireless transmissions and a personal firewall.^{20/} Depending on the sensitivity of the matter, Attorney may need to avoid using the public wireless connection entirely or notify Client of possible risks attendant to his use of the public wireless connection, including potential disclosure of confidential information and possible waiver of attorney-client privilege or work product protections, and seek her informed consent to do so.^{21/}

Finally, if Attorney's personal wireless system has been configured with appropriate security features,^{22/} the Committee does not believe that Attorney would violate his duties of confidentiality and competence by working on Client's matter at home. Otherwise, Attorney may need to notify Client of the risks and seek her informed consent, as with the public wireless connection.

CONCLUSION

An attorney's duties of confidentiality and competence require the attorney to take appropriate steps to ensure that his or her use of technology in conjunction with a client's representation does not subject confidential client information to an undue risk of unauthorized disclosure. Because of the evolving nature of technology and differences in security features that are available, the attorney must ensure the steps are sufficient for each form of technology being used and must continue to monitor the efficacy of such steps.

This opinion is issued by the Standing Committee on Professional Responsibility and Conduct of the State Bar of California. It is advisory only. It is not binding upon the courts, the State Bar of California, its Board of Governors, any persons, or tribunals charged with regulatory responsibilities, or any member of the State Bar.

^{20/} Local security features available for use on individual computers include operating system firewalls, antivirus and antispam software, secure username and password combinations, and file permissions, while network safeguards that may be employed include network firewalls, network access controls such as virtual private networks (VPNs), inspection and monitoring. This list is not intended to be exhaustive.

^{21/} Due to the possibility that files contained on a computer may be accessed by hackers while the computer is operating on an unsecure network connection and when appropriate local security features, such as firewalls, are not enabled, attorneys should be aware that *any* client's confidential information stored on the computer may be at risk regardless of whether the attorney has the file open at the time.

^{22/} Security features available on wireless access points will vary and should be evaluated on an individual basis.

Fordham International Law Journal

Volume 40, Issue 3

2017

Article 11

A Call To Cyberarms: The International Arbitrator's Duty To Avoid Digital Intrusion

Stephanie Cohen*

Mark Morrill†

*

†

Copyright ©2017 by the authors. *Fordham International Law Journal* is produced by The Berkeley Electronic Press (bepress). <http://ir.lawnet.fordham.edu/ilj>

A CALL TO CYBERARMS: THE INTERNATIONAL ARBITRATOR’S DUTY TO AVOID DIGITAL INTRUSION

Stephanie Cohen & Mark Morril***

I. Introduction	982
II. Data Security Threats in International Arbitration.....	986
III. Sources of the Arbitrator’s Duty to Avoid Intrusion	989
A. Duty of Confidentiality	990
B. Duty to Preserve and Protect the Integrity and Legitimacy of the Arbitral Process.....	994
C. Duty of Competence.....	997
D. Global Data Protection Laws and Regulations	1002
IV. Nature and Scope of the Arbitrator’s Duty to Avoid Intrusion	1004
A. An Umbrella Obligation.....	1004
B. An Interdependent Landscape with Independent Duties..	1005
C. Personal Accountability	1006
D. Continuous and Evolving.....	1009
E. Bounded by Reasonableness	1009
V. Implementing the Duty to Avoid Intrusion.....	1012

* Stephanie Cohen is a Canadian arbitrator of international and domestic commercial disputes based in New York City (www.cohenarbitration.com). Prior to establishing her practice as an arbitrator, she was Counsel in the international arbitration group at White & Case LLP.

** Mark Morril is an independent arbitrator and mediator based in New York City who focuses on complex commercial disputes (www.morriladr.com). Previously, he served as General Counsel of the publisher Simon & Schuster, then the world’s largest English language publisher, as Deputy General Counsel of the global media company Viacom and as a law firm partner.

The authors welcome comments addressed to cohen@cohenarbitration.com and mark.morril@morriladr.com.

A. Keeping Abreast of Developments in Relevant Technology and Understanding Associated Benefits and Risks.....	1013
B. Implementing Baseline Security	1014
C. Taking a Thoughtful Approach to Assets and Architecture	1015
D. Planning for a Data Breach	1017
E. Case Management Considerations	1018
VI. Looking to the Future	1019

I. INTRODUCTION

International commercial arbitration rests on certain fundamental attributes that cut across the different rule sets and cultural and legal systems in which it operates. There is common ground that any international commercial arbitration regime must encompass integrity and fairness, uphold the legitimate expectations of commercial parties, and respect essential elements of due process such as equal treatment of the parties, a fair opportunity for each party to present its case and neutral adjudicatory proceedings, untainted by illegal conduct.¹

The system and its integrity depend substantially on the role of the arbitrator. As Professor Rogers has stated: [T]he authoritative nature of adjudicatory outcomes, as well as their existence within a larger system, imposes on adjudicators an obligation to preserve the integrity and legitimacy of the adjudicatory system in which they operate.² Cyberbreaches of the arbitral process, including intrusion

1. See e.g., UNCITRAL MODEL LAW ON INT'L COM. ARB., art. 18 (1985) [hereinafter UNCITRAL Model Law], ("The parties shall be treated with equality and each party shall be given a full opportunity of presenting his case."); Convention on the Recognition and Enforcement of Foreign Arbitral Awards, art. V(1)(b) (1958) (party inability to present case is grounds to refuse recognition and enforcement of an award); ENGLISH ARBITRATION ACT 1, § 33 (1996) (general duty of tribunal); LONDON CT. OF INT'L ARB., LCIA ARBITRATION RULES (2014) [hereinafter LCIA RULES] art. 14.4 (conduct of proceedings); William Park, *Arbitrators and Accuracy*, 1 J. OF INT'L DISP. SETTLEMENT 43, note 89 (2010) (arbitrators rejecting complicity with money laundering, fake arbitrations, and other illicit schemes.); LEADING ARBITRATORS' GUIDE TO INTERNATIONAL ARBITRATION 485 (Lawrence W. Newman & Richard D. Hill eds., 3d ed., 2014); Klaus Peter Berger & J. Ole Jensen, *Due Process Paranoia and the Procedural Judgment Rule: a Safe Harbour for Procedural Management Decisions by International Arbitrators*, 32 (3) ARB. INT'L 415 (2016).

2. CATHERINE ROGERS, ETHICS IN INTERNATIONAL ARBITRATION 283 (2014).

into arbitration-related data and transmissions, pose a direct and serious threat to the integrity and legitimacy of the process.³ This article posits that the arbitrator, as the presiding actor, has an important, front-line duty to avoid intrusion into the process.

The focus here on cyberintrusion into the arbitral process does not imply that international arbitration is uniquely vulnerable to data breaches, but only that international arbitration proceedings are not immune to increasingly pervasive cyberattacks against corporations, law firms, government agencies and officials and other custodians of large electronic data sets of sensitive information.⁴ Similarly, our focus on the role and responsibilities of the arbitrator should not obscure that cybersecurity is a shared responsibility and that other actors have independent obligations.⁵ Arbitrators are not uniquely vulnerable to data breaches and are not guarantors of cybersecurity.⁶ In the highly interdependent landscape of international commercial arbitration, data associated with any arbitration matter will only be as secure as the weakest link. Since data security ultimately depends on the responsible conduct and vigilance of individuals, any individual

3. Though we focus primarily on the threat of data breaches, the analysis here is generally applicable to other forms of unauthorized digital intrusion in proceedings, such as surreptitious surveillance of a hearing or of arbitration counsel in their offices, or the inadvertent recording and disclosure of an otherwise private conversation between members of the tribunal.

4. See *infra* Part II.

5. Most notably, counsel have ethical duties to protect client confidentiality and to keep abreast of the risks and benefits of technology related to their practice. Further, all actors in the process may have contractual or regulatory obligations to protect sensitive personal or commercial information. See *infra* Sections III.A and III.C.

6. High profile examples of arbitration-related cyberattacks or data breaches have involved arbitral institutions, counsel, and parties as targets. See Zachary Zagger, *Hackers Target Anti-Doping, Appeals Bodies Amid Olympics*, LAW360.COM, (Aug. 12, 2016), <https://www.law360.com/articles/827962/hackers-target-anti-doping-appeals-bodies-amid-olympics> (reporting that hackers attempted to infiltrate the website of the Court of Arbitration for Sport during the Rio Olympic Games); Alison Ross, *Tribunal Rules on Admissibility of Hacked Kazakh Emails*, GLOBAL ARBITRATION REV., (Sept. 22, 2015), <http://globalarbitrationreview.com/article/1034787/tribunal-rules-on-admissibility-of-hacked-kazakh-emails> (reporting that privileged e-mails between a government and its arbitration counsel were disclosed by hackers of the government's internal network); Alison Ross, *Cybersecurity and Confidentiality Shocks for PCA*, GLOBAL ARBITRATION REV., (July 23, 2015), <http://globalarbitrationreview.com/article/1034637/cybersecurity-and-confidentiality-shocks-for-the-pca> (reporting that the Permanent Court of Arbitration website was hacked during a hearing of China-Philippines arbitration and counsel in a Russia-related arbitration received "Trojan downloaders" that, if opened, would have enabled hackers to listen in on conversations).

actor can be that weak link, whatever their practice setting, whatever the infrastructure they rely upon, and whatever role they play in an arbitration.⁷

We explore in Part II the threat that cybersecurity breaches pose to international commercial arbitrations, using some examples of high-profile breaches that already have occurred.⁸ We analyze in Part III the obligations that underpin the arbitrator's duty to avoid intrusion. That duty, in our view, need not be created anew. Rather, it rests securely on well-established duties of arbitrators to safeguard both the confidentiality and the legitimacy and integrity of proceedings, as well as to be competent to handle each individual matter.⁹ In an era of significant cyberthreats to the international commercial arbitration process, the duty to avoid intrusion is an inherent duty that follows as a matter of necessity from these earlier identified duties.

We then discuss, in Part IV, the nature and scope of the arbitrator's duty to avoid intrusion, which is bounded and fulfilled by taking reasonable measures to prevent unauthorized digital access to arbitration-related information. There is no bright line list of measures that will fulfill the duty. Rather, assessment of the cybersecurity necessary in international commercial arbitration is an ongoing, risk-

7. The impact of individual conduct on cybersecurity has been highlighted in recent high profile security breaches. *See, e.g.*, Gregory Krieg & Tal Kopan, *Is This the Email That Hacked John Podesta's Account?*, CNN (Oct. 28, 2016), <http://www.cnn.com/2016/10/28/politics/phishing-email-hack-john-podesta-hillary-clinton-wikileaks/index.html>; Eric Lipton, et al., *The Perfect Weapon: How Russian Cyberpower Invaded the United States*, N.Y. TIMES (Dec. 13, 2016), <http://www.nytimes.com/2016/12/13/us/politics/russia-hack-election-dnc.html?smprod=nytcore-ipad&smid=nytcore-ipad-share>; Tom Vanden Brook & Michael Winter, *Hackers Penetrated Pentagon E-mail*, USA TODAY (Aug. 7, 2015), <http://www.usatoday.com/story/news/nation/2015/08/06/russia-reportedly-hacks-pentagon-email-system/31228625>; Tom Fox-Brewster, *Sony Needed to Have Basic Digital Protection. It Failed*, THE GUARDIAN (Dec. 20, 2014), <https://www.theguardian.com/commentisfree/2014/dec/21/sony-hacking-north-korea-cyber-security>.

8. Although the focus of this article is on international commercial arbitration, many of the considerations discussed here will apply as well in investor-state and public international arbitration. Notably, some of the high profile data security breaches discussed in this article occurred in those contexts. *See supra* note 6. At the same time, however, there may be important differences between the scope of the arbitrator's duty to avoid intrusion in the two regimes owing to the public interest in investor-state arbitration and initiatives to increase transparency in the settlement of investor-state disputes. *See, e.g.*, UN Convention on Transparency in Treaty-Based Investor-State Arbitration (2015).

9. *See* William Park, *The Four Musketeers of Arbitral Duty: Neither One-For-All No All-For-One*, 8 ICC DOSSIERS 24 (2011).

based process that requires all participating individuals to understand data security threats in context. As threats evolve, participants must know their own digital architecture and security vulnerabilities (including those that arise from their personal day-to-day work habits) in order to implement protective measures responsive to the threats that apply to their data landscape and individual matters.

The specific protective measures required to satisfy the duty will depend on an analysis of the security risks and on the measures that are practically available, as both will undoubtedly evolve from time to time. They will also depend upon considerations of convenience, cost and efficiency, as the arbitrator may need to balance the duty to avoid intrusion against other duties, including the duty to conduct proceedings in an expeditious and cost-effective manner¹⁰ and, in the absence of overriding considerations, consistent with the parties' choices.¹¹

Finally, in Part V, we address some practical considerations for arbitrators as they determine what measures to implement to avoid intrusion and, in Part VI, suggest for future dialogue some ways in which all participants in the international commercial arbitration system may collaborate to address the ongoing threats. The fundamentals of effective cybersecurity management are accessible and not unduly burdensome. The arbitrator who keeps abreast of risks and benefits of technology in the arbitration process, is conscious of his or her digital assets and infrastructure, and who implements

10. See INT'L CHAMBER OF COMMERCE [ICC], RULES OF ARBITRATION (2017) [hereinafter ICC RULES], art. 22(1) (tribunal shall make every effort to conduct the arbitration in an expeditious and cost-effective manner); INT'L CTR. FOR DISP. RES., INTERNATIONAL CENTRE FOR DISPUTE RESOLUTION INTERNATIONAL ARBITRATION RULES (2014) [hereinafter ICDR RULES], art. 20(2) ("The tribunal shall conduct the proceedings with a view to expediting the resolution of the dispute"); LCIA RULES, *supra* note 1, at art. 14.4(ii) (tribunal's general duty to adopt suitable procedures, avoiding unnecessary delay or expense, so as to provide a fair and efficient means for the final resolution of the parties' dispute).

11. See, e.g., UNCITRAL Model Law, *supra* note 1, at art. 34(2)(a)(iv) (award may be set aside if "the arbitral procedure was not in accordance with the parties' agreement, unless such agreement was in conflict with a provision of this Law from which the parties cannot derogate"); LCIA RULES, *supra* note 1, at art. 14.2 ("The parties may agree on joint proposals for the conduct of their arbitration for consideration by the Arbitral Tribunal. They are encouraged to do so in consultation with the Arbitral Tribunal and consistent with the Arbitral Tribunal's general duties . . ."); ICDR RULES, *supra* note 10, at 1 (rules apply "subject to modifications that the parties may adopt in writing" except that "where any rule[] is in conflict with any provision of the law applicable to the arbitration from which the parties cannot derogate, that provision shall prevail").

reasonable protective measures, will readily meet the obligation to avoid intrusion.

II. DATA SECURITY THREATS IN INTERNATIONAL ARBITRATION

Cyberintrusion, or hacking as it is more commonly known, is often in the news in respect to geo-politics¹² and major corporate and government records data breaches.¹³ Law firms, too, are increasingly

12. See, e.g., U.S. Federal Bureau of Investigation and U.S. Department of Homeland Security, Joint Analysis Report, *GRIZZLY STEPPE-Russian Malicious Cyber Activity*, JAR-16-20296A (2016), https://www.us-cert.gov/sites/default/files/publications/JAR_16-2029_6A_GRIZZLY%20STEPPE-2016-1229.pdf (providing technical details regarding the tools and infrastructure used by the Russian civilian and military intelligence services to compromise and exploit networks and endpoints associated with the US election); David E. Sanger & Mark Mazzetti, *U.S. Had Cyberattack Plan if Nuclear Dispute Led to Conflict*, N.Y. TIMES (Feb. 16, 2016), <https://www.nytimes.com/2016/02/17/world/middleeast/us-had-cyberattack-planned-if-iran-nuclear-negotiations-failed.html>;

13. See, e.g., Vinu Goel and Nicole Perloth, *Yahoo Says 1 Billion Accounts Were Hacked*, N.Y. TIMES (Dec. 14, 2016), https://www.nytimes.com/2016/12/14/technology/yahoo-hack.html?_r=0 (stating that following a September 2016 disclosure that sensitive personal information associated with 500 million users was stolen in late 2014 in an apparently state-sponsored attack, Yahoo disclosed that a separate 2013 attack compromised more than one billion users.); Kevin McCoy, *Cyber Hack Got Access to Over 700,000 IRS Accounts*, USA TODAY (Feb. 26, 2016), <http://www.usatoday.com/story/money/2016/02/26/cyber-hack-gained-access-more-than-700000-irs-accounts/80992822/>; James Billington, *Hackers Carry Out \$55M Cyber Heist From Boeing Aerospace Parts Manufacturer*, INT'L BUS. TIMES (Jan. 27, 2016), <http://www.ibtimes.co.uk/hackers-carry-out-55m-cyber-heist-boeing-aerospace-parts-manufacturer-1540455>; Ahiza Garcia, *Target Settles for \$39 Million Over Data Breaches*, CNN (Dec. 2, 2015), <http://money.cnn.com/2015/12/02/news/companies/target-data-breach-settlement/> (noting that the 2013 hack of Target database compromised roughly forty million customers); Julie Hirschfield Davis, *Hacking of Government Computers Exposed 21.5 Million People*, N.Y. TIMES (July 9, 2015), <https://www.nytimes.com/2015/07/10/us/office-of-personnel-management-hackers-got-data-of-millions.html>; Anna Wilde Mathews, *Anthem: Hacked Database Included 78.8 Million People*, WALL ST. J. (Feb. 24, 2015), <http://www.wsj.com/articles/anthem-hacked-database-included-78-8-million-people-1424807364>. See generally Verizon, 2016 Data Breach Investigations Report [hereinafter Verizon Report], <http://www.verizonenterprise.com/verizon-insights-lab/dbir/2016/> (last visited Jan. 22, 2017) (analyzing a dataset provided by security service providers, law enforcement, and government agencies of more than 100,000 security incidents in 2015, revealing 3,141 confirmed data breaches in eighty-two countries); PricewaterhouseCoopers, Key Findings from the Global State of Information Security Survey (2017), <http://www.pwc.com/gx/en/issues/cyber-security/information-security-survey/assets/gsiss-report-cybersecurity-privacy-possibilities.pdf> [hereinafter PWC Report]; Sarah Kuranda, *New Federal Budget Proposal Raises Government Security Spending* (Feb. 9, 2016), <http://www.crn.com/print/news/security/300079648/new-federal-budget-proposal-raises-government-security-spending-ops-opportunity-for-vars.htm> (referencing hacks of United

reported as having fallen victim to cyberattacks.¹⁴ As awareness increases that corporations and players in the legal sector are attractive targets for cybercriminals, the multiple players involved in international private commercial arbitrations should realize that they too are vulnerable to cybercriminals.¹⁵ International commercial arbitrations routinely involve sensitive commercial and personal information, including information that is not publicly available and that has a potential to move markets or impact competition. Conveniently for hackers, this information is culled together in large data sets, ranging from pleadings and documents produced in disclosure, documentary evidence, witness statements, expert reports, memorials, transcripts, attorney work product, tribunal deliberation materials, and case management data. As the multiple players involved often live in different countries, the information is frequently exchanged and stored in electronic form, making it vulnerable to malevolent outside actors.

Data custodians, who hold sensitive data to varying degrees, include arbitral institutions, counsel, the parties and members of the arbitral tribunal (along with their respective support staff), as well as experts and vendors, including court reporters, translation services, couriers, and information technology (“IT”) professionals, among others. Hackers may attack individual actors directly¹⁶ or the digital

States Office of Personnel Management records and email accounts of the Director of the CIA and the Secretary of Homeland Security).

14. See, e.g., Nate Raymond, *U.S. Accuses Chinese Citizens of Hacking Law Firms*, INSIDER TRADING (Dec. 28, 2016), <http://www.reuters.com/article/us-cyber-insidertrading-idUSKBN14G1D5>; Michael Schmidt and Steven Lee Myers, *Panama Law Firm’s Leaked Files Detail Offshore Accounts Tied to World Leaders*, N.Y. TIMES (Apr. 3, 2016), <https://www.nytimes.com/2016/04/04/us/politics/leaked-documents-offshore-accounts-putin.html> (reporting that 11.5 million documents leaked from Panama law firm exposed the offshore accounts of 140 politicians and public officials). See also New York State Bar Ass’n Ethics Opinion 1019 (Aug. 2014) (“Cyber-security issues have continued to be a major concern for lawyers, as cyber-criminals have begun to target lawyers to access client information, including trade secrets, business plans and personal data. Lawyers can no longer assume that their document systems are of no interest to cyber-crooks.”).

15. For an overview of the major cyber risks in the practice of international arbitration and the tradecraft of the principal threat actors (hacktivists, state actors, and criminals), see James Pastore, *Practical Approaches to Cybersecurity in Arbitration*, 40 FORDHAM INT’L L.J. 1023 (2017). See also Verizon Report, *supra* note 13.

16. A prevalent method of attack that capitalizes on human error is ransomware, a form of malware frequently distributed through spear phishing e-mails sent to targeted individuals. The FBI explains:

infrastructure of their organizations.¹⁷ Moreover, each smartphone, tablet, laptop, thumb drive, other digital device, and cloud service used for the transmission or hosting of arbitration-related data offers a potential portal for unauthorized outsiders to gain access.

The participants in international commercial arbitrations are, to a large degree, digitally interdependent, in that the process typically involves the transmission and hosting of data and collaborative elements such as communications relating to the arbitration. Consequently, any break in the custody of sensitive data has the potential to affect all participants. Indeed, since participants will frequently play host not only to their own sensitive data, but also to the sensitive data of others, intrusion into data held by one participant may injure another more than the one whose data security was compromised.

Unauthorized access of sensitive data may result in the disclosure, or even acceptance into evidence of, illegally obtained, confidential, or privileged matter in ways that undermine fundamental elements of the adjudicatory process and its baseline due process elements.¹⁸ Disclosure of commercially sensitive information, trade

[V]ictims—upon seeing an e-mail addressed to them—will open it and may click on an attachment that appears legitimate, like an invoice or an electronic fax, but which actually contains the malicious ransomware code. Or the e-mail might contain a legitimate-looking URL, but when a victim clicks on it, they are directed to a website that infects their computer with malicious software. Once the infection is present, the malware begins encrypting files and folders on local drives, any attached drives, backup drives, and potentially other computers on the same network that the victim computer is attached to. Users and organizations are generally not aware they have been infected until they can no longer access their data or until they begin to see computer messages advising them of the attack and demands for a ransom payment in exchange for a decryption key.

FBI, *Cyber Crime*, <https://www.fbi.gov/investigate/cyber> (last visited Jan. 16, 2017).

17. In a July 2015 “watering hole” attack, for example, hackers implanted a malicious Adobe Flash file on the Permanent Court of Arbitration’s website that allowed them to infect the computer systems of website visitors who had not patched a known Adobe Flash security flaw. Luke Eric Peterson, *Permanent Court of Arbitration Website Goes Offline, with Cyber-Security Firm Contending that Security Flaw was Exploited in Concert with China-Philippines Arbitration*, IA REP. (July 23, 2015), <http://www.iareporter.com/articles/permanent-court-of-arbitration-goes-offline-with-cyber-security-firm-contending-that-security-flaw-was-exploited-in-lead-up-to-china-philippines-arbitration>.

18. See Alison Ross, *Tribunal Rules on Admissibility of Hacked Kazakh Emails*, GAR (Sept. 22, 2015) (reporting on unpublished order in *Caratube International Oil Co. LLP and Devincei Salah Hourani v. Republic of Kazakhstan*, ICSID Case No. ARB/13/13, admitting into evidence certain documents obtained from the public disclosure of documents hacked

secrets, or personal information may violate laws or contractual commitments in business-to-business or customer agreements, cause serious reputational and economic harm to individuals or businesses,¹⁹ trigger regulatory sanctions²⁰ or negligence claims,²¹ and impact the integrity of public securities markets.²² Further, since the parties, counsel and arbitrators frequently reside in different countries and may be subject to differing data security law, privacy regimes and ethical standards, the legal effect of a data breach may be uncertain and complex.²³ Last, and not least, data security breaches, particularly those resulting from a failure to implement reasonable security protocols, threaten to undermine public confidence in the very institution of international private commercial arbitration. We explore the latter consequence further below.

III. SOURCES OF THE ARBITRATOR'S DUTY TO AVOID INTRUSION

The arbitration rules, ethical codes, practice guidelines, and national laws that govern international commercial arbitration do not, by and large, establish an express duty for arbitrators or any other participant in the arbitral process to implement cybersecurity

from Kazakhstan's government computer network, yet excluding other documents on the basis of privilege).

19. See, e.g., Michael Cieply and Brooks Barnes, *Sony Hacking Fallout Includes Unraveling of Relationships in Hollywood*, N.Y. TIMES (Dec. 18, 2014), <https://www.nytimes.com/2014/12/19/business/media/sony-attack-is-unraveling-relationships-in-hollywood.html>.

20. See, e.g., *FINRA Fines Lincoln Financial Sub \$650,000 for Cybersecurity Shortcomings*, NAT'L L. REV. (Nov. 24, 2016), <http://www.natlawreview.com/article/finra-fines-lincoln-financial-sub-650000-cybersecurity-shortcomings>.

21. See, e.g., Robert Burnson, *Yahoo's Massive Data Breach Draws Negligence Suits by Users*, BLOOMBERG TECH. (Sept. 23, 2016), <https://www.bloomberg.com/news/articles/2016-09-23/yahoo-s-massive-data-breach-draws-negligence-lawsuit-by-user>; See also *Shore et al. v. Johnson & Bell, Ltd.*, No. 1:16-cv-04363 (Verified Complaint) (N.D. Ill. Apr. 15, 2016) (class action alleging a Chicago law firm was negligent and engaged in malpractice by using security practices that left client information vulnerable to hacking, including, for example, a ten year-old time-entry system that had not been updated with security patches).

22. Nate Raymond, *U.S. Accuses Chinese Citizens of Hacking Law Firms*, INSIDER TRADING (Dec. 28, 2016), <http://www.reuters.com/article/us-cyber-insidertrading-idUSKBN14G1D5> (reporting criminal charges for trading on confidential corporate information obtained by hacking into networks and servers of law firms working on mergers).

23. See *Cybersecurity and Arbitration: Protecting Your Documents and Ensuring Confidentiality*, NYSBA INSIDE (2016).

measures.²⁴ Why, then, does the arbitrator bear responsibility to avoid cybersecurity breaches? In our view, the arbitrator's duty to avoid intrusion rests on well-established arbitral duties: (i) the duty to protect the confidentiality and privacy of the proceedings, which will vary in different arbitrations, but exists to some degree in all proceedings; (ii) a fundamental duty to preserve and protect the integrity and legitimacy of the arbitral process; and (iii) a duty to be competent. In addition to these general duties, some arbitrators may have express or implied cybersecurity obligations by virtue of attorney codes of conduct, national data protection laws or regulations, or agreement with the parties.

A. Duty of Confidentiality

It is by now well-established that although parties generally have a right to keep international commercial arbitrations private (i.e., to exclude third parties from hearings),²⁵ it cannot be assumed that they have a general duty or right to keep arbitration-related information confidential (i.e., to refrain from disclosing, and to keep others from disclosing, such information to third parties).²⁶ Arbitrators are on slightly different footing. Although applicable law,²⁷ governing

24. See Section III.C for a discussion of the ethical obligations of lawyers under the ABA Model Rules of Professional Conduct, which regulate attorney conduct.

25. See Simon Crookenden, *Who Should Decide Arbitration Confidentiality Issues?* 25 *ARB. INT'L* 603, 603 (2009) ("The privacy of arbitration proceedings is generally recognised internationally."); see also, e.g., ICC RULES, *supra* note 10, at art. 26(3): ("... Save with the approval of the arbitral tribunal and the parties, persons not involved in the proceedings shall not be admitted."); ICDR RULES, *supra* note 10, at art. 23(6) ("Hearings are private unless the parties agree otherwise or the law provides to the contrary."); LCIA RULES, *supra* note 1, at art. 19.4: ("All hearings shall be held in private, unless the parties agree otherwise in writing."); SINGAPORE INT'L ARB. CTR., *ARBITRATION RULES OF THE SINGAPORE INTERNATIONAL ARBITRATION CENTRE* (2016) [hereinafter *SIAC RULES*], art. 24.4 ("Unless otherwise agreed by the parties, all meetings and hearings shall be in private, and any recordings, transcripts, or documents used in relation to the arbitral proceedings shall remain confidential.").

26. UNCITRAL Notes on Organizing Arbitral Proceedings, ¶ 50 (2016) [hereinafter *UNCITRAL Notes*], ("there is no uniform approach in domestic laws or arbitration rules regarding the extent to which participants in an arbitration are under a duty to observe the confidentiality of information relating to the arbitral proceedings"); L. Yves Fortier, *The Occasionally Unwarranted Assumption of Confidentiality*, 15 *ARB. INT'L* 131 (1999); Leon Trakman, *Confidentiality in International Commercial Arbitration*, 18 *ARB. INT'L* 1 (2002).

27. More often than not, whether an arbitrator has a duty of confidentiality is not addressed by national legislation. See BORN, *INTERNATIONAL COMMERCIAL ARBITRATION* 2003 (Wolters Kluwer, 2d ed. 2014); see also Joshua Karton, *A Conflict of Interests: Seeking a*

arbitration rules,²⁸ and party agreement may vary in the extent to which they obligate an arbitrator to keep *all* aspects of an arbitration proceeding confidential, it is uncontroversial that the arbitrator has a fundamental duty to keep at least *certain aspects* of a proceeding confidential. Gary Born takes a broad view of the confidentiality obligation, stemming from the arbitrator's adjudicatory role:

Even where confidentiality obligations are not imposed upon the parties by either their agreement or applicable national law, the arbitrators are subject to separate confidentiality obligations by virtue of their adjudicative function. One element of the arbitrator's role is the duty to maintain the confidentiality of the parties' written and oral submissions, evidence and other materials submitted in the arbitration. It is generally inconsistent with the arbitrator's mandate to disclose materials from the arbitration to third parties.²⁹

The AAA/ABA *Code of Ethics for Arbitrators in Commercial Disputes* is consistent with this view. Canon VI provides that “[a]n

Way Forward on Publication of International Arbitral Awards, 28 ARB. INT'L 447, 450 (2012).

28. Although they differ in scope, most institutional international arbitration rules, with the notable exception of the ICC Rules, impose an express obligation of confidentiality on arbitrators. *See, e.g.*, ICDR RULES, *supra* note 10, at art. 37(1) (“Confidential information disclosed during the arbitration by the parties or by witnesses shall not be divulged by an arbitrator [T]he members of the arbitral tribunal . . . shall keep confidential all matters relating to the arbitration or the award.”); LCIA RULES, *supra* note 1, at art. 30.2 (“The deliberations of the Arbitral Tribunal shall remain confidential to its members”); SIAC RULES, *supra* note 25, at art. 39.1 (“Unless otherwise agreed by the parties, a party and any arbitrator, including any Emergency Arbitrator . . . shall at all times treat all matters relating to the proceedings and the Award as confidential. The discussions and deliberations of the Tribunal shall be confidential.”), art. 39.3 (“ . . . matters relating to the proceedings” includes the existence of the proceedings, and the pleadings, evidence and other materials in the arbitral proceedings and all other documents produced by another party in the proceedings or the Award arising from the proceedings, but excludes any matter that is otherwise in the public domain”); JAMS FOUNDATION, JAMS INTERNATIONAL ARBITRATION RULES (2016), art. 17.1 (“Unless otherwise required by law, or unless the parties expressly agree, the Tribunal, the Administrator and JAMS International will maintain the confidentiality of the arbitration.”), art. 17.2 (“Unless otherwise required by law, an award will remain confidential, unless all of the parties consent to its publication.”); INT'L INST. FOR CONFLICT PREVENTION & RES., CPR 2014 RULES FOR ADMINISTERED ARBITRATION OF INTERNATIONAL DISPUTES (2014) [hereinafter CPR RULES], art. 20 (“Unless the parties agree otherwise, the parties, the arbitrators and CPR shall treat the proceedings, any related disclosure and the decisions of the Tribunal, as confidential”). *But see* ICC RULES, *supra* note 10, at app. I, art. 6 (“The work of the [ICC] Court is of a confidential nature which must be respected by everyone who participates in that work in whatever capacity.”).

29. BORN, *supra* note 27, at 2004.

arbitrator should be faithful to the relationship of trust and confidentiality inherent in that office.”³⁰ In particular, the arbitrator has a duty to “keep confidential all matters relating to the arbitration proceedings and decision” and “[i]n a proceeding in which there is more than one arbitrator, . . . [not to] inform anyone about the substance of the deliberations of the arbitrators.”³¹ Less comprehensively, the *IBA Rules of Ethics for Arbitrators* specify that the “deliberations of the arbitral tribunal and the contents of the award itself, remain confidential in perpetuity unless the parties release the arbitrators from this obligation.”³² At the same time, however, they encapsulate a general duty of confidentiality by stating that arbitrators should be “discreet.”³³

In contrast to arbitrators, who are thus bound by a duty of confidentiality,³⁴ the parties themselves may not have a *duty* to keep

30. Similarly, the Chartered Institute of Arbitrators Code of Professional and Ethical Conduct for Members (Oct. 2009) provides: “A member shall abide by the relationship of trust which exists between those involved in the dispute and (unless otherwise agreed by all the parties, or permitted or required by applicable law), both during and after completion of the dispute resolution process, shall not disclose or use any confidential information acquired in the course of or for the purposes of the process.” CHARTERED INST. OF ARBITRATORS, THE CHARTERED INSTITUTE OF ARBITRATORS CODE OF PROFESSIONAL AND ETHICAL CONDUCT FOR MEMBERS (Oct. 2009) [hereinafter CIARB ETHICS CODE], Rule 8.

31. AAA/ABA CODE OF ETHICS FOR ARBITRATORS IN COMMERCIAL DISPUTES, Canon VI (B), (C). *See also* Canon I (I) (“An arbitrator who withdraws prior to the completion of the arbitration, whether upon the arbitrator’s initiative or upon the request of one or more of the parties, should take reasonable steps to protect the interests of the parties in the arbitration, including return of evidentiary materials and protection of confidentiality.”).

32. INT’L BAR ASSOC., IBA RULES OF ETHICS FOR ARBITRATORS, article 9. The IBA Rules of Ethics are not binding, but are deemed to reflect internationally acceptable guidelines developed by practicing lawyers from all continents. *Id.* at Introductory Note.

33. *Id.*

34. We note that while many arbitrators are lawyers and will have professional ethical obligations to preserve client confidentiality, by their terms, such obligations apply only when a lawyer is acting in a representative capacity for a client and not when serving as an arbitrator, who does not represent any party but has equal duties to all. BORN, *supra* note 27 at 1970; CPR-Georgetown Commission on Ethics and Standards in ADR, Proposed New Model Rule of Professional Conduct Rule 4.5: The Lawyer as Third-Party Neutral (2002), Rule 4.5.2, comments [1], [3]. Nonetheless, to the extent that lawyers’ duties of confidentiality have been updated to take account of cyberthreats, analysis of those duties may inform how the international arbitrator should view the nature and scope of his or her duty to avoid intrusion. *See, e.g.*, U.K. Information Commission Office, Monetary Penalty Notice under the Data Protection Act 1998, Supervisory Powers of the Information Commissioner (Mar. 10, 2017), <https://ico.org.uk/media/action-veve-taken/mpns/2013678/mpn-data-breach-barrister-20170316.pdf> (fining UK family law barrister for failing to take “appropriate technical

arbitration proceedings or certain aspects of them confidential. Nonetheless, there is a common *expectation* among users of international commercial arbitration³⁵ that the overall process will be confidential.³⁶ More specifically, parties and institutions expect that the arbitrator will maintain the confidentiality of the arbitration.³⁷

measures against the unauthorised or unlawful processing of personal data” in relation to confidential client files where the barrister failed to encrypt such files on her home computer and her husband inadvertently made the files accessible on an online directory while attempting to update software, noting that the Bar Council and barrister’s chambers had issued guidance to barristers that a computer used by family members or others may require encryption of files to prevent unauthorized access to confidential material by shared users).

35. Notably, expectations of privacy and confidentiality may differ in investor-state arbitration. As explained in the UNCITRAL Notes on Organizing Arbitral Proceedings:

[t]he specific characteristics of investor-State arbitration arising under an investment treaty have prompted the development of transparency regimes for such arbitrations. The investment treaty under which the investor-State arbitration arises may include specific provisions on publication of documents, open hearings, and confidential or protected information. In addition, the applicable arbitration rules referred to in those investment treaties may contain specific provisions on transparency. Further, parties to a treaty-based arbitration may agree to apply certain transparency provisions.

UNCITRAL Notes, *supra* note 26, at ¶ 55.

36. Paul D. Friedland, *Arbitration Clauses for International Contracts* 21 (Juris, 2d ed. 2007) (“Notwithstanding the usual absence of prohibitions on party disclosure, there is an expectation and tradition of confidentiality in arbitration, which a party violates at its own peril vis-à-vis the arbitrators.”); Queen Mary Univ. of London Sch. of Int’l Arb., 2010 International Arbitration Survey: Choices in International Arbitration, at 29, http://www.whitecase.com/files/upload/fileRepository/2010International_Arbitration_Survey_Choices_in_International_Arbitration.pdf, 29 (Fifty percent of corporations indicated that they “consider that arbitration is confidential even where there is no specific clause to that effect in the arbitration rules . . . or agreement”); Int’l Inst. for Conflict Prevention & Res., General Commentary for CPR Rules for Administered Arbitration of International Disputes, *available at* <https://www.cpradr.org/resource-center/rules/international-other/arbitration/international-administered-arbitration-rules> (“Parties that choose arbitration over litigation of an international dispute do so primarily to avoid the unfamiliarity and uncertainty of litigation in a foreign court; also out of a need or desire for a proceeding that is confidential and relatively speedy.”); ICC International Court of Arbitration, Note to Parties and Arbitral Tribunals on the Conduct of the Arbitration under the ICC Rules of Arbitration, ¶ 27 (July 13, 2016) (“The [ICC] Court endeavors to make the arbitration process more transparent in ways that do not compromise expectations of confidentiality that may be important to parties.”)

37. UNCITRAL Notes, *supra* note 26, at ¶ 53 (“Whereas the obligation of confidentiality imposed on the parties and their counsel may vary with the circumstances of the case as well as the applicable arbitration law and arbitration rules, arbitrators are generally expected to keep the arbitral proceedings, including any information related to or obtained during those proceedings, confidential.”) (emphasis added); LCIA Notes for Arbitrators, ¶ 6 (June 29, 2015) (“Parties to arbitrations are entitled to expect of the process a just, well-reasoned and enforceable award. To that end, they are entitled to expect arbitrators: . . . to maintain the confidentiality of the arbitration. . . .”) (emphasis added).

Moreover, in the adversarial and adjudicatory context, each actor in arbitration has legitimate expectations of privacy as to the data that defines or supports its role in the process. Irrespective of the extent to which the proceeding as a whole is entirely confidential or in some respects public, counsel and clients expect that they alone will have access to their communications and case strategy, for example, while arbitrators expect that no one else will have access to their deliberations or draft adjudicative documents and other work product. Those who intrude on these boundaries by hacking or other unauthorized access may break the law³⁸; at a minimum, they will threaten legitimate expectations as to privacy in any adjudicatory process and the integrity of the process as a whole. In sum, since cyberintrusion undermines or negates the legitimate expectations of confidentiality that exist in international commercial arbitration as well as the legitimate expectations of privacy that exist to some degree in all adjudicatory proceedings, it follows that the arbitrator's special duty to protect confidentiality extends to an obligation to avoid intrusion by non-participants who are determined to defeat those expectations.³⁹

B. Duty to Preserve and Protect the Integrity and Legitimacy of the Arbitral Process

The arbitrator's duty to avoid intrusion also rests on a duty to protect the integrity and legitimacy of the arbitral process. Unauthorized intrusion by hackers or other malevolent actors threatens more than confidentiality: it is a direct threat to the fair, neutral, and orderly process that underlies all arbitrations and to public trust in the arbitral process. If we accept that hacking threatens the integrity of the process, it follows that the arbitrator's obligation to protect the integrity of the process encompasses some form of duty to avoid such intrusion.

38. In the United States, for example, certain federal laws criminalize hacking and most states have computer crime laws that address unauthorized access. *See* Computer Fraud and Abuse Act, 18 U.S.C. § 1030; National Conference of State Legislatures, Computer Crime Statutes (Dec. 5, 2016), <http://www.ncsl.org/research/telecommunications-and-information-technology/computer-hacking-and-unauthorized-access-laws.aspx>.

39. *See* UNCITRAL Notes, *supra* note 26, at ¶ 58(b).

Our premise that the arbitrator has a duty to avoid intrusion does not require resolution of the ongoing debate as to whether a commercial arbitrator is a mere independent service provider to the parties or if the arbitrator has a broader, adjudicative role with responsibilities also to society and the rule of law.⁴⁰ Recognizing the deference to party autonomy that characterizes international commercial arbitration, it is well-established that arbitrators also have important and independent responsibilities to maintain their own reputations and probity, to support the interests of society and to uphold the legitimacy and integrity of the arbitral process.⁴¹ Even the most articulate and well-respected proponents of the arbitrator as service provider model recognize that there are limits to party autonomy and to arbitrators' fidelity to the parties' instructions.⁴²

There is little doubt that the use in an arbitration of data illegally obtained by or on behalf of a party would irreparably taint

40. See ROGERS, *supra* note 2; Lon L. Fuller, *The Forms and Limits of Adjudication*, 92 HARV. L. REV. 353, 392 (1978) (common features of the power to adjudicate delegated by the state to judges and by consent of the parties to arbitrators); Panel Discussion, *Arbitrator Ethics Through the Lens of Arbitrator Role: Are Arbitrators Adjudicators or Service Providers?*, 10 WORLD ARB. & MED. REV. 3, 309 (2016); Margaret Moses, *The Role of the Arbitrator: Adjudicator or Service Provider?*, 10 WORLD ARB. & MED. REV. 3, 367 (2016)

41. See e.g., Julie Bédard, Timothy Nelson and Amanda Kalantirsky, *Arbitrating in Good Faith and Protecting the Integrity of the Arbitral Process*, 3 PARIS J. INT'L ARB. 737, 749 (2010); ABA/AAA CODE OF ETHICS FOR ARBITRATORS IN COM. DISPUTES, Canon 1 ("An arbitrator should uphold the integrity and fairness of the arbitration process An arbitrator has a responsibility not only to the parties but also to the process of arbitration itself, and must observe high standards of conduct so that the integrity and fairness of the process will be preserved."); ICC RULES, *supra* note 10, at art. 5 ("[T]he emergency arbitrator shall act fairly and impartially and ensure that each party has a reasonable opportunity to present its case"); JAMS FOUNDATION, JAMS ARBITRATOR ETHICS GUIDELINES, 1 ("[A]n arbitrator should uphold the dignity and the integrity of the office of the arbitration process"); CIARB ETHICS CODE, *supra* note 30, at Part 2, Rule 2 ("A member shall maintain the integrity and fairness of the dispute resolution process.").

42. See Luca G. Radicati di Brozolo, *Party Autonomy and the Rules Governing the Merits of the Dispute in Commercial Arbitration*, in LIMITS TO PARTY AUTONOMY IN INTERNATIONAL COMMERCIAL ARBITRATION, 339 (Juris, 2016); see also Teresa Cheng, *panelist, The Theory and Reality of the Arbitrator: What is an International Arbitrator?* 7 WORLD ARB. & MED. REV. 4, 639 (2013) (commenting at the 25th Annual Workshop of the Institute for Transnational Arbitration that although arbitrators are independent service providers, there is also a duty to oneself as well as a duty to the arbitral process); ROGERS, *supra* note 2; ILA REPORT, *infra* note 47, at 17; Park, *Arbitrators and Accuracy*, *supra* note 1, at n.59 (stating faithfulness to the agreement would not justify violation of international public policy.)

proceedings.⁴³ Different issues arise when external actors compromise the data security of arbitration-related information. Here, the participants are victims of the intrusion and the matter presumably may proceed, with such corrective or ongoing protective steps as the tribunal may deem appropriate.⁴⁴ Nonetheless, such an incident, particularly if it follows from a failure to adequately secure data, inevitably will erode the confidence and trust of participants, and potentially the public, in the international private commercial arbitration process.⁴⁵ The arbitrator, along with the parties, counsel, and other actors in the process, is in a position to take reasonable protective measures to avoid that risk.

While much attention has been focused on the implied *powers* of arbitrators to fill in gaps in institutional rules or the parties' agreement where necessary to protect due process and the legitimacy of the process, less attention has been paid to the scope of the arbitrator's *duties*.⁴⁶ The ILCA Arbitration Committee's *Final Report*

43. ILCA REPORT, *infra* note 47, at 18; Bernard Hanotiau, *Misdeeds, Wrongful Conduct and Illegality in Arbitral Proceedings*, in INTERNATIONAL COMMERCIAL ARBITRATION: IMPORTANT CONTEMPORARY QUESTIONS, 285 (Kluwer Law International, 2003); REDFERN AND HUNTER ON INTERNATIONAL ARBITRATION ¶ 5.76 (5th ed., 2009).

44. See *Caratube*, *supra* note 18 (considering the admissibility of illegally obtained evidence, accepting some and excluding some).

45. See Jan Paulsson, *Metaphors, Maxims and Other Mischief, The Freshfields Arbitration Lecture 2013*, 30 ARB. INT'L 4, 630 (2014) ("[P]ublic confidence is perforce at stake in the arbitral context as well [as in the judicial process], because arbitration cannot thrive without the support of the general legal system."); Charles Brower, *Keynote Address: The Ethics of Arbitration: Perspectives from a Practicing International Arbitrator*, 5 BERKELEY J. OF INT'L L. PUBLICIST, 1 (2010) ("[A]rbitrators and arbitral institutions also have an interest in maintaining legitimacy, both for the mutual acceptance of their awards by the parties before them and for broad public acceptance of the entire law-based system of which they are a part.").

46. Two widely cited cases involving the appearance of new counsel after an ICSID tribunal was constituted focused on the arbitrator's role in preserving the integrity of the arbitration proceedings. Although the tribunals reached differing results on applications to disqualify counsel and had differing views on the nature and extent of an arbitrator's inherent powers, both stated that the arbitrators had some inherent power, and presumably some obligation, to protect the essential integrity of the proceeding. See *Hrvatska Elektroprivreda d.d. v. Republic of Slovenia*, ICSID Case No. ARB/05/24, 15, (2008) (Tribunal's Ruling Regarding the Participation of David Mildon QC in further Stages of the Proceeding); *Rompotrol Group NV v. Romania*, ICSID Case No. ARB/06/03, 5-6 (2008) (Decision of the Tribunal on the Participation of a Counsel); see also Bédard, et al., *supra* note 41 at n.69. Similarly, in *Caratube*, although the tribunal found that the claimants failed to prove the respondent had engaged in any threatening or intimidating action that could cause an irreparable harm to the claimants' rights in the arbitration, including a right to the "integrity and the legitimacy of the arbitration," the tribunal implicitly recognized its authority to take

on The Inherent Powers of Arbitrator in International Commercial Arbitration noted that the implied powers necessary to protect the core functions of arbitration amount to affirmative arbitral duties:

It is in such situations that a third and final category of non-enumerated powers becomes relevant, encompassing that authority which can be said to be truly inherent, namely those powers necessary to safeguard a tribunal's jurisdiction and the integrity of its proceedings. Stated differently, these powers are those required to decide a legal dispute fairly and in a manner consistent with at least the minimal requisites of due process and public policy. They trace their roots most clearly to the original notion of inherent powers as protecting jurisdiction and curtailing procedural abuses, and their exercise may justify overriding party preferences. . . . Such powers are so core to the function of arbitration that they might be more properly termed arbitral duties, the fulfillment of which is a necessary function of serving as a competent arbitrator.⁴⁷

We conclude, then, that the arbitrator's duty to uphold the legitimacy and integrity of the arbitral process, and to ensure confidence and trust in arbitration, further supports the premise that the arbitrator has a duty to avoid intrusion.

C. Duty of Competence

It is commonly accepted that an arbitrator has a duty of competence.⁴⁸ Various arbitrator ethics codes expressly require arbitrators to be "competent." Canon 1 of the *ABA/AAA Code of Ethics for Arbitrators in Commercial Disputes*, which requires an arbitrator to uphold the integrity and fairness of the arbitration process, provides that an arbitrator should accept appointment in a

measures to preserve the integrity of the arbitration insofar as it stressed the "[p]arties' general duty, arising from the principle of good faith, not to take any action that may aggravate the present dispute, affect the integrity of the arbitration and the equality of the Parties"

Caratube supra note 18, at ¶¶ 111, 154.

47. INTERNATIONAL LAW ASSOCIATION, REPORT FOR THE BIENNIAL CONFERENCE IN WASHINGTON, D.C., April 2014 (final report 2016) [hereinafter ILA REPORT], at 17, <http://www.ila-hq.org/download.cfm/docid/04ED7050-5C2A-4A56-92FCF1857A094C8B> (last visited Jan. 22, 2017).

48. See Henry Gabriel and Anjanette H. Raymond, *Ethics for Commercial Arbitrators: Basic Principles and Emerging Standards*, 5 WYO. L. REV. 453 (2005); ILA REPORT, *supra* note 47 (stating the duty to protect integrity of the proceeding is core to necessary function of serving as a competent arbitrator).

particular matter only if fully satisfied that he or she is “competent to serve.” The *IBA Rules of Ethics for International Arbitrators* provide a more general requirement that “international arbitrators should be . . . competent” in addition to a specific requirement that the arbitrator be competent to determine the issues in dispute in a particular matter.⁴⁹

While the arbitrator ethics codes do not define competence, important context and definition of the meaning of the term may be drawn from the evolution of lawyer ethics codes in recent years. Recognizing the need to provide some definition of competence and to update ethical codes to reflect the rise of globalization and technology, governing bar associations and disciplinary authorities have amended lawyer ethical codes to provide explicit linkage between general competence requirements and the need to keep abreast of technology.⁵⁰ For example, the American Bar Association (“ABA”) *Model Rules of Professional Conduct*, first introduced by the ABA in 1983, and adopted over time in various forms by most states in the United States,⁵¹ provide the following lawyer competence requirement:

Rule 1.1 Competence

A lawyer shall provide competent representation to a client.
Competent representation requires the legal knowledge,

49. See Introductory Note and Rule 2.2; see also CIARB ETHICS CODE, *supra* note 30, at Part 2, Rule 4 “Competence” (“A member shall accept an appointment or act only if appropriately qualified or experienced.”).

50. Lawyer ethics rules obviously do not bind non-lawyer arbitrators. Indeed, some of the rules are limited to the context of client representation and thus do not expressly apply even to lawyers who, when serving as arbitrators, are not representing clients. For example, ABA Model Rule 1.1, standing alone in the form quoted in the accompanying text, does not apply directly to arbitrators, even if they are lawyers practicing in a jurisdiction where this version of the Model Rules applies. In France, the Règlement Intérieur National, the French code of ethics for lawyers, contains a general competency requirement in respect to client work in Article 1.3 (“L’avocat . . . fait preuve, à l’égard de ses clients, de compétence . . .”), <http://codeonto.avocatparis.org/acces-article>; see also UK SOLICITORS REGULATORY AUTHORITY, SRA CODE OF CONDUCT 2011 (Version 18, 2016) [hereinafter UK SRA CODE OF CONDUCT] at 0-1.5 (“[t]he service you provide to clients is competent . . .”), <http://www.sra.org.uk/solicitors/handbook/code/content.page>.

51. A notable exception is California, which maintains its own Rules of Professional Conduct. California Rule 3-110 (A) provides a general competence requirement (“A member shall not intentionally, recklessly, or repeatedly fail to perform legal services with competence.”).

skill, thoroughness and preparation reasonably necessary for the representation.

Notably, ABA Model Rule 1.1 is limited by its terms to the lawyer serving in a representational function. However, the Preamble to the Model Rules notes that a lawyer may serve in other roles, including “as a third party neutral, a non-representational role helping the parties to resolve a dispute or other matter,” and goes on to state that, “[i]n all professional functions a lawyer should be competent, prompt and diligent.”⁵²

New York State did not adopt the Model Rules until 2009 and did not adopt the Preamble quoted above. However, Model Rule 1.1 as adopted in New York added a more general competency requirement, in addition to the client-oriented rule: “A lawyer shall not handle a legal matter that the lawyer knows or should know that the lawyer is not competent to handle”⁵³ Thus, at least as to lawyers working as arbitrators in jurisdictions that have adopted the ABA Preamble or who have adopted a rule similar to Rule 1.1(b) as in effect in New York State, there is a direct ethical obligation of competence.⁵⁴ From 2009 to 2013, the ABA Commission

52. AM. BAR. ASSOC., PREAMBLE: A LAWYER’S RESPONSIBILITIES, ¶4. By referring to “professional functions,” the Preamble is broad enough to avoid the debate over whether participants are engaged in the practice of law. *See* Birbrower, Montalbano, Condon & Frank, P.C. v. Superior Court, 17 Cal.4th 119 (Cal. 1998), *cert den.*, 525 U.S. 920 (1998); Schiff Hardin LLP, *Arbitration and the Unauthorized Practice of Law*, 13 ARIAS QUARTERLY U.S. 1, 16-19 (2006), <http://www.schiffhardin.com/Templates/Media/files/archive/binary/spector-arbitration.pdf>.

53. NY Judiciary Law (Appendix: Code of Prof. Resp. §1200, Rule 1.1 (b)); The New York State Bar Association Committee on Standards of Professional Conduct (“COSAC”) 2007 Report recommending the adoption of the Model Rules noted that the new rules were beneficial in describing competent representation as requiring the “legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation,” in contrast to the previous Lawyer’s Code of Professional Responsibility that “did not define or describe competent representation.” New York State Bar Association Proposed Rules of Professional Conduct 11 (2007), *available at* <http://www.nysba.org/workarea/DownloadAsset.aspx?id=26635>; New York City Bar Association Professional Responsibility Committee Report on COSAC Proposals Rules 1.1-1.4, 3.1, 3.2, 3.5-3.9, and 8.1-8.4 (2006) *available at* http://www.nycbar.org/pdf/report/Prof_Resp_COSAC_506.pdf (proposed Rule 1.1 “helpfully fleshes out the definition of ‘competent representation’”). Notably also, in adopting Model Rule 1.1 (b), New York State intended to preserve the concept in prior Disciplinary Rule 6-101 (competent representation) and its accompanying Ethical Consideration 6-2 that a lawyer should attain and maintain competence by keeping abreast of current legal literature and developments. *Id.*

54. Also useful by analogy is *The Code of Conduct for Lawyers in the EU*, issued by the Council of Bars and Law Societies of the European Union, which bridges the gap from the

on Ethics 20/20 recommended proposed amendments to the Model Rules to account for, among other things, rapid changes in technology affecting the practice of law. In 2012, the ABA House of Delegates adopted a revised Comment 8 to Model Rule 1.1, to provide in respect to competency, that “to maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, including the benefits and risks associated with technology.” In amending Comment 8, the ABA took the position that the revised language did not impose any new obligations on lawyers, but, rather, simply reminded lawyers that in the current environment, an awareness of technology, including the benefits and risks associated with it, is part of the lawyer’s general ethical duty to remain competent.⁵⁵ The same may be said in respect to an arbitrator’s competence obligation.

In its 2014 report recommending that New York adopt the revised comment 8 to Model Rule 1.1, the New York State Bar Association Committee on Standards of Professional Conduct noted that:

... to keep abreast of changes in law practice, a lawyer needs to understand the risks and benefits of technology relevant to the lawyer’s particular practice. For example, if a lawyer’s clients are communicating with the lawyer by web-based document-sharing technology or by social media, the lawyer should have some understanding of how to ensure that confidential communications remain confidential. The proposed amendment impresses upon lawyers the key role that technology plays in law practice and creates the expectation that lawyers will keep abreast of the

regulation of lawyers working in a representational capacity in the judicial system to those working in arbitration by providing that “[t]he rules governing a lawyer’s relations with the courts apply also to his relations with arbitrators.” CCBE, CODE OF CONDUCT FOR LAWYERS IN THE EUROPEAN UNION (2002) at art. 4.5, available at http://www.idhae.org/pdf/code2002_en.pdf.

55. See Karin Jenson, Coleman Watson, & James Sherer, *Ethics, Technology, and Attorney Competence*, available at <http://www.law.georgetown.edu/cle/materials/eDiscovery/2014/frimordocs/EthicsIneDiscoveryBakerHostetler.pdf> (last visited Jan. 14, 2017); see also The State Bar Of California Standing Committee on Professional Responsibility and Conduct, Formal Opinion Interim No. 11-0004 (2014) (“An attorney’s obligations under the ethical duty of competence evolve as new technologies develop and become integrated with the practice of law.”); INT’L BAR ASSOC., IBA INTERNATIONAL PRINCIPLES ON CONDUCT FOR THE LEGAL PROFESSION (2011), http://www.ibanet.org/barassociations/BIC_resources.aspx (“Competence . . . includes competent and effective client, file and practice-management strategies.”).

benefits and risks associated with the technology relevant to their own legal practice.⁵⁶

Whether or not adopted in the form encompassing the more general obligation provided in the New York version of the rules, the Model Rules, and particularly Comment 8 to Model Rule 1.1 as it now reads, are relevant to inform and define the meaning of competence as applied to arbitrators, as well as in their direct regulation of lawyer conduct.⁵⁷

Achieving digital literacy, including an understanding of the measures reasonably necessary to avoid cyberintrusion in an arbitration, is also closely related to the attention institutions, users, and counsel have paid in recent years to the role of the arbitrator in

56. Report of The New York State Bar Association Committee On Standards Of Attorney Conduct (“COSAC”) Proposed Amendments to the New York Rules of Professional Conduct and Related Comments 10 (2014), <http://www.nysba.org/WorkArea/DownloadAsset.aspx?id=54063>.

57. See, e.g., In re: Amendments to Rules Regulating the Florida Bar 4-1.1 and 6-10.3, No. SC16-574 (Sept. 29, 2016), at <http://www.floridasupremecourt.org/decisions/2016/sc16-574.pdf> (amending the comment to rule on competence to address technology); Law Society of Upper Canada, Technology Practice Management Guideline, Guideline 5.5 (“Competent Use of Information Technologies. Lawyers should have a reasonable understanding of the technologies used in their practice or should have access to someone who has such understanding”) & 5.10 (“Security Measures. Lawyers should be familiar with the security risks inherent in any of the information technologies used in their practices including unauthorized copying of electronic data, computer viruses which may destroy electronic information and hardware, hackers gaining access to lawyers’ electronic files, power failures and electronic storms resulting in damage to hardware or electronic information, theft of vast amounts of electronic information stored in stolen hardware. Lawyers should adopt adequate measures to protect against security threats and, if necessary, to replace hardware and reconstruct electronic information.”), available at <http://www.lsuc.on.ca/with.aspx?id=2147491197> (last visited Jan. 22, 2017); Canadian Bar Association, *Legal Ethics in a Digital World* (Sept. 2, 2015), <https://www.cba.org/getattachment/Sections/Ethics-and-Professional-Responsibility-Committee/Resources/Resources/2015/Legal-Ethics-in-a-Digital-World/guidelines-eng.pdf>; Philippe Doyle Gray, *The Pillars of Digital Security*, BAR NEWS: J. OF THE NEW SOUTH WALES BAR ASSOCIATION (Summer 2014), <http://www.philippedoylegray.com/content/view/56/45/> (although the Law Society of New South Wales has not adopted professional conduct rules addressing technology, it has published guidelines for lawyers about the use of technology such as cloud computing and social media); E-Law Committee of the Law Society of South Africa, LSSA Guidelines on the Use of Internet-Based Technologies in Legal Practice (2014), www.lssa.org/za/index.php?; see also UK SRA CODE OF CONDUCT, *supra* note 50, at O-4.5 (“You have effective systems and controls in place to enable you to identify risks to client confidentiality”); O-7.5 (“You comply with . . . data protection legislation.”); IB-7.5 (“Identifying and monitoring . . . IT failures and abuses.”).

case management.⁵⁸ In the highly digitized and interdependent world of international arbitration, management of technology and baseline data security competence manifestly have become critical components of an arbitrator's competence to organize and conduct arbitration proceedings.⁵⁹

D. Global Data Protection Laws and Regulations

In any given arbitration matter, data held by an arbitrator may be subject to specific cybersecurity obligations arising from international or national data protection laws and regulations that govern how certain information can be collected, stored, and transferred.⁶⁰ While there is no universal international approach to data protection, nearly 110 countries⁶¹ have enacted laws aimed at protecting personal information by regulating categories of data or industry sectors, such as the financial and health care industries.⁶² As the key players in

58. See, e.g., ICC RULES, *supra* note 10, at app. IV (case management techniques); LCIA RULES, *supra* note 1, at art. 14 (conduct of the proceedings); ICDR RULES, *supra* note 10, at art. 20.2 (conduct of the proceedings) (“In establishing procedures for the case, the tribunal and the parties may consider how technology, including electronic communications, could be used to increase the efficiency and economy of the proceedings.”); College of Commercial Arbitrators, *Protocols for Expedient, Cost-Effective Commercial Arbitration* (2010) 69 (arbitrators should take control of the arbitration and actively manage it from start to finish); ICC Commission Report, *Controlling Time and Costs in Arbitration* (2d. ed. 2012); Christopher Newmark, *Controlling Time and Costs in Arbitration*, in *LEADING ARBITRATORS’ GUIDE TO INTERNATIONAL ARBITRATION* *supra* note 1.

59. The UNCITRAL Notes on Organizing Arbitral Proceedings (2016) urge that arbitrators consider issues relating to the means of communication to be used during the proceedings at the outset, noting that the parties and the tribunal “may need to consider issues of compatibility, storage, access, data security as well as related costs when selecting electronic means of communication.” UNCITRAL Notes, *supra* note 26, at ¶¶ 56, 58.

60. See UNCTAD, *Data Protection Regulations and International Data Flows: Implications for Trade and Development*, UNCTAD/WEB/DTL/STICT/2016/1/iPub, http://unctad.org/en/PublicationsLibrary/dtlstict2016d1_en.pdf (last visited Jan. 9, 2017) (overview of international and national laws and regulations) (“UNCTAD on Data Protection”); see also European Union Data Protection Directive (95/46/EC) (implemented in each of the twenty-eight EU Member States through national data protection law).

61. See UNCTAD on Data Protection at 42 (108 countries have either comprehensive data protection laws or partial data protection laws).

62. In the United States, for example, there is no omnibus privacy or data protection legislation, but a patchwork of federal privacy laws that generally regulate security breach notification statutes by sector and state. See, e.g., Health Insurance Portability and Accountability Act, 42 U.S.C. § 1301 *passim* [hereinafter HIPPA] (health information); Federal Trade Commission Act, 15 U.S.C. §§ 41-58 (consumer protection); Gramm-Leach-

international arbitrations frequently reside in different countries, resulting in continuous cross-border exchanges of information, it follows that the same data may be subject to multiple, and potentially inconsistent, laws. For example, the legal concept of “personal information” or “personally identifiable information” subject to reasonable protection from unauthorized access is defined more broadly under EU law than it is under US law.⁶³

While it is beyond the scope of this article to address the complex conflict-of-law issues that may arise in these situations,⁶⁴ the global proliferation of data protection laws indicates that: (i) participants in international arbitrations who share the sensitive information of others may have legal obligations to ensure that arbitrators, acting in the capacity of service providers, safeguard that information by complying with certain security standards⁶⁵; and (ii) increasingly, both participants and non-participants in an arbitration may have legally enforceable interests (or rights)⁶⁶ in the way that arbitrators secure and handle e-mail correspondence, witness statements,⁶⁷ and other electronically-exchanged documents that routinely disclose personally identifiable information. Moreover,

Bliley Act, 15 U.S.C. §§ 6801-6827 (financial information); National Conference of State Legislators, Security Breach Notification Laws (Jan. 4, 2016), <http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx> (forty-seven states have enacted legislation entitling individuals to notice of breaches of information of personally identifiable information).

63. See Practical Law, Expert Q&A on Data Security in Arbitration (Dec. 1, 2016) (stemming from the concept in EU countries that privacy is a fundamental human right, a person’s name and place of employment can be considered protected information).

64. Although not the focus of this article, we note that the potential for the application of disparate data protection laws strongly favors early discussions between opposing counsel about how arbitration-related data will be handled as well as discussion of data security with the tribunal by at least the first case management conference.

65. For example, an individual or organization that must comply with health information privacy rules under HIPAA is required to have any “business associate” it engages to help carry out its functions agree to comply with those rules as well. HIPAA, *supra* note 62. See also EU Directive 2016/1148 (July 6, 2016).

66. See, e.g., Charter of Fundamental Rights of the European Union (2012/C 326/02), art. 7 (“Everyone has the right to respect for his or her private and family life, home and communications”) & 8(1) (“Everyone has the right to the protection of personal data concerning him or her.”).

67. See INT’L BAR ASSOC., IBA RULES ON THE TAKING OF EVIDENCE IN INTERNATIONAL ARBITRATION (2010), art. 4(5) (specifying personal information to be included in fact witness statements).

when security incidents occur, a web of breach notification obligations may be triggered.⁶⁸

Although it is not evident that the obligations or legal interests that may arise under the current global data protection regime create a bright-line duty, independent of any specific case, for arbitrators to avoid cyberintrusion, their prevalence at least supports the notion that to maintain user confidence in international arbitration process, arbitrators must not only be prepared and competent to handle sensitive information securely, but also appear to the public to be so prepared. Global data protection laws thus behoove arbitrators to be proactive (and not merely reactive, on a case-by-case basis) in dealing with cybersecurity.

IV. NATURE AND SCOPE OF THE ARBITRATOR'S DUTY TO AVOID INTRUSION

This article posits that the arbitrator's duty in relation to cybersecurity is one of avoiding intrusion, which we define as the duty to take reasonable measures to prevent unauthorized digital access to arbitration-related information. In the following sections, we first explore the nature and scope of the duty and then discuss some practical measures that will assist the arbitrator in fulfilling the duty.

A. An Umbrella Obligation

As we have shown above, the arbitrator's duty in relation to cybersecurity is not a new, independent obligation, but rather a natural extension in the digital age of an arbitrator's existing duties to keep arbitration-related information confidential, to preserve and protect the integrity and legitimacy of the arbitral process, and to be competent. By grouping the implied cybersecurity responsibilities arising under each of these duties under the new umbrella of the "duty to avoid intrusion," we recognize the unique challenges that cyberthreats pose to the practice of international arbitration in the digital age.

This is a matter of substance, not just terminology. Recognition of the threat and each actor's acceptance of responsibility to take part in addressing it are key building blocks to effective cybersecurity in

68. Practical Law, *supra* note 63.

the international commercial arbitration regime. In this article, which focuses on the arbitrator's role, we emphasize that the fulfillment of existing arbitrator duties in the digital age encompasses a duty to be proactive and vigilant in guarding against cyberintrusion.

B. An Interdependent Landscape with Independent Duties

Since the data arbitrators are entrusted to keep confidential generally originates in the arbitration from the parties and their counsel, it may be tempting for arbitrators to view cybersecurity as an issue for the parties, and particularly counsel, to address on a case-by-case basis. Parties and their counsel indisputably do have legal and ethical responsibilities to safeguard the data that they import into an arbitration.⁶⁹ In many instances, they will be uniquely positioned to secure that data and to advise the arbitrator regarding specific security precautions necessary in the case or required by law. Any view that purports to isolate any one particular participant in the arbitration process as having sole responsibility for cybersecurity, however, or to relieve the arbitrator from any responsibility for cybersecurity outside of the bounds of individual cases, ignores the interdependent digital landscape discussed above and is shortsighted. Since any break in the custody of sensitive data may affect all participants in the arbitral process, cybersecurity is an inherently shared responsibility.

While interdependent with other actors, the arbitrator's cybersecurity duty also stands alone. The arbitrator who takes the view that others are primarily responsible abjures the arbitrator's special role as adjudicator as well as the arbitrator's underlying duties to safeguard the integrity and legitimacy of the process and the confidentiality of arbitration-related information. The obligations of other players in the arbitral process (including the parties, counsel, arbitral institutions and third party service providers among others) may be governed by differing standards and other legal regimes, only some of which overlap with those governing arbitrators.

Moreover, the arbitrator's day-to-day data security architecture and practices pre-exist individual matters and persist after the matter is concluded. Thus, the strength of the arbitrator's routine cybersecurity practices will impact the overall security of arbitration-

69. See *supra* Section III.D (discussing national data protection laws and regulations); Section III.C (discussing cybersecurity obligations arising from attorney ethical codes).

related data from the first moment the arbitrator becomes involved with a case, before counsel or the parties have an opportunity to address security protocols that may be appropriate for the specific data involved in the matter, and will continue after the matter ends as the arbitrator maintains at least some data for conflicts or other record-keeping purposes.

C. Personal Accountability

As arbitrators are appointed for their personal qualifications and reputational standing,⁷⁰ it is broadly accepted in international arbitration that the arbitrator's mandate is personal and cannot be delegated.⁷¹ While this notion is raised most often in discussions about impermissible delegation of decision-making responsibilities to arbitral secretaries, the personal nature of the arbitrator's mandate has implications for cybersecurity as well. In particular, it is important for arbitrators to recognize that even if the security of their digital infrastructure is established and monitored by IT personnel, or they work in a large law firm setting where they have little to no influence over firm-wide security policies, they cannot assume that their responsibilities in relation to cybersecurity have been met.

First, effective security depends on individual choices and conduct.⁷² Hackers' most valuable currency is human carelessness.⁷³

70. BORN, *supra* note 27, at 2013. ("Arbitrators are almost always selected because of their personal standing and reputation . . .").

71. See Eric Schwartz, *The Rights and Duties of ICC Arbitrators*, in *ICC International Court of Arbitration Bulletin, Special Supplement, The Status of the Arbitrator (1995)* at 86; see also BORN, *supra* note 27, at 1999. ("An arbitrator's obligations include the duty not to delegate his or her responsibilities or tasks to third parties. . . . Most fundamentally, an arbitrator cannot delegate the duty of deciding a case, attending hearings or deliberations, or evaluating the parties' submissions and evidence to others: these are the essence of the arbitrator's adjudicative function and they are personal, non-delegable duties.")

72. To highlight the fundamental role played by individuals in protecting confidential information, whether reliance is placed on notepads, mobile telephones, or the cloud, Philippe Doyle Gray shares this anecdote:

I regularly walk from the Supreme Court of New South Wales down King Street to stop at the intersection with Elizabeth Street. So too do other lawyers. When it's raining we huddle under the awning of the Sydney University Law School, but in fine weather we gather around the traffic lights waiting for the signal that it's safe for pedestrians to cross. Usually, I see paper files or lever-arch folders neatly stating the names of the clients concerned, and sometimes the nature of their confidential affairs. Often, I can't help but overhear a colleague talking about his matter. A few

Even if an arbitrator operates in an environment with the digital architecture of Fort Knox, important security actions will always remain in the arbitrator's personal control. Law firm or IT policy may dictate to an arbitrator, for example, that strong, complex passwords be used on all laptops and other devices and that passwords be changed regularly. However, an arbitrator risks completely undermining that security protocol by conveniently storing a reminder of the password du jour on a post-it note stuck to the cover of a laptop,⁷⁴ and then working away on the laptop in an airport lounge or other public environment, or, worse, forgetting the laptop in the security line or the airplane seat pocket after a long international flight.⁷⁵ Similarly, although IT policy may dictate that no USB drive can be used in a networked computer before it is manually scanned for viruses by the IT department, an arbitrator sitting in a hearing in Vienna may decide before the flight home to take the USB drive handed out at a recent arbitration conference and use it to transfer

times, sensitive material was inadvertently broadcast to passers-by that happened to include me. Once, I even overheard a colleague—speaking on his mobile phone—discuss settlement negotiations during a mediation that had adjourned over lunch: he openly discussed not only the parties' respective offers, but his own client's bottom line. The real security problems lie not in CLOUD COMPUTING, but in ourselves.

Gray, *supra* note 57. See also *Harleysville Ins. Co. v. Holding Funeral Home*, Case No. 1:15cv00057 (W.D. Va., Feb. 9, 2017), <http://bit.ly/2mSkyuu> (court held that insurer's attorney-client privilege was waived where entire claims file was loaded onto a cloud service and made accessible to anyone via hyperlink without password protection, stating this was the "cyber world equivalent of leaving its claims file on a bench in the public square").

73. In December 2015, The Wall Street Journal reported that "[w]eeks after J.P. Morgan Chase & Co. was hit with a massive data breach that exposed information from 76 million households, the country's biggest bank by assets sent a fake phishing email as a test to its more than 250,000 employees. Roughly 20% of them clicked on it, according to people familiar with the email." Robin Sidel, *Banks Battle Staffers' Vulnerability to Hacks*, WALL ST. J., (Dec. 21, 2015), <https://www.wsj.com/articles/the-weakest-link-in-banks-fight-against-hackers-1450607401>. See Int'l Chamber of Commerce [ICC], *Cyber Security Guide for Business*, at 8, ICC Doc. 450/1081-5 (2015) ("35% of security incidents are a result of human error rather than deliberate attacks. More than half of the remaining security incidents were the result of a deliberate attack that could have been avoided if people had handled information in a more secure manner.").

74. According to Verizon's 2016 Data Breach Investigations Report, "63% of confirmed data breaches involved weak, default or stolen passwords." Verizon Report, *supra* note 13, at 20. See also Fox-Brewster, *supra* note 7 (Sony hack revealed chief executive's password was "guessable to any semi-skilled hacker" and that passwords to internal accounts were stored in a file marked "passwords").

75. Laptops and other devices are reportedly lost over 100 times more frequently than they are stolen. Verizon Report, *supra* note 13, at 44.

notes from deliberations stored on her laptop to a public computer in the hotel business center for printing.

Second, there is danger in complacency. Arbitrators understandably want to spend time on the practice of arbitration, not on routine practice management. However, an arbitrator who dismisses cybersecurity as an “IT issue” and who assumes that “others are taking care of it” fails to appreciate how a failure to heed cybersecurity may undermine his or her ability to keep arbitration-related information confidential as well as user trust and confidence in the integrity of the international arbitration regime. Notwithstanding the steady flow of news reports about cyberbreaches, it appears that “many [attorneys and law firms] are not using security measures that are viewed as basic by security professionals and are used more frequently in other businesses and professions.”⁷⁶ Arbitrators who rely on IT personnel to support their practice should thus bear in mind that their existing data security framework and digital architecture may well require an upgrade or adaptation to the unique aspects of international arbitration. Indeed, just as an arbitrator should not entrust (but may be aided by) the conflicts department in his or her law firm to determine whether he or she is bound to make any disclosures in an arbitration,⁷⁷ an arbitrator may be assisted by, but should not entrust, an IT department to fulfill the duty to avoid intrusion.⁷⁸

76. David G. Ries, *Security*, ABA TECHREPORT 2016, 1-2, <http://www.americanbar.org/content/dam/aba/publications/techreport/2016/security/security.authcheckdam.pdf> (reporting on 2016 survey of attorneys and law firms about security incidents and safeguards). See also Matthew Goldstein, *Citigroup Report Chides Law Firms for Silence on Hackings*, N.Y. TIMES (Mar. 26, 2015), <https://nyti.ms/1NkjfKo> (In March 2015, Citigroup’s internal cyberintelligence team advised bank employees to be “mindful that digital security at many law firms, despite improvements, generally remains below the standards for other industries.”).

77. See, e.g., *Ometto v. ASA Bioenergy Holding A.G. et al.*, 12 Civ. 1328(JSR), 2013 WL 174259 (S.D.N.Y. Jan. 7, 2013).

78. The importance of “executive-level” attention to effective cyberrisk management is frequently emphasized by cybersecurity experts. See, e.g., ICC, *Cyber Security Guide for Business*, *supra* note 73, at 4 (2015); Tucker Bailey et al., *Why Senior Leaders Are the Front Line Against Cyberattacks*, MCKINSEY & CO. (June 2014), <http://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/why-senior-leaders-are-the-front-line-against-cyberattacks>.

D. Continuous and Evolving

The duty to avoid intrusion is a continuous obligation, which is not limited in time. In part, this follows from the nature of the arbitrator's duty of confidentiality. Since arbitrators may maintain digital information from their cases beyond the lifetime of an individual matter, ranging from case administration data (including as part of conflicts or billing systems), correspondence, procedural decisions, awards, and parties' evidentiary submissions, parties and other participants have a reasonable expectation that arbitrators will continue to safeguard the confidentiality of such information once a case ends.⁷⁹ Furthermore, as we have discussed above, because arbitrators accept appointments in new matters with a digital architecture and certain security practices already in place, parties and other participants have a reasonable expectation that arbitrators will heed cybersecurity from the time of appointment (and necessarily before).

The ongoing nature of the arbitrator's duty to avoid intrusion also flows from the underlying duty to be competent. Because cyberthreats are constantly evolving alongside advancing technology, an arbitrator cannot take effective steps to avoid intrusion unless he or she keeps abreast of the changing nature and scope of cyber risks. Otherwise, the arbitrator will not be in any position to analyze risks and weigh appropriate responses, including, for example, with respect to whether new or additional security measures may be warranted, what work-arounds might be acceptable when complying with an established security protocol proves to be impossible or impractical, or whether a new product or service is adequately secure.

E. Bounded by Reasonableness

Cybersecurity professionals routinely advise that in today's environment of ever-escalating data breaches, there is no longer any question of *if* one's digital infrastructure and data will be hacked, but

79. Int'l Law Ass'n, *Draft Report of the Committee on International Commercial Arbitration for the 2010 Hague Conference, Confidentiality in International Arbitration*, at 18 (2010), <http://www.ila-hq.org/en/committees/index.cfm/cid/19> (although there is uncertainty regarding the duration of duties of confidentiality in arbitration, the "fact that the duty of confidentiality usually covers the award seems to point to an expectation that the regime of confidentiality should outlive the arbitral proceedings and that the obligations will not cease after the end of the arbitration.").

only *when*.⁸⁰ As a practical reality, it follows that the arbitrator cannot guarantee that arbitration-related information will remain safe from hackers,⁸¹ but can only take steps to mitigate the risks of cyberintrusion. In *LabMD, Inc. v. Federal Trade Commission*, the U.S. Federal Trade Commission (“FTC”) explained why “reasonableness,” assessed “in light of the sensitivity and volume of consumer information [a company] holds, the size and complexity of its business, and the cost of available tools to improve security and reduce vulnerabilities,” is an appropriate touchstone for determining whether a company has implemented appropriate data security measures:

[The FTC] has made clear that it does not require perfect security; reasonable and appropriate security is a continuous process of assessing and addressing risks; there is no one-size-fits-all data security program; and the mere fact that a breach occurred does not mean that a company has violated the law.⁸²

Notably, reasonableness, not perfection, also bounds the lawyer’s confidentiality duty under the ABA Model Rules to protect information relating to the representation of a client from unauthorized access.⁸³

80. U.S. Attorney Preet Bharara recently made such a pronouncement in announcing criminal indictments of hackers who traded on confidential law firm information, saying, “This case of cyber meets securities fraud should serve as a wake-up call for law firms around the world: you are and will be targets of cyber hacking, because you have information valuable to would-be criminals.” Nate Raymond, *U.S. Accuses Chinese Citizens of Hacking Law Firms, Insider Trading*, REUTERS, (Dec. 28, 2016), <http://www.reuters.com/article/us-cyber-insidertrading-idUSKBN14G1D5>. See also, e.g., Verizon Report, *supra* note 13, at 3 (“No locale, industry or organization is bulletproof when it comes to the compromise of data.”); ICC, *Cyber Security Guide for Business*, *supra* note 73, at 10 (“Even the best protected enterprise will at some point experience an information security breach. We live in an environment where this is a question of when, not if.”).

81. ICC, *Cyber Security Guide for Business*, *supra* note 73, at 4 (2015) (“[A]ll business managers including executives and directors must recognize that cyber risk management is an on-going process where no absolute security is, or will be, available.”).

82. *LabMD, Inc.*, F.T.C. No. 9357, 2016 WL 4128215 (F.T.C. July 28, 2016). California’s Attorney General notes in her Breach Report 2016 that “reasonable security” is the general standard for information security adopted not only in California but also the major United States federal data security laws and regulations. See *infra*, note 111.

83. Model Rule 1.6(c) provides “[a] lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client.” MODEL RULES OF PROF’L CONDUCT, r. 1.6(c) (AM. BAR ASS’N, 1983). (emphasis added)

A risk-based approach, bounded by reasonableness, is similarly appropriate as we examine the scope and boundaries of the arbitrator's duty to avoid the ever-evolving threats of cyberintrusion in international commercial arbitration. It follows from the conclusion there is no one-size-fits-all data security program for consumer-facing corporations that there is no one-size fits-all data security program for international commercial arbitrators; any such program would risk obsolescence and fail to account for significant contextual differences. Furthermore, as Pastore argues, a de-contextualized approach to data security may be counterproductive "in that it over-designates [sensitive] information (desensitizing practitioners to the truly critical information) and results in overly cumbersome processes for information that, in reality, needs little to no additional protections."⁸⁴

In addition, a standard of reasonableness under the circumstances is familiar in the law, particularly in areas where the facts and circumstances vary widely and evolve over time. The reasonableness approach enables consideration of the trade-offs that will sometimes exist between increased security measures and other interests.⁸⁵ To the extent the arbitrator's duty to avoid intrusion is in tension with other important values such as conducting the proceedings expeditiously and cost-effectively and in accordance with the parties' preferences,⁸⁶ arbitrators should be entitled to weigh all of the relevant circumstances to determine the correct balance.⁸⁷ Arbitrators, institutions, users, and counsel should be able to understand and embrace such a standard for cybersecurity.

Accordingly, it is appropriate to limit the arbitrator's duty to an obligation to take such measures to protect digital security as he or she deems reasonable in light of the relevant facts and circumstances, including developments in technology and evolving security risks, the arbitrator's individual practice setting and digital architecture, the sensitivity of the data to be protected, and any party preferences or

84. Pastore, *supra* note 15.

85. *See generally* Pastore, *supra* note 15.

86. *See supra* note 10.

87. The UNCITRAL Notes on Organizing Arbitral Proceedings (2016) note that data security is but one factor to be considered when deciding whether to use electronic means of communication for proceedings. Other factors to be considered may include compatibility, storage, access and related costs. *See* UNCITRAL Notes, *supra* note 26.

other case-specific factors present in the matters over which the arbitrator presides.

V. IMPLEMENTING THE DUTY TO AVOID INTRUSION

In the absence of a detailed roadmap for data security, the challenge for international arbitrators is to determine what specific measures they should implement to avoid intrusion, in their own infrastructure and in arbitrations over which they preside, given that what constitutes “reasonable” measures will vary based on a risk assessment of the arbitrator’s individual digital architecture and data assets, the prevalent data security threats, available protective measures and, in relation to individual matters, case-specific factors.⁸⁸ Although it is by no means comprehensive, in this Part, we aim to highlight certain practical measures and general principles that are likely to be relevant for all international arbitrators, regardless of practice setting and individual risk profile.⁸⁹ In doing so, we further aim to show that the fundamentals of effective cyberrisk management need not be overwhelming or unduly burdensome. In addition, since cyberintrusion in the arbitral process can potentially arise from both intentional, targeted attacks on arbitral participants⁹⁰ and from the

88. Security framework standards are generally directed at organizations rather than business professionals. *See generally* NAT’L INST. OF STANDARDS AND TECH., SPECIAL PUBLICATION 800-53 REVISION 4, SECURITY AND PRIVACY CONTROLS FOR FEDERAL INFORMATION SYSTEMS AND ORGANIZATIONS (2013); FRAMEWORK FOR IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY (2014), *available at* www.nist.gov; INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, ISO/IEC 27002:2013 *Information Technology, Security Techniques, Code of Practice for Information Security Controls*, *available at* www.iso.org (last visited Jan. 22, 2017); Center for Internet Security, *Critical Security Controls for Effective Cyber Defense*, Version 6 (Oct. 15, 2015), www.cisecurity.org/.

89. A recent working paper from the Washington Legal Foundation suggests eight data security best practices based on an analysis of FTC enforcement actions:

- Limit the collection, retention, and use of sensitive data;
- Restrict access to sensitive data;
- Implement robust authentication procedures;
- Store and transmit sensitive information securely;
- Implement procedures to identify and address vulnerabilities;
- Develop and test new products and services with privacy and security in mind;
- Require service providers to implement appropriate security measures;
- Properly secure documents, media, and devices.

Kurt Wimmer, Ashden Fein, Catlin M. Meade & Andrew Vaden, *Data Security Best Practices Derived From Ftc § 5 Enforcement Actions*, at 6 (Washington Legal Foundation Paper No. 199, 2017).

90. *See supra* notes 13-14.

inadvertent⁹¹ disclosure or compromise of arbitration-related information (e.g., by way of a weak password, lost mobile device, or other human error),⁹² we discuss below potential responses to external threats and safeguards to prevent or mitigate damage if data security is compromised.

A. Keeping Abreast of Developments in Relevant Technology and Understanding Associated Benefits and Risks

There are readily accessible resources for arbitrators to educate themselves as to the evolving nature and scope of major data security threats, with a view to understanding the significance and effectiveness of specific security protocols, such as standards for passwords. These resources have been developed by bar associations, law firms, and others.⁹³ For example, the ABA has taken the lead internationally in developing guidance for legal practitioners in responding to the challenges of the digital world and regularly posts short, digestible articles online on topics such as ransomware and encryption, in addition to offering educational webinars and seminars.⁹⁴ Such resources frequently highlight ethical opinions from state bar associations on the responsible use of technology in the legal

91. Even a single misdirected e-mail—within an arbitration proceeding—can have serious consequences for the perceived integrity and legitimacy of proceedings. In *Horndom Ltd. v. White Sail Shipping, Optima Shipping and Integral Petroleum (SCC Arbitration V094/2011)*, the respondents challenged their own appointee to the tribunal after he accidentally copied one of the parties' lawyers on an e-mail complaining that counsel were getting "above their station" and that he was "rather sick of these parties." While the arbitrator admitted that disagreement over the hearing date resulted in his "frustration with procedural matters" and "intemperate expression," according to the respondents, the inadvertent disclosure of this otherwise private exchange among tribunal members revealed the arbitrator's "personal animosity" toward counsel and raised justifiable doubts about his impartiality. *See also* Alison Ross, *Accidental cc Triggers Double Arbitrator Challenge in Stockholm*, GLOB. ARB. REV. (Oct. 17, 2016), <http://globalarbitrationreview.com/article/1069329/accidental-cc-triggers-double-arbitrator-challenge-in-stockholm>.

92. An episode of the popular CBS TV show *The Good Wife* was based on the disclosure of confidential information resulting from an open feed when a video camera was mistakenly left on after a teleconferenced deposition. *THE GOOD WIFE*, (CBS, 2014), http://www.cbs.com/shows/the_good_wife/episodes/213197/.

93. *See, e.g., supra* note 88 and accompanying text.

94. *Law Technology Resource Center*, AMERICAN BAR ASSOCIATION http://www.americanbar.org/groups/departments_offices/legal_technology_resources/resource.s.html (last visited Jan. 20, 2017).

profession. One particularly noteworthy resource, available only to ABA members, are e-mail alerts from the FBI about evolving cyber risks and threats targeting law firms.

Other bar associations worldwide, such as the Law Society of Upper Canada, also have developed helpful online resources.⁹⁵ For the most part, such resources are available for free online (i.e., to members and non-members alike) and can assist arbitrators in finding quick, practical answers to technical questions written for legal professionals (such as what are the risks of public wifi and what alternatives are available for mobile wifi access). Meanwhile, to keep a handle on evolving data protection obligations internationally, now that most major law firms have a dedicated data privacy or cybersecurity practice group, arbitrators may also find it helpful to sign up for e-mail alerts from several law firms based in different jurisdictions.

B. Implementing Baseline Security

Cybersecurity experts agree that good cyber “hygiene”—basic everyday habits relating to technological use—is essential to a strong, baseline defense.⁹⁶ Significantly, these are habits that every arbitrator, regardless of practice setting, can readily implement, with minimal cost and without the need for IT support. Basic cyber hygiene best practices include:

- creating access controls, including strong, complex passwords⁹⁷ and two-factor authentication when available⁹⁸;

95. See *Technology Practice Tips*, LAW SOCIETY OF UPPER CANADA <http://www.lsuc.on.ca/technology-practice-tips-podcasts-list/> (podcasts on “everything you ever wanted to know about technology, but were afraid to ask” including “[p]ractical and important information about passwords, encryption, social media, smartphone security, websites and much more . . . in an accessible, conversational manner.”).

96. See, e.g., FED. TRADE COMM’N, *START WITH SECURITY: A GUIDE FOR BUSINESS, LESSONS LEARNED FROM FTC CASES* (June 2015), <https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf>; Wimmer et. al., *supra* note 89.

97. On some devices, including many phones and tablets, biometric authentication technologies such as fingerprint scanners now are available to perform the authentication and access control function. See PWC Report, *supra* note 13, at 9-12.

98. Many services and sites that store sensitive information, including cloud storage and e-mail providers, offer two-factor authentication whereby access requires a password plus something else that you have; typically, a security code that is either sent by text message or e-mail to a separate device or generated via an app that works offline such as Google Authenticator, or a biometric like a fingerprint. See *Two-Factor Authentication for AppleID*,

- guarding digital “perimeters” with firewalls, antivirus and antispyware software, operating system updates and other software patches⁹⁹;
- adopting secure protocols such as encryption for the storage and transmission of sensitive data¹⁰⁰;
- being mindful of public internet use in hotel lobbies, airports, coffee shops, and elsewhere and considering making use of personal cellular hotspots and virtual private networks¹⁰¹; and
- being mindful of what one downloads.¹⁰²

C. Taking a Thoughtful Approach to Assets and Architecture

As Pastore explains, determining what cybersecurity should be implemented turns on knowledge of one’s “assets” and “architecture.”¹⁰³ That is, what sensitive information do you have (e.g., customer lists of a client, sensitive trade secrets developed through substantial R&D expenditures, or potentially market-moving information about future business plans), and where do you store it (e.g., with a third-party cloud provider, on portable (and easily lost) external media like thumb drives, or on networks accessible by other practitioners in the firm without regard to whether the need access to such data).¹⁰⁴ This exercise will be relevant in respect to the arbitrator’s own practice-related data, such as conflicts and billing records, closed case records, as well as the data received in matters where the arbitrator is presiding. If the arbitrator works in an organizational setting, it will also be relevant in respect to the arbitrator’s use of personal devices, which are often not subject to

APPLE, <https://support.apple.com/en-us/HT204915> (last visited Jan. 22, 2017); *Google Two-Step Verification*, GOOGLE, <https://www.google.com/landing/2step/> (last visited Jan. 22, 2017); Seth Rosenblatt & Jason Cipriani, *Two-Factor Authentication (What You Need to Know)*, CNET, (June 15, 2015), <https://www.cnet.com/news/two-factor-authentication-what-you-need-to-know-faq/>.

99. See *Protections, How to Protect Your Computer*, FBI, <https://www.fbi.gov/investigate/cyber> (last visited Jan. 20, 2017).

100. See e.g., Alex Castle, *How to Encrypt Almost Anything*, PC WORLD, (Jan, 18, 2013), <http://www.pcmag.com/article/2025462/how-to-encrypt-almost-anything.html>.

101. Pastore, *supra* note 15.

102. See *supra* note 99.

103. In this article, we frequently refer synonymously to one’s digital “infrastructure.”

104. Pastore, *supra* note 15.

established security protocols.¹⁰⁵

Once the arbitrator knows and classifies the sensitivity of the different data he or she holds and knows where it is located, the arbitrator will be in a position to assess what protocols may be appropriate for storage and transfer of the information.¹⁰⁶ In addition, the arbitrator will be in a position to consider what steps can be taken to reduce the risk that sensitive data will be compromised in a cyberattack or following human error. For example:

- Though the arbitrator may own both a tablet and laptop, do arbitration-related documents need to be accessible on both devices, or is it sufficient that they are loaded on one? (Here, an important consideration is whether the data really needs to be loaded onto a portable device and subjected to the enhanced risks of travel.)
- Can the arbitrator enable notifications for e-mail¹⁰⁷ or cloud services¹⁰⁸ when unauthorized data access may have occurred and remotely revoke that access or wipe data?
- When working at home, does the arbitrator use a separate device in lieu of a shared family computer? If not, are there other steps the arbitrator can take to segregate business data (e.g., by using separate computer logins)?

By the same token, at the conclusion of a case, the arbitrator should seek to avoid holding onto case-related data longer than is

105. According to the ABA TechReport 2016, most lawyers (74%) use a personal rather than firm-issued phone for their legal work and a majority (51%) use a tablet for legal work, the vast majority of which (81%) are personal devices. Nonetheless, “only 43% of lawyers reported having a mobile technology policy for their firm, meaning the majority of law firms don’t even have a policy for how mobile devices should be used and how client data should be stored and transmitted on them.” Aaron Street, *Mobile Technology*, ABA TECHREPORT (2016), <http://www.americanbar.org/publications/techreport/2016/mobile.html>.

106. Pastore discusses this analysis in greater detail. *See* Pastore *supra* note 15.

107. Such measures are generally not available for free consumer e-mail services. Thus it is generally preferable to use paid professional versions of these services, which have more robust security protocols.

108. Numerous lawyer ethics opinions have considered whether the use of cloud services is compatible with an attorney’s obligation to maintain confidentiality. The decisions generally have concluded that lawyers may use the services, provided that they take reasonable steps to select a reliable vendor, implement available security and address the potential risks. *See* Cloud Ethics Opinions Around the U.S., AMERICAN BAR ASSOCIATION, http://www.americanbar.org/groups/departments_offices/legal_technology_resources/resources/charts_fyis/cloud-ethics-chart.html

necessary.¹⁰⁹ With a view to developing an individualized document retention policy, the arbitrator should give thought to what information will be kept, why, for how long, where case information resides now (across which devices and in what applications/programs), and where the materials will be stored. At a minimum, the arbitrator will want to retain basic case administration data for the purposes of future conflicts checks. Otherwise, the arbitrator may wish to consider questions such as:

- During the life of a case, can the arbitrator use file-naming conventions to facilitate identifying and segregating types of documents, such as pleadings and exhibits, that the arbitrator is unlikely to have any interest in retaining after a case ends?
- Does applicable law preclude the arbitrator from retaining certain data or mandate that it be stored or disposed of in any particular fashion?
- To the extent that it is desirable and appropriate to retain arbitrator work product, such as procedural orders and awards, for personal future reference, would it be workable to retain anonymized Word documents in lieu of final PDF copies?
- If the arbitrator practices in an organizational setting that has a document retention policy, are documents kept longer than necessary to comply with rules applicable to the attorney-client relationship, which do not apply to service as an arbitrator?

D. Planning for a Data Breach

Separate from considering data breach protocols for individual cases, there are a number of useful reasons for the arbitrator to consider more generally how he or she would respond to a data breach if and when one arises. First, by thinking through what steps should be taken in the event of various scenarios, the arbitrator may be able to identify and remediate security vulnerabilities that he or she had not considered. Second, the arbitrator will be in a better position to react quickly to control or limit the damage that flows from a security incident, and possibly avoid triggering duties to notify data owners, regulators, insurers, law enforcement, or others that a security

109. Pastore, *supra* note 15.

incident occurred.¹¹⁰ This exercise is particularly important for international arbitrators for whom international travel is a fact of life, as travel creates special risks of inadvertent data loss and vulnerability to unlawful intrusion.

The prospect of a lost laptop, for example, may prompt an arbitrator to consider:

- Is the laptop protected by a strong password?
- Is full disk encryption enabled?¹¹¹
- Can the arbitrator make use of location tracking and/or remote data wiping to minimize potential disclosure of sensitive information?¹¹²
- Can the arbitrator provide the police with the serial number for the laptop?
- Can the arbitrator avoid lost productivity by restoring information on the laptop from a back-up?
- Is there sensitive data on the laptop that could trigger breach notification duties? If so, could that data be handled differently (e.g., securely destroyed or encrypted)?

E. Case Management Considerations

In our view, the arbitrator must be attuned to data security issues in the organizing phase of the arbitration. Taking into account such

110. See, e.g., U.S. Department of Health & Human Services, *Guidance Regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA)*, https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/#_edn1 (last accessed Jan. 21, 2017) (explaining that there is often a safe harbor for data breach notification if sensitive information has been encrypted or otherwise de-sensitized); Kamala D. Harris, Attorney General California, Department of Justice, *Breach Report 2016*, available at <https://oag.ca.gov/breachreport2016> (last accessed Jan. 21, 2017) (explaining major differences between state notification statutes); See Cal. Civil Code § 1798.82 (demonstrating that in 2016, California amended its data breach notification law effective January 1, 2017 to trigger notification obligations not only if unencrypted data is compromised, but also if encrypted data is breached along with any encryption key that could render the data readable or useable).

111. See *Turn On Full Disk Encryption (Windows 10)*, MICROSOFT, <https://support.microsoft.com/en-us/instantanswers/e7d75dd2-29c2-16ac-f03d-20cfd54202f/turn-on-device-encryption>; see also *Use FileVault to Encrypt the Start-Up Disk on Your MAC*, APPLE, <https://support.apple.com/en-us/HT204837>.

112. These measures are available for Apple devices including laptops, for example, but only if the “find my iPhone” feature has been activated first.

factors as the size and complexity of the case, the likelihood that confidential or sensitive data will be stored or transmitted, the parties' resources, sophistication, and preferences, as well as potential legal obligations arising under applicable law or rules in relation to data privacy or confidentiality, the arbitrator should consider whether to raise the topic of data security at the initial case management or procedural conference.¹¹³ Thereafter, the continuing scope of the arbitrator's duty will depend on factors such as the extent to which the parties or their counsel assume responsibility for data security and the arbitrator's own assessment of the ongoing risks and the measures he or she can reasonably implement in addition to or in lieu of measures other actors are undertaking.

The arbitrator may also seek the cooperation of the parties and counsel in avoiding the unnecessary transmission of sensitive data to the tribunal. For example, at the outset of an arbitration, the arbitrator may consider telling counsel that, apart from reliance documents submitted with the parties' memorials, the arbitrator is not to be copied on, or provided with, any pre-hearing disclosure that the parties may otherwise exchange. Likewise, if the arbitrator can anticipate that sensitive personal information (such as tax returns) or commercial information (such as pricing information or trade secrets) will be exchanged, consideration may be given to having irrelevant information redacted (e.g., to show only the last four digits of a social security number). Alternatively, it may be possible to aggregate or anonymize data before it is provided to the arbitrator without diminishing either party's ability to fairly present its case.

VI. LOOKING TO THE FUTURE

We conclude this article with the well-worn maxim that "it takes a village." We hope that the challenge we present to arbitrators will stimulate discussion in the international commercial arbitration community and prompt other participants to focus on their own responsibilities and how their individual security architecture and practices may undermine or support the security measures taken by

113. See UNCITRAL Notes, *supra* note 26. Consistent with the 2016 UNCITRAL Notes on Organizing Arbitral Proceedings, we do not intend to suggest a binding requirement for the tribunal or parties to act in any particular manner.

others. As awareness of cybersecurity risks in arbitration increases, we hope to see dialogue around questions such as the following:

- Should arbitral institutions amend their rules to flag data security for consideration in the initial organizing phase of an arbitration, as their rules now do with respect to other important topics,¹¹⁴ and/or should they expressly establish duties for the parties, counsel, institution and arbitrators to implement reasonable measures to avoid intrusion?
- Should counsel be charged with developing a data security plan in individual arbitration matters¹¹⁵ and/or providing a secure platform for the transmission and storage of data in each matter?
- How should tribunals resolve party conflicts about appropriate security measures, breach notification obligations, and related costs?
- Should arbitrators routinely disclose their data security practices to parties and counsel (e.g., in relation to cloud computing or post-award document retention) and should those practices be subject to the parties' comments and consent?
- Should arbitral institutions or other participants develop shared secured platforms for data storage and transmission that would be available to parties as a non-exclusive choice?
- What kinds of training and education programs should be developed for parties, counsel, arbitrators, and other participants to provide baseline knowledge, as well as updated information on evolving data security threats and updates on available protective measures?

114. See e.g., ICC RULES, *supra* note 10, at art. 22, (effective case management) and Appendix IV (case management techniques); ICDR RULES, *supra* note 10, at art. 20(2) (noting that the tribunal and the parties may consider how technology, including electronic communications, could be used to increase the efficiency and economy of the proceedings) and art. 20(7) (establishing the parties' duty to avoid unnecessary delay and expense and the tribunal's power to "allocate costs, draw adverse inferences, and take such additional steps as are necessary to protect the efficiency and integrity of the arbitration"); LCIA RULES, *supra* note 1, at art. 14 (avoiding unnecessary delay and expense) and art. 30 (confidentiality).

115. See David J. Kessler, et al., *Protective Orders in the Age of Hacking*, NYLJ, (Mar. 16, 2015), reprint at 1 ("In the age of cyber attacks, hacking, and digital corporate espionage... [p]rotective orders should be upgraded to require reasonable levels of security to protect an opponents' data and more stringent notification requirements if unauthorized access does occur . . .").

- Should institutions that maintain rosters of arbitrators require their arbitrators to complete mandatory cybersecurity training?
- Should arbitrator ethical codes be updated to define competence to include an obligation to keep abreast of new developments in arbitration and its practice, and to consider the benefits and risks associated with technology?
- Should professional organizations like the International Bar Association or the Chartered Institute of Arbitrators develop cybersecurity checklists or guidance notes for arbitrators, counsel, or other participants?

There will no right answer to these and other relevant questions, but we are confident that dialogue will be constructive. What will constitute a reasonable data security program and what reasonable measures individual participants in the process should take will continue to evolve. Our hope is that increased awareness will ensure that a process will emerge in every arbitration to identify data security risks and develop a response, having regard to the nature and scope of the risks, the desires and resources of the parties, and other relevant factors.



**Debevoise
& Plimpton**

Protocol to Promote Cybersecurity in International Arbitration

Debevoise Protocol to Promote Cybersecurity in International Arbitration

As the prevalence of malicious cyberactors and cyberattacks on high-profile companies and government organizations grows, parties to commercially or politically sensitive international arbitrations increasingly express concerns with respect to cybersecurity. Cybersecurity threats may create significant operational and legal problems that can compromise the arbitral process, including loss or unauthorized disclosure of sensitive data, breaches of attorney-client confidentiality, adverse media coverage and reputational damage, costs associated with breach notification or data recovery, and legal liability. In addition to the threat cyberattacks pose to the parties to an arbitration, failing to address this problem could ultimately lead to a loss of confidence in the arbitral system.

To respond to these concerns, the practitioners at Debevoise & Plimpton LLP have developed this Protocol to Promote Cybersecurity in International Arbitration. This Protocol operates on three principles: (i) Establishing Secure Protocols for the Transfer of Sensitive Information at the Outset of Proceedings, (ii) Limiting Disclosure and Use of Sensitive Information, and (iii) Developing Procedures for Disclosing Cyber Incidents.

The Protocol reflects our continued commitment to counsel clients on the most critical issues in international arbitration. We believe consideration of the procedures reflected in this Protocol will improve the arbitration process while appropriately managing risks. The procedures reflected in this Protocol are meant to be adaptable, so that parties, counsel and arbitral tribunals can use the flexibility inherent in international arbitration to develop procedures relevant and appropriate for each individual arbitration.



Protocols for Transfer and Storage of Sensitive Information

1. We will request that the arbitral tribunal establish protocols and procedures for the transfer of sensitive information at the outset of proceedings, usually in the first procedural conference. What constitutes such sensitive information should be defined in light of the particular circumstances of a dispute.
 - a. These protocols and procedures may include: (i) defining categories of sensitive information, updated as necessary through the course of the proceeding; and (ii) agreeing on processes for the secure transfer of such sensitive information between and among the tribunal and the parties.
 - b. This may include barring certain transfer methods (e.g., use of public WiFi to access sensitive information) or adopting certain transfer methods (e.g., use of secure portals instead of email).
2. We will ask the arbitral tribunal and the parties to consider and, if appropriate, agree to specific encryption standards for the transmission of sensitive information.
3. We will propose and encourage arbitral tribunals to disfavor the use of insecure email for the transmission of sensitive information unless additional measures are taken to secure the information. Such additional measures may include applying passwords to documents containing sensitive information that will be transmitted via separate channels (e.g., texting or via a phone call).
4. We will propose that, where possible, email accounts maintained by third party public servers (e.g., Gmail) have additional access protections such as multi-factor authentication (e.g., use of a token or similar mechanism in addition to username and password).
5. If third-party cloud storage is used, we will consider whether the third-party cloud storage incorporates adequate security protocols.
6. We will consider, and ask that the arbitral tribunal and opposing party consider, applicable governmental cross-border restrictions on the transfer of sensitive information and adopt reasonable measures to facilitate compliance with any restrictions.

Limited Disclosure and Use of Sensitive Information

7. Before submitting any sensitive information to the arbitral tribunal or opposing party, we will weigh the sensitivity of that information against the relevance and materiality of that information for that arbitration.
8. We will explore with the arbitral tribunal whether sensitive information may be submitted in a form that is only screen viewable (i.e., not downloadable or printable). If sensitive information is permitted to be printed, we will ask the tribunal to establish consistent policies and procedures related to the destruction of printed materials.
9. To the extent practicable, we will limit the persons who have access to sensitive information to those persons having a need-to-know with respect to such information.
10. To the extent practicable, access to sensitive information on computer systems should be restricted to those using a secure log-in ID and password, with a unique log-in ID and password assigned to each individual. We will consider, and ask that the arbitral tribunal and opposing party consider, the use of multi-factor authentication to access accounts or portals used to transmit and receive sensitive information.
11. We will restrict the ability to transfer sensitive information to mobile devices only if they use encryption or other appropriate security protocols.
12. At the client's request, we will establish procedures for returning or destroying sensitive information upon the conclusion of the arbitration.

Procedure for Disclosing Data Breaches

13. We will take reasonable steps to mitigate any potential breach, including by contracting with third-party vendors as necessary.
14. We will propose and work with the arbitral tribunal to establish policies and procedures related to detecting breaches, determining their scope, and notifying affected parties. Where the existence of the arbitration is itself confidential, we will work with the tribunal to consider means of notifying affected parties that best preserve the confidentiality of the arbitration.
15. We will propose and work with the arbitral tribunal to establish point-persons for each party to the arbitration and the tribunal itself to be responsible for coordinating communications in the event of a data breach or other incident that exposes or affects sensitive information.
16. We will consider whether there are any legal obligations to report the breach to affected parties, regulatory agencies, or other authorities.

Debevoise & Plimpton

New York

919 Third Avenue
New York, NY 10022
+1 212 909 6000

Washington, D.C.

801 Pennsylvania Avenue N.W.
Washington, D.C. 20004
+1 202 383 8000

London

65 Gresham Street
London
EC2V 7NQ
+44 20 7786 9000

Paris

4 place de l'Opéra
75002 Paris
+33 1 40 73 12 12

Frankfurt

Taunustor 1 (TaunusTurm)
60310 Frankfurt am Main
+49 69 2097 5000

Moscow

Business Center Mokhovaya
Ulitsa Vozdvizhenka, 4/7
Stroyeniye 2
Moscow, 125009
+7 495 956 3858

Hong Kong

21/F AIA Central
1 Connaught Road Central
Hong Kong
+852 2160 9800

Shanghai

13/F, Tower 1
Jing'an Kerry Centre
1515 Nanjing Road West
Shanghai 200040
+86 21 5047 1800

Tokyo

Shin Marunouchi Bldg. 11F
1-5-1 Marunouchi, Chiyoda-ku
Tokyo 100-6511
+81 3 4570 6680



**START
WITH**

SECURITY

A GUIDE FOR BUSINESS



FEDERAL TRADE COMMISSION | BUSINESS.FTC.GOV

START WITH SECURITY

1. **Start with security.**

2. **Control access to data sensibly.**

3. **Require secure passwords and authentication.**

4. **Store sensitive personal information securely and protect it during transmission.**

5. **Segment your network and monitor who's trying to get in and out.**

6. **Secure remote access to your network.**

7. **Apply sound security practices when developing new products.**

8. **Make sure your service providers implement reasonable security measures.**

9. **Put procedures in place to keep your security current and address vulnerabilities that may arise.**

10. **Secure paper, physical media, and devices.**

When managing your network, developing an app, or even organizing paper files, sound security is no accident. Companies that consider security from the start assess their options and make reasonable choices based on the nature of their business and the sensitivity of the information involved. Threats to data may transform over time, but the fundamentals of sound security remain constant. As the Federal Trade Commission outlined in *Protecting Personal Information: A Guide for Business*, you should know what personal information you have in your files and on your computers, and keep only what you need for your business. You should protect the information that you keep, and properly dispose of what you no longer need. And, of course, you should create a plan to respond to security incidents.

In addition to *Protecting Personal Information*, the FTC has resources to help you think through how those principles apply to your business. There's an online tutorial to help train your employees; publications to address particular data security challenges; and news releases, blog posts, and guidance to help you identify – and possibly prevent – pitfalls.

There's another source of information about keeping sensitive data secure: the lessons learned from the more than 50 law enforcement actions the FTC has announced so far. These are settlements – no findings have been made by a court – and the specifics of the orders apply just to those companies, of course. But learning about alleged lapses that led to law enforcement can help your company improve its practices. And most of these alleged practices involve basic, fundamental security missteps. Distilling the facts of those cases down to their essence, here are ten lessons to learn that touch on vulnerabilities that could affect your company, along with practical guidance on how to reduce the risks they pose.

1

Start with security.

From personal data on employment applications to network files with customers' credit card numbers, sensitive information pervades every part of many companies. Business executives often ask how to manage confidential information. Experts agree on the key first step: Start with security. Factor it into the decisionmaking in every department of your business – personnel, sales, accounting, information technology, etc. Collecting and maintaining information “just because” is no longer a sound business strategy. Savvy companies think through the implication of their data decisions. By making conscious choices about the kind of information you collect, how long you keep it, and who can access it, you can reduce the risk of a data compromise down the road. Of course, all of those decisions will depend on the nature of your business. Lessons from FTC cases illustrate the benefits of building security in from the start by going lean and mean in your data collection, retention, and use policies.

Don't collect personal information you don't need.

Here's a foundational principle to inform your initial decision-making: No one can steal what you don't have. When does your company ask people for sensitive information? Perhaps when they're registering online or setting up a new account. When was the last time you looked at that process to make sure you really need everything you ask for? That's the lesson to learn from a number of FTC cases. For example, the FTC's complaint against [RockYou](#) charged that the company collected lots of information during the site registration process, including the user's email address and email password. By collecting email passwords – not something the business needed – and then storing them in clear text, the FTC said the company created an unnecessary risk to people's email accounts. The business could have avoided that risk simply by not collecting sensitive information in the first place.

Hold on to information only as long as you have a legitimate business need.

Sometimes it's necessary to collect personal data as part of a transaction. But once the deal is done, it may be unwise to keep it. In the FTC's [BJ's Wholesale Club](#) case, the company collected customers' credit and debit card information to process transactions in its retail stores. But according to the complaint, it continued to store that data for up to 30 days – long after the sale was complete. Not only did that violate bank rules, but by holding on to the information without a legitimate business need, the FTC said BJ's Wholesale Club created an unreasonable risk. By exploiting other weaknesses in the company's security practices, hackers stole the account data and used it to make counterfeit credit and debit cards. The business could have limited its risk by securely disposing of the financial information once it no longer had a legitimate need for it.

Don't use personal information when it's not necessary.

You wouldn't juggle with a Ming vase. Nor should businesses use personal information in contexts that create unnecessary risks. In the *Accretive* case, the FTC alleged that the company used real people's personal information in employee training sessions, and then failed to remove the information from employees' computers after the sessions were over. Similarly, in *foru International*, the FTC charged that the company gave access to sensitive consumer data to service providers who were developing applications for the company. In both cases, the risk could have been avoided by using fictitious information for training or development purposes.

2

Control access to data sensibly.

Once you've decided you have a legitimate business need to hold on to sensitive data, take reasonable steps to keep it secure. You'll want to keep it from the prying eyes of outsiders, of course, but what about your own employees? Not everyone on your staff needs unrestricted access to your network and the information stored on it. Put controls in place to make sure employees have access only on a "need to know" basis. For your network, consider steps such as separate user accounts to limit access to the places where personal data is stored or to control who can use particular databases. For paper files, external drives, disks, etc., an access control could be as simple as a locked file cabinet. When thinking about how to control access to sensitive information in your possession, consider these lessons from FTC cases.

Restrict access to sensitive data.

If employees don't have to use personal information as part of their job, there's no need for them to have access to it. For example, in *Goal Financial*, the FTC alleged that the company failed to restrict employee access to personal information stored in paper files and on its network. As a result, a group of employees transferred more than 7,000 consumer files containing sensitive information to third parties without authorization. The company could have prevented that misstep by implementing proper controls and ensuring that only authorized employees with a business need had access to people's personal information.

Limit administrative access.

Administrative access, which allows a user to make system-wide changes to your system, should be limited to the employees tasked to do that job. In its action against *Twitter*, for example, the FTC alleged that the company granted almost all of its employees administrative control over Twitter's system, including the ability to reset user account passwords, view users' nonpublic tweets, and send tweets on users' behalf. According to the complaint, by providing administrative access to just about everybody in-house, Twitter increased the risk that a compromise of any of its employees' credentials could result in a serious breach. How could the company have reduced that risk? By ensuring that employees' access to the system's administrative controls was tailored to their job needs.

3

Require secure passwords and authentication.

If you have personal information stored on your network, strong authentication procedures – including sensible password “hygiene” – can help ensure that only authorized individuals can access the data. When developing your company's policies, here are tips to take from FTC cases.

Insist on complex and unique passwords.

“Passwords” like 121212 or qwerty aren't much better than no passwords at all. That's why it's wise to give some thought to the password standards you implement. In the *Twitter* case, for example, the company let employees use common dictionary words as administrative passwords, as well as passwords they were already using for other accounts. According to the FTC, those lax practices left Twitter's system vulnerable to hackers who used password-guessing tools, or tried passwords stolen from other services in the hope that Twitter employees used the same password to access the company's system. Twitter could have limited those risks by implementing a more secure password system – for example, by requiring employees to choose complex passwords and training them not to use the same or similar passwords for both business and personal accounts.

Store passwords securely.

Don't make it easy for interlopers to access passwords. In *Guidance Software*, the FTC alleged that the company stored network user credentials in clear, readable text that helped a hacker access customer credit card information on the network. Similarly, in *Reed Elsevier*, the FTC charged that the business allowed customers to store user credentials in a vulnerable format in cookies on their computers. In *Twitter*, too, the FTC said the company failed to establish policies that prohibited employees from storing administrative passwords in plain text in personal email accounts. In each of those cases, the risks could have been reduced if the companies had policies and procedures in place to store credentials securely. Businesses also may want to consider other protections – two-factor authentication, for example – that can help protect against password compromises.

Guard against brute force attacks.

Remember that adage about an infinite number of monkeys at an infinitive number of typewriters? Hackers use automated programs that perform a similar function. These brute force attacks work by typing endless combinations of characters until hackers luck into someone's password. In the *Lookout Services*, *Twitter*, and *Reed Elsevier* cases, the FTC alleged that the businesses didn't suspend or disable user credentials after a certain number of unsuccessful login attempts. By not adequately restricting the number of tries, the companies placed their networks at risk. Implementing a policy to suspend or disable accounts after repeated login attempts would have helped to eliminate that risk.

Protect against authentication bypass.

Locking the front door doesn't offer much protection if the back door is left open. In *Lookout Services*, the FTC charged that the company failed to adequately test its web application for widely-known security flaws, including one called "predictable resource location." As a result, a hacker could easily predict patterns and manipulate URLs to bypass the web app's authentication screen and gain unauthorized access to the company's databases. The company could have improved the security of its authentication mechanism by testing for common vulnerabilities.

4

Store sensitive personal information securely and protect it during transmission.

For many companies, storing sensitive data is a business necessity. And even if you take appropriate steps to secure your network, sometimes you have to send that data elsewhere. Use strong cryptography to secure confidential material during storage and transmission. The method will depend on the types of information your business collects, how you collect it, and how you process it. Given the nature of your business, some possibilities may include Transport Layer Security/Secure Sockets Layer (TLS/SSL) encryption, data-at-rest encryption, or an iterative cryptographic hash. But regardless of the method, it's only as good as the personnel who implement it. Make sure the people you designate to do that job understand how your company uses sensitive data and have the know-how to determine what's appropriate for each situation. With that in mind, here are a few lessons from FTC cases to consider when securing sensitive information during storage and transmission.

Keep sensitive information secure throughout its lifecycle.

Data doesn't stay in one place. That's why it's important to consider security at all stages, if transmitting information is a necessity for your business. In *Superior Mortgage Corporation*, for example, the FTC alleged that the company used SSL encryption to secure the transmission of sensitive personal information between the customer's web browser and the business's website server. But once the information reached the server, the company's service provider decrypted it and emailed it in clear, readable text to the company's headquarters and branch offices. That risk could have been prevented by ensuring the data was secure throughout its lifecycle, and not just during the initial transmission.

Use industry-tested and accepted methods.

When considering what technical standards to follow, keep in mind that experts already may have developed effective standards that can apply to your business. Savvy companies don't start from scratch when it isn't necessary. Instead, they take advantage of that collected wisdom. The *ValueClick* case illustrates that principle. According to the FTC, the company stored sensitive customer information collected through its e-commerce sites in a database that used a non-standard, proprietary form of encryption. Unlike widely-accepted encryption algorithms that are extensively tested, the complaint charged that ValueClick's method used a simple alphabetic substitution system subject to significant vulnerabilities. The company could have avoided those weaknesses by using tried-and-true industry-tested and accepted methods for securing data.

Ensure proper configuration.

Encryption – even strong methods – won't protect your users if you don't configure it properly. That's one message businesses can take from the FTC's actions against *Fandango* and *Credit Karma*. In those cases, the FTC alleged that the companies used SSL encryption in their mobile apps, but turned off a critical process known as SSL certificate validation without implementing other compensating security measures. That made the apps vulnerable to man-in-the-middle attacks, which could allow hackers to decrypt sensitive information the apps transmitted. Those risks could have been prevented if the companies' implementations of SSL had been properly configured.

5

Segment your network and monitor who's trying to get in and out.

When designing your network, consider using tools like firewalls to segment your network, thereby limiting access between computers on your network and between your computers and the internet. Another useful safeguard: intrusion detection and prevention tools to monitor your network for malicious activity. Here are some lessons from FTC cases to consider when designing your network.

Segment your network.

Not every computer in your system needs to be able to communicate with every other one. You can help protect particularly sensitive data by housing it in a separate secure place on your network. That's a lesson from the *DSW* case. The FTC alleged that the company didn't sufficiently limit computers from one in-store network from connecting to computers on other in-store and corporate networks. As a result, hackers could use one in-store network to connect to, and access personal information on, other in-store and corporate networks. The company could have reduced that risk by sufficiently segmenting its network.

Monitor activity on your network.

“Who’s that knocking on my door?” That’s what an effective intrusion detection tool asks when it detects unauthorized activity on your network. In the *Dave & Buster’s* case, the FTC alleged that the company didn’t use an intrusion detection system and didn’t monitor system logs for suspicious activity. The FTC says something similar happened in *Cardsystem Solutions*. The business didn’t use sufficient measures to detect unauthorized access to its network. Hackers exploited weaknesses, installing programs on the company’s network that collected stored sensitive data and sent it outside the network every four days. In each of these cases, the businesses could have reduced the risk of a data compromise or its breadth by using tools to monitor activity on their networks.

6

Secure remote access to your network.

Business doesn’t just happen in the office. While a mobile workforce can increase productivity, it also can pose new security challenges. If you give employees, clients, or service providers remote access to your network, have you taken steps to secure those access points? FTC cases suggest some factors to consider when developing your remote access policies.

Ensure endpoint security.

Just as a chain is only as strong as its weakest link, your network security is only as strong as the weakest security on a computer with remote access to it. That’s the message of FTC cases in which companies failed to ensure that computers with remote access to their networks had appropriate endpoint security. For example, in *Premier Capital Lending*, the company allegedly activated a remote login account for a business client to obtain consumer reports, without first assessing the business’s security. When hackers accessed the client’s system, they stole its remote login credentials and used them to grab consumers’ personal information. According to the complaint in *Settlement One*, the business allowed clients that didn’t have basic security measures, like firewalls and updated antivirus software, to access consumer reports through its online portal. And in *Lifelock*, the FTC charged that the company failed to install antivirus programs on the computers that employees used to remotely access its network. These businesses could have reduced those risks by securing computers that had remote access to their networks.

Put sensible access limits in place.

Not everyone who might occasionally need to get on your network should have an all-access, backstage pass. That's why it's wise to limit access to what's needed to get the job done. In the *Dave & Buster's* case, for example, the FTC charged that the company failed to adequately restrict third-party access to its network. By exploiting security weaknesses in the third-party company's system, an intruder allegedly connected to the network numerous times and intercepted personal information. What could the company have done to reduce that risk? It could have placed limits on third-party access to its network – for example, by restricting connections to specified IP addresses or granting temporary, limited access.

7

Apply sound security practices when developing new products.

So you have a great new app or innovative software on the drawing board. Early in the development process, think through how customers will likely use the product. If they'll be storing or sending sensitive information, is your product up to the task of handling that data securely? Before going to market, consider the lessons from FTC cases involving product development, design, testing, and roll-out.

Train your engineers in secure coding.

Have you explained to your developers the need to keep security at the forefront? In cases like *MTS*, *HTC America*, and *TRENDnet*, the FTC alleged that the companies failed to train their employees in secure coding practices. The upshot: questionable design decisions, including the introduction of vulnerabilities into the software. For example, according to the complaint in *HTC America*, the company failed to implement readily available secure communications mechanisms in the logging applications it pre-installed on its mobile devices. As a result, malicious third-party apps could communicate with the logging applications, placing consumers' text messages, location data, and other sensitive information at risk. The company could have reduced the risk of vulnerabilities like that by adequately training its engineers in secure coding practices.

Follow platform guidelines for security.

When it comes to security, there may not be a need to reinvent the wheel. Sometimes the wisest course is to listen to the experts. In actions against *HTC America*, *Fandango*, and *Credit Karma*, the FTC alleged that the companies failed to follow explicit platform guidelines about secure development practices. For example, Fandango and Credit Karma turned off a critical process known as SSL certificate validation in their mobile apps, leaving the sensitive information consumers transmitted through those apps open to interception through man-in-the-middle attacks. The companies could have prevented this vulnerability by following the iOS and Android guidelines for developers, which explicitly warn against turning off SSL certificate validation.

Verify that privacy and security features work.

If your software offers a privacy or security feature, verify that the feature works as advertised. In *TRENDnet*, for example, the FTC charged that the company failed to test that an option to make a consumer's camera feed private would, in fact, restrict access to that feed. As a result, hundreds of "private" camera feeds were publicly available. Similarly, in *Snapchat*, the company advertised that messages would "disappear forever," but the FTC says it failed to ensure the accuracy of that claim. Among other things, the app saved video files to a location outside of the app's sandbox, making it easy to recover the video files with common file browsing tools. The lesson for other companies: When offering privacy and security features, ensure that your product lives up to your advertising claims.

Test for common vulnerabilities.

There is no way to anticipate every threat, but some vulnerabilities are commonly known and reasonably foreseeable. In more than a dozen FTC cases, businesses failed to adequately assess their applications for well-known vulnerabilities. For example, in the *Guess?* case, the FTC alleged that the business failed to assess whether its web application was vulnerable to Structured Query Language (SQL) injection attacks. As a result, hackers were able to use SQL attacks to gain access to databases with consumers' credit card information. That's a risk that could have been avoided by testing for commonly-known vulnerabilities, like those identified by the Open Web Application Security Project (OWASP).

8

Make sure your service providers implement reasonable security measures.

When it comes to security, keep a watchful eye on your service providers – for example, companies you hire to process personal information collected from customers or to develop apps. Before hiring someone, be candid about your security expectations. Take reasonable steps to select providers able to implement appropriate security measures and monitor that they’re meeting your requirements. FTC cases offer advice on what to consider when hiring and overseeing service providers.

Put it in writing.

Insist that appropriate security standards are part of your contracts. In *GMR Transcription*, for example, the FTC alleged that the company hired service providers to transcribe sensitive audio files, but failed to require the service provider to take reasonable security measures. As a result, the files – many containing highly confidential health-related information – were widely exposed on the internet. For starters, the business could have included contract provisions that required service providers to adopt reasonable security precautions – for example, encryption.

Verify compliance.

Security can’t be a “take our word for it” thing. Including security expectations in contracts with service providers is an important first step, but it’s also important to build oversight into the process. The *Upromise* case illustrates that point. There, the company hired a service provider to develop a browser toolbar. Upromise claimed that the toolbar, which collected consumers’ browsing information to provide personalized offers, would use a filter to “remove any personally identifiable information” before transmission. But, according to the FTC, Upromise failed to verify that the service provider had implemented the information collection program in a manner consistent with Upromise’s privacy and security policies and the terms in the contract designed to protect consumer information. As a result, the toolbar collected sensitive personal information – including financial account numbers and security codes from secure web pages – and transmitted it in clear text. How could the company have reduced that risk? By asking questions and following up with the service provider during the development process.

9

Put procedures in place to keep your security current and address vulnerabilities that may arise.

Securing your software and networks isn't a one-and-done deal. It's an ongoing process that requires you to keep your guard up. If you use third-party software on your networks, or you include third-party software libraries in your applications, apply updates as they're issued. If you develop your own software, how will people let you know if they spot a vulnerability, and how will you make things right? FTC cases offer points to consider in thinking through vulnerability management.

Update and patch third-party software.

Outdated software undermines security. The solution is to update it regularly and implement third-party patches. In the *TJX Companies* case, for example, the FTC alleged that the company didn't update its anti-virus software, increasing the risk that hackers could exploit known vulnerabilities or overcome the business's defenses. Depending on the complexity of your network or software, you may need to prioritize patches by severity; nonetheless, having a reasonable process in place to update and patch third-party software is an important step to reducing the risk of a compromise.

Heed credible security warnings and move quickly to fix them.

When vulnerabilities come to your attention, listen carefully and then get a move on. In the *HTC America* case, the FTC charged that the company didn't have a process for receiving and addressing reports about security vulnerabilities. HTC's alleged delay in responding to warnings meant that the vulnerabilities found their way onto even more devices across multiple operating system versions. Sometimes, companies receive security alerts, but they get lost in the shuffle. In *Fandango*, for example, the company relied on its general customer service system to respond to warnings about security risks. According to the complaint, when a researcher contacted the business about a vulnerability, the system incorrectly categorized the report as a password reset request, sent an automated response, and marked the message as "resolved" without flagging it for further review. As a result, Fandango didn't learn about the vulnerability until FTC staff contacted the company. The lesson for other businesses? Have an effective process in place to receive and address security vulnerability reports. Consider a clearly publicized and effective channel (for example, a dedicated email address like `security@yourcompany.com`) for receiving reports and flagging them for your security staff.

Network security is a critical consideration, but many of the same lessons apply to paperwork and physical media like hard drives, laptops, flash drives, and disks. FTC cases offer some things to consider when evaluating physical security at your business.

Securely store sensitive files.

If it's necessary to retain important paperwork, take steps to keep it secure. In the *Gregory Navone* case, the FTC alleged that the defendant maintained sensitive consumer information, collected by his former businesses, in boxes in his garage. In *Lifelock*, the complaint charged that the company left faxed documents that included consumers' personal information in an open and easily accessible area. In each case, the business could have reduced the risk to their customers by implementing policies to store documents securely.

Protect devices that process personal information.

Securing information stored on your network won't protect your customers if the data has already been stolen through the device that collects it. In the 2007 *Dollar Tree* investigation, FTC staff said that the business's PIN entry devices were vulnerable to tampering and theft. As a result, unauthorized persons could capture consumer's payment card data, including the magnetic stripe data and PIN, through an attack known as "PED skimming." Given the novelty of this type of attack at the time, and a number of other factors, staff closed the investigation. However, attacks targeting point-of-sale devices are now common and well-known, and businesses should take reasonable steps to protect such devices from compromise.

Keep safety standards in place when data is en route.

Savvy businesses understand the importance of securing sensitive information when it's outside the office. In *Accretive*, for example, the FTC alleged that an employee left a laptop containing more than 600 files, with 20 million pieces of information related to 23,000 patients, in the locked passenger compartment of a car, which was then stolen. The *CBR Systems* case concerned alleged unencrypted backup tapes, a laptop, and an external hard drive – all of which contained sensitive information – that were lifted from an employee's car. In each case, the business could have reduced the risk to consumers' personal information by implementing reasonable security policies when data is en route. For example, when sending files, drives, disks, etc., use a mailing method that lets you track where the package is. Limit the instances when employees need to be out and about with sensitive data in their possession. But when there's a legitimate business need to travel with confidential information, employees should keep it out of sight and under lock and key whenever possible.

Dispose of sensitive data securely.

Paperwork or equipment you no longer need may look like trash, but it's treasure to identity thieves if it includes personal information about consumers or employees. For example, according to the FTC complaints in [Rite Aid](#) and [CVS Caremark](#), the companies tossed sensitive personal information – like prescriptions – in dumpsters. In [Goal Financial](#), the FTC alleged that an employee sold surplus hard drives that contained the sensitive personal information of approximately 34,000 customers in clear text. The companies could have prevented the risk to consumers' personal information by shredding, burning, or pulverizing documents to make them unreadable and by using available technology to wipe devices that aren't in use.

Looking for more information?

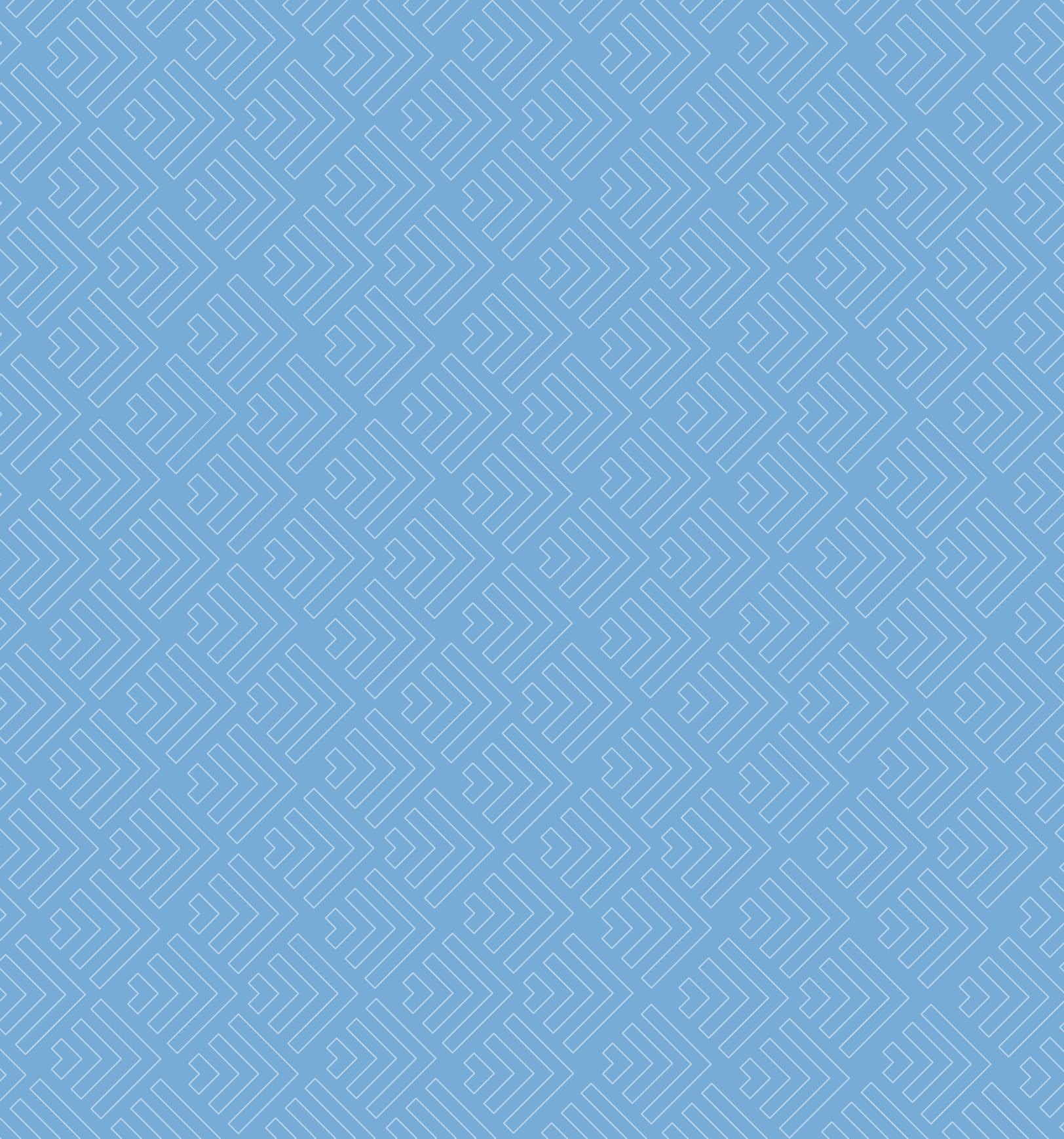
The FTC's Business Center (business.ftc.gov) has a Data Security section with an up-to-date listing of relevant cases and other free resources.

About the FTC

The FTC works for the consumer to prevent fraudulent, deceptive, and unfair practices in the marketplace. The Business Center gives you and your business tools to understand and comply with the law. Regardless of the size of your organization or the industry you're in, knowing – and fulfilling – your compliance responsibilities is smart, sound business. Visit the Business Center at business.ftc.gov.

Your Opportunity to Comment

The National Small Business Ombudsman and 10 Regional Fairness Boards collect comments from small businesses about federal compliance and enforcement activities. Each year, the Ombudsman evaluates the conduct of these activities and rates each agency's responsiveness to small businesses. Small businesses can comment to the Ombudsman without fear of reprisal. To comment, call toll-free 1-888-REGFAIR (1-888-734-3247) or go to sba.gov/ombudsman.



Federal Trade Commission
business.ftc.gov
June 2015

ETHICS OPINION 820

[LAWHUBSM \(HTTP://MYLAWHUB.NYSBA.ORG/\)](http://mylawhub.nysba.org/) | [CLE \(/CLE/CONTINUING LEGAL EDUCATION HOME/\)](#)

[EVENTS \(/STORE/CALENDARSCHEDULE.ASPX?EXCLUDEEVENTTYPE=X\)](#) | [SECTIONS & COMMITTEES \(/SECTIONSANDCOMMITTEES/\)](#)

[PUBLICATIONS \(/CUSTOMTEMPLATES/SECONDARYSTANDARD.ASPX?ID=43579\)](#) | [PRACTICE RESOURCES \(/PRACTICERESOURCES\)](#)

[LEADERSHIP & ADVOCACY \(/LEADERSHIPANDADVOCACY/\)](#) | [MEMBERSHIP \(/CUSTOMTEMPLATES/SECTIONLANDING.ASPX?ID=50848\)](#)

[MEMBERS ONLY \(HTTP://WWW.NYSBA.ORG/MYNYSBA.ASPX\)](http://www.nysba.org/mynysba.aspx)

[Home \(/\)](#) | [Ethics Opinion 820 \(/CustomTemplates/Content.aspx?id=5222\)](#)


[\(/CustomTemplates/Content.aspx?id=5222&css=print\)](#)  [Like 0](#)

New York State Bar Association Committee on Professional Ethics

Opinion #820 - 02/08/2008

Topic: Use of e-mail service provider that scans e-mails for advertising purposes.

Digest: A lawyer may use an e-mail service provider that conducts computer scans of e-mails to generate computer advertising, where the e-mails are not reviewed by or provided to human beings other than the sender and recipient.

Code: DR 4-101; EC 4-3.

QUESTION

May a lawyer use an e-mail service provider that scans e-mails by computer for keywords and then sends or displays instantaneously (to the side of the e-mails in question) computer-generated advertisements to users of the service based on the e-mail communications?

OPINION

Our starting point is N.Y. State 709 (1998), which addressed the use of Internet e-mail. We concluded based on developing experience that there is a reasonable expectation that e-mails will be as private as other forms of telecommunication and that therefore, under DR 4-101,^[1] a lawyer ordinarily may utilize unencrypted e-mail to transmit confidential information. We also noted, however, that a lawyer may not transmit client confidences by e-mail where there is a heightened risk of interception, and that "[a] lawyer who uses Internet e-mail must also stay abreast of this evolving technology to assess any changes in the likelihood of interception as well as the availability of improved technologies that may reduce such risks at reasonable cost."^[2]

In recent years, some e-mail providers have offered free or low-cost e-mail services in which, in exchange for providing the user with e-mail services - sending and receiving e-mail and providing storage on the provider's servers - the provider's computers scan e-mails and send or display targeted advertising to the user of the service. The e-mail provider identifies the presumed interests of the service's user by scanning for keywords in e-mails opened by the user. The provider's computers then send advertising that reflects the keywords in the e-mail. As an example, an e-mail that referred to travel to a particular locale might be accompanied by an advertisement for travel service providers in that locale.

Under the particular e-mail provider's published privacy policies, no individuals other than e-mail senders and recipients read the e-mail messages, are otherwise privy to their content or receive targeted advertisements from the service provider. Consequently, when the e-mail service provider sends or generates instantaneous computer-generated advertising based on computer scans of the lawyer's e-mails with clients, the risks posed to client confidentiality are not meaningfully different from the risks in using other e-mail service providers that do not employ this practice. We conclude, therefore, that the obligation to preserve client confidentiality does not preclude using such a service.^[3]

We would reach the opposite conclusion if the e-mails were reviewed by human beings or if the service provider reserved the right to disclose the e-mails or the substance of the communications to third parties without the sender's permission (or a lawful judicial order). Merely scanning the content of e-mails by computer to generate computer advertising, however, does not pose a threat to client confidentiality, because the practice does not increase the risk of others obtaining knowledge of the e-mails or access to the e-mails' content. A lawyer must exercise due care in selecting an e-mail service provider to ensure that its policies and stated practices protect client confidentiality.^[4] Unless the lawyer learns information suggesting that the provider is materially departing from conventional privacy policies or is using the information it obtains by computer-scanning of e-mails for a purpose that, unlike computer-generated advertising, puts confidentiality at risk, the use of such e-mail services comports with DR 4-101.

CONCLUSION

A lawyer may use an e-mail service provider that conducts computer scans of e-mails to generate computer advertising, where the e-mails are not reviewed by or provided to other individuals.

(32-07)

[1] Under DR 4?101 of the New York Lawyer's Code of Professional Responsibility, lawyers are required to preserve the confidences and secrets of their clients, subject to certain exceptions, and to exercise reasonable care to prevent their employees, associates and others whose services they utilize from disclosing such confidences and secrets.

[2] N.Y. State 709.

[3] DR 4-101(B)(3) of the New York Code provides that a lawyer may not "knowingly . . . [u]se a confidence or secret of a client for the advantage of the lawyer or of a third person, unless the client consents after full disclosure." It might be argued that, under the literal text of this provision, using such an e-mail provider would constitute improper "use" of a client's confidences or secrets for the benefit of a third party -- namely, the e-mail service provider that sells the advertising. We do not believe that the incidental "use" here, or the benefits derived therefrom, are within the contemplation of the rule anymore than the profits earned by other providers of services to lawyers, such as litigation support companies, which handle or are exposed to client confidences. See EC 4?3 (quoted below). We note as well that the advertisements go only to e-mail recipients who are themselves users of the e-mail service provider and presumably chose to receive the advertising. The use therefore also does not "disadvantage" clients within the meaning of DR 4-101(B)(2) by subjecting them to "junk mail" that the clients have not elected to receive.

[4] Cf. EC 4?3 ("Unless the client otherwise directs, it is not improper for a lawyer to give limited information to an outside agency necessary for statistical, bookkeeping, accounting, data processing, banking, printing, or other legitimate purposes, provided the lawyer exercises due care in the selection of the agency and warns the agency that the information must be kept confidential.").

Related Files

[use of e-mail service provider that scans e-mails for advertising purposes. \(http://old.nysba.org/Content/ContentFolders/EthicsOpinions/Opinions751825/EO_820.pdf\)](http://old.nysba.org/Content/ContentFolders/EthicsOpinions/Opinions751825/EO_820.pdf)(PDF File)

COMMUNITY RESOURCES

- [Hire a New York Attorney \(/lawyerreferral/\)](#)
- [Find a Mediator \(/DRSMediator/\)](#)
- [Family Healthcare Decisions Act Resource Center \(/FHCDA/\)](#)
- [Client's Rights and Responsibilities \(/CustomTemplates/SecondaryStandard.aspx?id=26544\)](#)
- [Free Legal Assistance \(http://www.lawhelp.org/ny/\)](#)
- [Judicial Election Information \(/CustomTemplates/SecondaryStandard.aspx?id=26540\)](#)
- [A Guide to Attorney Disciplinary Procedures in New York State \(/CustomTemplates/SecondaryStandard.aspx?id=26561\)](#)
- [When Mass Disaster Strikes \(/CustomTemplates/SecondaryStandard.aspx?id=26564\)](#)
- [Law, Youth and Citizenship Program](#)

NEWS CENTER

- [News Center \(/newscenter/\)](#)
- [News Releases \(/pressrelease.aspx\)](#)
- [Vital Statistics \(/CustomTemplates/SecondaryStandard.aspx?id=26982\)](#)
- [Legislative Priorities \(/CustomTemplates/SecondaryStandard.aspx?id=601\)](#)
- [State Bar Reports \(/CustomTemplates/SecondaryStandard.aspx?id=26785\)](#)
- [Press Kit \(/CustomTemplates/SecondaryStandard.aspx?id=26786\)](#)
- [Media Services and Public Affairs Department](#)
- [Contacts \(/CustomTemplates/SecondaryStandard.aspx?id=26787\)](#)

ABOUT NYSBA

- [Need password help? \(/pwhelp\)](#)
- [How Do I ... \(/howdoi/\)](#)
- [History and Structure of the Association \(/CustomTemplates/SecondaryStandard.aspx?id=27825\)](#)
- [Download Asset Report \(/DownloadAsset.aspx?id=65698\)](#)
- [Diversity and Inclusion \(/CustomTemplates/SecondaryStandard.aspx?id=27268\)](#)
- [Leadership Profiles \(/CustomTemplates/SecondaryStandard.aspx?id=27051\)](#)
- [Executive Committee Profiles \(/CustomTemplates/SecondaryStandard.aspx?id=27051\)](#)
- [Section Chair Profiles \(/CustomTemplates/SecondaryStandard.aspx?id=27052\)](#)
- [NYSBA Staff \(/CustomTemplates/SecondaryStandard.aspx?id=53139\)](#)

ONLINE STORE

- [NYSBA Online Marketplace \(/store\)](#)
- [Books and Form Products \(http://www.nysba.org/CustomTemplates/SecondaryStandard.aspx?id=34501\)](#)
- [Downloadable Forms \(/CustomTemplates/SecondaryStandard.aspx?id=1045\)](#)
- [Practice Forms \(/store/SearchResults.aspx?Category=DISK\)](#)
- [CLE On Demand - Audio and Video \(/CLEONLINE/\)](#)
- [CLE on CD \(/CLE_on_CD/\)](#)
- [CLE on DVD \(/CLE_on_DVD/\)](#)
- [CLE Coursebooks \(/CLE_Coursebooks/\)](#)
- [LegalEase Pamphlet Series \(/CustomTemplates/SecondaryStandard.aspx?id=27986\)](#)

CONNECT WITH NYSBA

-  <http://www.facebook.com/nysba>
-  <http://www.twitter.com/nysba>
-  <http://www.nysba.org/LinkedIn>
-  <http://instagram.com/nystatebar>
-  <http://www.youtube.com/nysba>
- [SITE MAP \(/SITEMAP.ASPX?ID=43\)](#)
- [COPYRIGHT \(/CUSTOMTEMPLATES/CONTENT.ASPX?ID=46\)](#)
- [PRIVACY POLICY \(/CUSTOMTEMPLATES/CONTENT.ASPX?ID=44\)](#)
- [TERMS OF USE \(/CUSTOMTEMPLATES/CONTENT.ASPX?ID=44\)](#)

<http://www.nysba.org/CustomTemplates/SectionLanding.aspx?id=27693>

[Mock Trial \(/NYSMockTrial/\)](#)

[Employment at NYSBA \(/employment/\)](#)

[Social Media Links \(/CustomTemplates/SecondaryStandard.aspx?id=54252\)](#)

[NYSBA Social Media Policy \(/socialmediapolicy/\)](#)

[NYSBA Awards and Competitions \(/awards/\)](#)

[Advertise with NYSBA \(http://www.nysba.org/CustomTemplates/SecondaryStandard.aspx?id=27727\)](#)

[Doing Business With NYSBA \(/CustomTemplates/SecondaryStandard.aspx?id=27826\)](#)

[Directions to the State Bar Center \(/map/\)](#)

[ID=45\)](#)

[CONTACT US \(/CONTACT/\)](#)

[HOW DO I... \(/HOWDOI/\)](#)



One Elk Street, Albany , NY 12207
Phone: 518-463-3200 Secure Fax: 518.463.5993

© 2016 New York State Bar Association

ETHICS OPINION 842

[CLE \(/CLE/CONTINUING LEGAL EDUCATION HOME/\)](#) | [EVENTS \(/STORE/CALENDAR/SCHEDULE.ASPX?EXCLUDEEVENTTYPE=X\)](#)

[SECTIONS & COMMITTEES \(/SECTIONSANDCOMMITTEES/\)](#) | [PUBLICATIONS \(/CUSTOMTEMPLATES/SECONDARYSTANDARD.ASPX?ID=43579\)](#)

[PRACTICE RESOURCES \(/PRACTICERESOURCES\)](#) | [LEADERSHIP & ADVOCACY \(/LEADERSHIPANDADVOCACY/\)](#) | [MEMBERSHIP \(/REVISEDMEMBERSHIPHOME/\)](#)

[MEMBERS ONLY \(/CUSTOMTEMPLATES/SECONDARYSTANDARD.ASPX?ID=27180\)](#)

[Home \(/\)](#) | [Ethics Opinion 842 \(/CustomTemplates/Content.aspx?id=1499\)](#)

 [\(/CustomTemplates/Content.aspx?id=1499&css=print\)](#) 
  Like 0

COMMITTEE ON PROFESSIONAL ETHICS

Opinion 842 (9/10/10)

Topic: Using an outside online storage provider to store client confidential information.

Digest: A lawyer may use an online data storage system to store and back up client confidential information provided that the lawyer takes reasonable care to ensure that confidentiality will be maintained in a manner consistent with the lawyer's obligations under Rule 1.6. In addition, the lawyer should stay abreast of technological advances to ensure that the storage system remains sufficiently advanced to protect the client's information, and should monitor the changing law of privilege to ensure that storing the information online will not cause loss or waiver of any privilege.

Rules: 1.4, 1.6(a), 1.6(c)

QUESTION

1. **MAY A LAWYER USE AN ONLINE SYSTEM TO STORE A CLIENT'S CONFIDENTIAL INFORMATION WITHOUT VIOLATING THE DUTY OF CONFIDENTIALITY OR ANY OTHER DUTY? IF SO, WHAT STEPS SHOULD THE LAWYER TAKE TO ENSURE THAT THE INFORMATION IS SUFFICIENTLY SECURE?**

OPINION

2. **VARIOUS COMPANIES OFFER ONLINE COMPUTER DATA STORAGE SYSTEMS THAT ARE MAINTAINED ON AN ARRAY OF INTERNET SERVERS LOCATED AROUND THE WORLD. (THE ARRAY OF INTERNET SERVERS THAT STORE THE DATA IS OFTEN CALLED THE "CLOUD.") A SOLO PRACTITIONER WOULD LIKE TO USE ONE OF THESE ONLINE "CLOUD" COMPUTER DATA STORAGE SYSTEMS TO STORE CLIENT CONFIDENTIAL INFORMATION. THE LAWYER'S AIM IS TO ENSURE THAT HIS CLIENTS' INFORMATION WILL NOT BE LOST IF SOMETHING HAPPENS TO THE LAWYER'S OWN COMPUTERS. THE ONLINE DATA STORAGE SYSTEM IS PASSWORD-PROTECTED AND THE DATA STORED IN THE ONLINE SYSTEM IS ENCRYPTED.**

3. **A DISCUSSION OF CONFIDENTIAL INFORMATION IMPLICATES RULE 1.6 OF THE NEW YORK RULES OF PROFESSIONAL CONDUCT (THE "RULES"), THE GENERAL RULE GOVERNING CONFIDENTIALITY. RULE 1.6(A) PROVIDES AS FOLLOWS:**

A LAWYER SHALL NOT KNOWINGLY REVEAL CONFIDENTIAL INFORMATION . . . OR USE SUCH INFORMATION TO THE DISADVANTAGE OF A CLIENT OR FOR THE ADVANTAGE OF A LAWYER OR A THIRD PERSON, UNLESS:

- (1) THE CLIENT GIVES INFORMED CONSENT, AS DEFINED IN RULE 1.0(J);**
- (2) THE DISCLOSURE IS IMPLIEDLY AUTHORIZED TO ADVANCE THE BEST INTERESTS OF THE CLIENT AND IS EITHER REASONABLE UNDER THE CIRCUMSTANCES OR CUSTOMARY IN THE PROFESSIONAL COMMUNITY; OR**
- (3) THE DISCLOSURE IS PERMITTED BY PARAGRAPH (B).**

4. THE OBLIGATION TO PRESERVE CLIENT CONFIDENTIAL INFORMATION EXTENDS BEYOND MERELY PROHIBITING AN ATTORNEY FROM REVEALING CONFIDENTIAL INFORMATION WITHOUT CLIENT CONSENT. A LAWYER MUST ALSO TAKE REASONABLE CARE TO AFFIRMATIVELY PROTECT A CLIENT'S CONFIDENTIAL INFORMATION. SEE N.Y. COUNTY 733 (2004) (AN ATTORNEY "MUST DILIGENTLY PRESERVE THE CLIENT'S CONFIDENCES, WHETHER REDUCED TO DIGITAL FORMAT, PAPER, OR OTHERWISE"). AS A NEW JERSEY ETHICS COMMITTEE OBSERVED, EVEN WHEN A LAWYER WANTS A CLOSED CLIENT FILE TO BE DESTROYED, "[S]IMPLY PLACING THE FILES IN THE TRASH WOULD NOT SUFFICE. APPROPRIATE STEPS MUST BE TAKEN TO ENSURE THAT CONFIDENTIAL AND PRIVILEGED INFORMATION REMAINS PROTECTED AND NOT AVAILABLE TO THIRD PARTIES." NEW JERSEY OPINION (2006), QUOTING NEW JERSEY OPINION 692 (2002).

5. IN ADDITION, RULE 1.6(C) PROVIDES THAT AN ATTORNEY MUST "EXERCISE REASONABLE CARE TO PREVENT . . . OTHERS WHOSE SERVICES ARE UTILIZED BY THE LAWYER FROM DISCLOSING OR USING CONFIDENTIAL INFORMATION OF A CLIENT" EXCEPT TO THE EXTENT DISCLOSURE IS PERMITTED BY RULE 1.6(B). ACCORDINGLY, A LAWYER MUST TAKE REASONABLE AFFIRMATIVE STEPS TO GUARD AGAINST THE RISK OF INADVERTENT DISCLOSURE BY OTHERS WHO ARE WORKING UNDER THE ATTORNEY'S SUPERVISION OR WHO HAVE BEEN RETAINED BY THE ATTORNEY TO ASSIST IN PROVIDING SERVICES TO THE CLIENT. WE NOTE, HOWEVER, THAT EXERCISING "REASONABLE CARE" UNDER RULE 1.6 DOES NOT MEAN THAT THE LAWYER GUARANTEES THAT THE INFORMATION IS SECURE FROM ANY UNAUTHORIZED ACCESS.

6. TO DATE, NO NEW YORK ETHICS OPINION HAS ADDRESSED THE ETHICS OF *STORING* CONFIDENTIAL INFORMATION ONLINE. HOWEVER, IN N.Y. STATE 709 (1998) THIS COMMITTEE ADDRESSED THE DUTY TO PRESERVE A CLIENT'S CONFIDENTIAL INFORMATION WHEN *TRANSMITTING* SUCH INFORMATION ELECTRONICALLY. OPINION 709 CONCLUDED THAT LAWYERS MAY TRANSMIT CONFIDENTIAL INFORMATION BY E-MAIL, BUT CAUTIONED THAT "LAWYERS MUST ALWAYS ACT REASONABLY IN CHOOSING TO USE E-MAIL FOR CONFIDENTIAL COMMUNICATIONS." THE COMMITTEE ALSO WARNED THAT THE EXERCISE OF REASONABLE CARE MAY DIFFER FROM ONE CASE TO THE NEXT. ACCORDINGLY, WHEN A LAWYER IS ON NOTICE THAT THE CONFIDENTIAL INFORMATION BEING TRANSMITTED IS "OF SUCH AN EXTRAORDINARILY SENSITIVE NATURE THAT IT IS REASONABLE TO USE ONLY A MEANS OF COMMUNICATION THAT IS COMPLETELY UNDER THE LAWYER'S CONTROL, THE LAWYER MUST SELECT A MORE SECURE MEANS OF COMMUNICATION THAN UNENCRYPTED INTERNET E-MAIL." SEE ALSO RULE 1.6, CMT. 17 (A LAWYER "MUST TAKE REASONABLE PRECAUTIONS" TO PREVENT INFORMATION COMING INTO THE HANDS OF UNINTENDED RECIPIENTS WHEN TRANSMITTING INFORMATION RELATING TO THE REPRESENTATION, BUT IS NOT REQUIRED TO USE SPECIAL SECURITY MEASURES IF THE MEANS OF COMMUNICATING PROVIDES A REASONABLE EXPECTATION OF PRIVACY).

7. ETHICS ADVISORY OPINIONS IN SEVERAL OTHER STATES HAVE APPROVED THE USE OF ELECTRONIC STORAGE OF CLIENT FILES PROVIDED THAT SUFFICIENT PRECAUTIONS ARE IN PLACE. SEE, E.G., NEW JERSEY OPINION 701 (2006) (LAWYER MAY USE ELECTRONIC FILING SYSTEM WHEREBY ALL DOCUMENTS ARE SCANNED INTO A DIGITIZED FORMAT AND ENTRUSTED TO SOMEONE OUTSIDE THE FIRM PROVIDED THAT THE LAWYER EXERCISES "REASONABLE CARE," WHICH INCLUDES ENTRUSTING DOCUMENTS TO A THIRD PARTY WITH AN ENFORCEABLE OBLIGATION TO PRESERVE CONFIDENTIALITY AND SECURITY, AND EMPLOYING AVAILABLE TECHNOLOGY TO GUARD AGAINST REASONABLY FORESEEABLE ATTEMPTS TO INFILTRATE DATA); ARIZONA OPINION 05-04 (2005) (ELECTRONIC STORAGE OF CLIENT FILES IS PERMISSIBLE PROVIDED LAWYERS AND LAW FIRMS "TAKE COMPETENT AND REASONABLE STEPS TO ASSURE THAT THE CLIENT'S CONFIDENCES ARE NOT DISCLOSED TO THIRD PARTIES THROUGH THEFT OR INADVERTENCE"); SEE ALSO ARIZONA OPINION 09-04 (2009) (LAWYER MAY PROVIDE CLIENTS WITH AN ONLINE FILE STORAGE AND RETRIEVAL SYSTEM THAT CLIENTS MAY ACCESS, PROVIDED LAWYER TAKES REASONABLE PRECAUTIONS TO PROTECT

SECURITY AND CONFIDENTIALITY AND LAWYER PERIODICALLY REVIEWS SECURITY MEASURES AS TECHNOLOGY ADVANCES OVER TIME TO ENSURE THAT THE CONFIDENTIALITY OF CLIENT INFORMATION REMAINS REASONABLY PROTECTED).

8. BECAUSE THE INQUIRING LAWYER WILL USE THE ONLINE DATA STORAGE SYSTEM FOR THE PURPOSE OF PRESERVING CLIENT INFORMATION - A PURPOSE BOTH RELATED TO THE RETENTION AND NECESSARY TO PROVIDING LEGAL SERVICES TO THE CLIENT - USING THE ONLINE SYSTEM IS CONSISTENT WITH CONDUCT THAT THIS COMMITTEE HAS DEEMED ETHICALLY PERMISSIBLE. SEE N.Y. STATE 473 (1977) (ABSENT CLIENT'S OBJECTION, LAWYER MAY PROVIDE CONFIDENTIAL INFORMATION TO OUTSIDE SERVICE AGENCY FOR LEGITIMATE PURPOSES RELATING TO THE REPRESENTATION PROVIDED THAT THE LAWYER EXERCISES CARE IN THE SELECTION OF THE AGENCY AND CAUTIONS THE AGENCY TO KEEP THE INFORMATION CONFIDENTIAL); CF. NY CPLR 4548 (PRIVILEGED COMMUNICATION DOES NOT LOSE ITS PRIVILEGED CHARACTER SOLELY BECAUSE IT IS COMMUNICATED BY ELECTRONIC MEANS OR BECAUSE "PERSONS NECESSARY FOR THE DELIVERY OR FACILITATION OF SUCH ELECTRONIC COMMUNICATION MAY HAVE ACCESS TO" ITS CONTENTS).

9. WE CONCLUDE THAT A LAWYER MAY USE AN ONLINE "CLOUD" COMPUTER DATA BACKUP SYSTEM TO STORE CLIENT FILES PROVIDED THAT THE LAWYER TAKES REASONABLE CARE TO ENSURE THAT THE SYSTEM IS SECURE AND THAT CLIENT CONFIDENTIALITY WILL BE MAINTAINED. "REASONABLE CARE" TO PROTECT A CLIENT'S CONFIDENTIAL INFORMATION AGAINST UNAUTHORIZED DISCLOSURE MAY INCLUDE CONSIDERATION OF THE FOLLOWING STEPS:

- (1) ENSURING THAT THE ONLINE DATA STORAGE PROVIDER HAS AN ENFORCEABLE OBLIGATION TO PRESERVE CONFIDENTIALITY AND SECURITY, AND THAT THE PROVIDER WILL NOTIFY THE LAWYER IF SERVED WITH PROCESS REQUIRING THE PRODUCTION OF CLIENT INFORMATION;**
- (2) INVESTIGATING THE ONLINE DATA STORAGE PROVIDER'S SECURITY MEASURES, POLICIES, RECOVERABILITY METHODS, AND OTHER PROCEDURES TO DETERMINE IF THEY ARE ADEQUATE UNDER THE CIRCUMSTANCES;**
- (3) EMPLOYING AVAILABLE TECHNOLOGY TO GUARD AGAINST REASONABLY FORESEEABLE ATTEMPTS TO INFILTRATE THE DATA THAT IS STORED; AND/OR**
- (4) INVESTIGATING THE STORAGE PROVIDER'S ABILITY TO PURGE AND WIPE ANY COPIES OF THE DATA, AND TO MOVE THE DATA TO A DIFFERENT HOST, IF THE LAWYER BECOMES DISSATISFIED WITH THE STORAGE PROVIDER OR FOR OTHER REASONS CHANGES STORAGE PROVIDERS.**

10. TECHNOLOGY AND THE SECURITY OF STORED DATA ARE CHANGING RAPIDLY. EVEN AFTER TAKING SOME OR ALL OF THESE STEPS (OR SIMILAR STEPS), THEREFORE, THE LAWYER SHOULD PERIODICALLY RECONFIRM THAT THE PROVIDER'S SECURITY MEASURES REMAIN EFFECTIVE IN LIGHT OF ADVANCES IN TECHNOLOGY. IF THE LAWYER LEARNS INFORMATION SUGGESTING THAT THE SECURITY MEASURES USED BY THE ONLINE DATA STORAGE PROVIDER ARE INSUFFICIENT TO ADEQUATELY PROTECT THE CONFIDENTIALITY OF CLIENT INFORMATION, OR IF THE LAWYER LEARNS OF ANY BREACH OF CONFIDENTIALITY BY THE ONLINE STORAGE PROVIDER, THEN THE LAWYER MUST INVESTIGATE WHETHER THERE HAS BEEN ANY BREACH OF HIS OR HER OWN CLIENTS' CONFIDENTIAL INFORMATION, NOTIFY ANY AFFECTED CLIENTS, AND DISCONTINUE USE OF THE SERVICE UNLESS THE LAWYER RECEIVES ASSURANCES THAT ANY SECURITY ISSUES HAVE BEEN SUFFICIENTLY REMEDIATED. SEE RULE 1.4 (MANDATING COMMUNICATION WITH CLIENTS); SEE ALSO N.Y. STATE 820 (2008) (ADDRESSING WEB-BASED EMAIL SERVICES).

11. NOT ONLY TECHNOLOGY ITSELF BUT ALSO THE LAW RELATING TO TECHNOLOGY AND THE PROTECTION OF CONFIDENTIAL COMMUNICATIONS IS CHANGING RAPIDLY. LAWYERS USING ONLINE STORAGE SYSTEMS (AND ELECTRONIC MEANS OF COMMUNICATION GENERALLY) SHOULD MONITOR THESE LEGAL DEVELOPMENTS, ESPECIALLY REGARDING INSTANCES WHEN USING TECHNOLOGY MAY WAIVE AN OTHERWISE APPLICABLE PRIVILEGE. SEE, E.G., CITY OF ONTARIO, CALIF. V. QUON, 130 S. CT. 2619, 177 L.ED.2D 216 (2010) (HOLDING THAT CITY DID NOT VIOLATE FOURTH AMENDMENT WHEN IT REVIEWED TRANSCRIPTS OF MESSAGES SENT AND RECEIVED BY POLICE OFFICERS ON POLICE

DEPARTMENT PAGERS); *SCOTT V. BETH ISRAEL MEDICAL CENTER*, 17 MISC. 3D 934, 847 N.Y.S.2D 436 (N.Y. SUP. 2007) (E-MAILS BETWEEN HOSPITAL EMPLOYEE AND HIS PERSONAL ATTORNEYS WERE NOT PRIVILEGED BECAUSE EMPLOYER'S POLICY REGARDING COMPUTER USE AND E-MAIL MONITORING STATED THAT EMPLOYEES HAD NO REASONABLE EXPECTATION OF PRIVACY IN E-MAILS SENT OVER THE EMPLOYER'S E-MAIL SERVER). *BUT SEE STENGART V. LOVING CARE AGENCY, INC.*, 201 N.J. 300, 990 A.2D 650 (2010) (DESPITE EMPLOYER'S E-MAIL POLICY STATING THAT COMPANY HAD RIGHT TO REVIEW AND DISCLOSE ALL INFORMATION ON "THE COMPANY'S MEDIA SYSTEMS AND SERVICES" AND THAT E-MAILS WERE "NOT TO BE CONSIDERED PRIVATE OR PERSONAL" TO ANY EMPLOYEES, COMPANY VIOLATED EMPLOYEE'S ATTORNEY-CLIENT PRIVILEGE BY REVIEWING E-MAILS SENT TO EMPLOYEE'S PERSONAL ATTORNEY ON EMPLOYER'S LAPTOP THROUGH EMPLOYEE'S PERSONAL, PASSWORD-PROTECTED E-MAIL ACCOUNT).

12. THIS COMMITTEE'S PRIOR OPINIONS HAVE ADDRESSED THE DISCLOSURE OF CONFIDENTIAL INFORMATION IN METADATA AND THE PERILS OF PRACTICING LAW OVER THE INTERNET. WE HAVE NOTED IN THOSE OPINIONS THAT THE DUTY TO "EXERCISE REASONABLE CARE" TO PREVENT DISCLOSURE OF CONFIDENTIAL INFORMATION "MAY, IN SOME CIRCUMSTANCES, CALL FOR THE LAWYER TO STAY ABREAST OF TECHNOLOGICAL ADVANCES AND THE POTENTIAL RISKS" IN TRANSMITTING INFORMATION ELECTRONICALLY. N.Y. STATE 782 (2004), *CITING* N.Y. STATE 709 (1998) (WHEN CONDUCTING TRADEMARK PRACTICE OVER THE INTERNET, LAWYER HAD DUTY TO "STAY ABREAST OF THIS EVOLVING TECHNOLOGY TO ASSESS ANY CHANGES IN THE LIKELIHOOD OF INTERCEPTION AS WELL AS THE AVAILABILITY OF IMPROVED TECHNOLOGIES THAT MAY REDUCE SUCH RISKS AT REASONABLE COST"); *SEE ALSO* N.Y. STATE 820 (2008) (SAME IN CONTEXT OF USING E-MAIL SERVICE PROVIDER THAT SCANS E-MAILS TO GENERATE COMPUTER ADVERTISING). THE SAME DUTY TO STAY CURRENT WITH THE TECHNOLOGICAL ADVANCES APPLIES TO A LAWYER'S CONTEMPLATED USE OF AN ONLINE DATA STORAGE SYSTEM.

CONCLUSION

13. A LAWYER MAY USE AN ONLINE DATA STORAGE SYSTEM TO STORE AND BACK UP CLIENT CONFIDENTIAL INFORMATION PROVIDED THAT THE LAWYER TAKES REASONABLE CARE TO ENSURE THAT CONFIDENTIALITY IS MAINTAINED IN A MANNER CONSISTENT WITH THE LAWYER'S OBLIGATIONS UNDER RULE 1.6. A LAWYER USING AN ONLINE STORAGE PROVIDER SHOULD TAKE REASONABLE CARE TO PROTECT CONFIDENTIAL INFORMATION, AND SHOULD EXERCISE REASONABLE CARE TO PREVENT OTHERS WHOSE SERVICES ARE UTILIZED BY THE LAWYER FROM DISCLOSING OR USING CONFIDENTIAL INFORMATION OF A CLIENT. IN ADDITION, THE LAWYER SHOULD STAY ABREAST OF TECHNOLOGICAL ADVANCES TO ENSURE THAT THE STORAGE SYSTEM REMAINS SUFFICIENTLY ADVANCED TO PROTECT THE CLIENT'S INFORMATION, AND THE LAWYER SHOULD MONITOR THE CHANGING LAW OF PRIVILEGE TO ENSURE THAT STORING INFORMATION IN THE "CLOUD" WILL NOT WAIVE OR JEOPARDIZE ANY PRIVILEGE PROTECTING THE INFORMATION.

(75-09)

COMMUNITY RESOURCES

[Hire a New York Attorney \(/lawyerreferral/\)](#)
[Find a Mediator \(/DRSMediator/\)](#)
[Family Healthcare Decisions Act Resource Center \(/FHCDCA/\)](#)
[Client Rights and Responsibilities \(/CustomTemplates/SecondaryStandard.aspx?id=26544\)](#)
[Free Legal Assistance \(http://www.lawhelp.org/ny/\)](#)
[Judicial Election Information \(/CustomTemplates/SecondaryStandard.aspx?id=26540\)](#)

NEWS CENTER

[News Center \(/newscenter/\)](#)
[News Releases \(/pressrelease.aspx\)](#)
[Advertising with NYSBA \(/CustomTemplates/SecondaryStandard.aspx?id=27727\)](#)
[Vital Statistics \(/CustomTemplates/SecondaryStandard.aspx?id=26982\)](#)
[Legislative Priorities \(/CustomTemplates/SecondaryStandard.aspx?id=601\)](#)
[State Bar Reports \(/CustomTemplates/SecondaryStandard.aspx?id=2785x?\)](#)
[Press Kit](#)

ABOUT NYSBA

[Need password help? \(/pwhelp\)](#)
[How Do I... \(/howdoi/\)](#)
[History and Structure of the Association? \(/CustomTemplates/SecondaryStandard.aspx?id=27825\)](#)
[Annual Report to Membership 2014-2015 \(/DownloadAsset.aspx?id=57117\)](#)
[Bylaws \(/Bylaws\)](#)
[Leadership Profiles \(/CustomTemplates/SecondaryStandard.aspx?id=27268\)](#)
[Executive Committee](#)

ONLINE STORE

[NYSBA Online Marketplace \(/store\)](#)
[Books and Form Products \(http://www.nysba.org/CustomTemplates/SecondaryStandard.aspx?id=34501\)](#)
[Downloadable Forms \(/CustomTemplates/SecondaryStandard.aspx?id=1045\)](#)
[Practice Forms \(/store/SearchResults.aspx?Category=DISK\)](#)
[CLE On Demand - Audio and Video \(/CLEONLINE/\)](#)
[CLE on CD \(/CLE on CD/\)](#)
[CLE on DVD \(/CLE on DVD/\)](#)

CONNECT WITH NYSBA

 <http://www.facebook.com/nysba>
 <http://www.twitter.com/nysba>
 <http://www.nysba.org/LinkedIn>
 <http://instagram.com/nystatebar>
 <http://www.youtube.com/nysba>
[SITE MAP \(/SITEMAP.ASPX?ID=43\)](#)

[Resolving Conflict with a](#) ([/CustomTemplates/SecondaryStandard.aspx?id=26916](#))

[New York Attorney](#) ([/CustomTemplates/SecondaryStandard.aspx?id=26561](#))

[When Mass Disaster Strikes](#)

[Law, Youth and Citizenship Program](#) ([http://www.nysba.org/CustomTemplates/SectionLanding.aspx?id=27693](#))

[Mock Trial \(/NYSMockTrial/\)](#)

[Profiles](#) ([/CustomTemplates/SecondaryStandard.aspx?id=27051](#))

[Media Services and Public Affairs Department](#) ([/CustomTemplates/SecondaryStandard.aspx?id=26961](#))

[NYSBA Staff](#) ([/CustomTemplates/SecondaryStandard.aspx?id=53139](#))

[Employment at NYSBA](#) ([/employment/](#))

[Social Media Links](#) ([/CustomTemplates/SecondaryStandard.aspx?id=54252](#))

[NYSBA Social Media Policy](#) ([/socialmediapolicy/](#))

[NYSBA Awards and Competitions \(/awards/\)](#)

[Doing Business With NYSBA](#) ([/CustomTemplates/SecondaryStandard.aspx?id=27826](#))

[Directions to the Bar Center](#) ([/map/](#))

[CLE Coursebooks](#)

[CLE Coursebooks \(/CLECoursebooks/\)](#)

[LegalEase Pamphlet Series](#)

[Profiles of NYSBA Section Chairs](#) ([/CustomTemplates/SecondaryStandard.aspx?id=27986](#))

[NYSBA Staff](#) ([/CustomTemplates/SecondaryStandard.aspx?id=53139](#))

[Employment at NYSBA](#) ([/employment/](#))

[Social Media Links](#) ([/CustomTemplates/SecondaryStandard.aspx?id=54252](#))

[NYSBA Social Media Policy](#) ([/socialmediapolicy/](#))

[NYSBA Awards and Competitions \(/awards/\)](#)

[Doing Business With NYSBA](#) ([/CustomTemplates/SecondaryStandard.aspx?id=27826](#))

[Directions to the Bar Center](#) ([/map/](#))

[COPYRIGHT](#)

[/CUSTOMTEMPLATES/CONTENT.ASPX?ID=46](#)

[PRIVACY POLICY](#)

[/CUSTOMTEMPLATES/CONTENT.ASPX?ID=44](#)

[TERMS OF USE](#)

[/CUSTOMTEMPLATES/CONTENT.ASPX?ID=45](#)

[CONTACT US \(/CONTACT/\)](#)

[HOW DO I ... \(/HOWDOI/\)](#)



One Elk Street, Albany , NY 12207
Phone: 518-463-3200 Secure Fax: 518.463.5993

© 2015 New York State Bar Association



Ransomware

Ransomware is a form of malware that targets both human and technical weaknesses in organizations in an effort to deny the availability of critical data and/or systems. When the victim organization determines they are no longer able to access their data, the cyber actor demands the payment of a ransom, at which time the actor purportedly provides an avenue to the victim to regain access to their data. Recent iterations target enterprise end users, making awareness and training a critical preventative measure.

Infection Vectors

Ransomware is frequently delivered through phishing e-mails to end users. Early ransomware e-mails were often generic in nature, but more recent e-mails are highly targeted to both the organization and individual, making scrutiny of the document and sender important to prevent exploitation. An e-mail compromise occurs in one of two ways:

1. Receipt of an e-mail containing malicious attachments, including: .pdf, .doc, .xls, and .exe file extensions. These attachments are described as something that appears legitimate, such as an invoice or electronic fax, but contain malicious code.
2. Receipt of an e-mail that appears legitimate but contains a link to a website hosting an exploit kit.

When the user opens the malicious file or link in the phishing e-mail, the most frequent end result is the rapid encryption of files and folders containing business-critical information and data. Recent ransomware campaigns have employed robust encryption that prevents most attempts to break the encryption and recover the data.

Another infection method involves adversaries hacking a known website to plant the malware. End users are infected when visiting the compromised website while using outdated browsers, browser plugins, and other software.

After infection, the malware usually calls home to command and control (C2) infrastructure to obtain encryption keys from the adversary. Once keys are obtained, the malware begins rapidly encrypting files and folders on local drives, attached drives, and network shares to which the infected user has access. Organizations are generally not aware that they have been infected until users are no longer able to access data or begin to see messages advising them of the attack and demanding a ransom payment.

While the FBI normally recommends organizations invest in measures to prevent, detect, and remediate cyber exploitation, the key areas to focus on with ransomware are prevention, business continuity, and remediation. It is very difficult to detect a successful ransomware compromise before it is too late. The best approach is to focus on defense in depth, or several layers of security, as there is no single method to prevent a compromise. As ransomware techniques and malware continue to evolve and become more sophisticated, even with the most robust prevention controls in place, there is no guarantee against exploitation. This fact makes contingency and remediation planning crucial to business recovery and continuity, and those plans should be tested regularly to ensure the integrity of sensitive data in the event of a compromise.

CyberDIVISION
FEDERAL BUREAU OF INVESTIGATION

Prevention Considerations

- Focus on awareness and training. Since end users are targeted, employees should be made aware of the threat of ransomware, how it is delivered, and trained on information security principles and techniques.
- Patch the operating system, software, and firmware on devices. All endpoints should be patched as vulnerabilities are discovered. This can be made easier through a centralized patch management system.
- Ensure anti-virus and anti-malware solutions are set to automatically update and regular scans are conducted.
- Manage the use of privileged accounts. Implement the principle of least privilege. No users should be assigned administrative access unless absolutely needed. Those with a need for administrator accounts should only use them when necessary; and they should operate with standard user accounts at all other times.
- Implement least privilege for file, directory, and network share permissions. If a user only needs to read specific files, they should not have write access to those files, directories, or shares. Configure access controls with least privilege in mind.
- Disable macro scripts from office files transmitted via e-mail. Consider using Office Viewer software to open Microsoft Office files transmitted via e-mail instead of full office suite applications.
- Implement software restriction policies (SRP) or other controls to prevent the execution of programs in common ransomware locations, such as temporary folders supporting popular Internet browsers, or compression/decompression programs, including those located in the AppData/LocalAppData folder.

Business Continuity Considerations

- Regularly back up data and verify its integrity.
- Secure your backups. Ensure backups are not connected to the computers and networks they are backing up. Examples might be securing backups in the cloud or physically storing them offline. Some instances of ransomware have the capability to lock cloud-based backups when systems continuously back up in real-time, also known as persistent synchronization. Backups are critical in ransomware; if you are infected, backups may be the best way to recover your critical data.

Other Considerations

Some other considerations that can be highly dependent on organizational budget and system configuration include:

- Implement application whitelisting. Only allow systems to execute programs known and permitted by security policy.
- Use virtualized environments to execute operating system environments or specific programs.
- Categorize data based on organizational value, and implement physical/logical separation of networks and data for different organization units. For example, sensitive research or business data should not reside on the same server and/or network segment as an organization's e-mail environment.
- Require user interaction for end user applications communicating with websites uncategorized by the network proxy or firewall. Examples include requiring users to type information or enter a password when their system communicates with a website uncategorized by the proxy or firewall.

The Ransom

The FBI does not advocate paying a ransom to an adversary. Paying a ransom does not guarantee an organization will regain access to their data. In fact, some individuals or organizations were never provided with decryption keys after paying a ransom. Paying a ransom emboldens the adversary to target other organizations for profit and provides a lucrative environment for other criminals to become involved. Finally, by paying a ransom, an organization is funding illicit activity associated with criminal groups, including potential terrorist groups, who likely will continue to target an organization. While the FBI does not advocate paying a ransom, there is an understanding that when businesses are faced with an inability to function, executives will evaluate all options to protect their shareholders, employees, and customers.

In all cases, the FBI encourages organizations to contact their local FBI Cyber Task Force immediately to report a ransomware event and request assistance. The FBI works with federal, state, local, and international partners to pursue cyber actors globally and assist victims of cyber crime. Victims are also encouraged to report cyber incidents to the FBI's Internet Crime Complaint Center (www.ic3.gov).

KEY DATA-SECURITY TAKEAWAYS

Five Easy Steps to Better Data Security

1. Use full disk encryption for all computers
2. Encrypt files on portable storage devices
3. Use two-factor authentication
4. Never send passwords by the same media as password-protected files
5. Investigate VPN technologies and secure file transfer

Single Best Way to Promote Data Security

Do not transmit or receive confidential or private information you do not really need

AMERICAN BAR ASSOCIATION

STANDING COMMITTEE ON ETHICS AND PROFESSIONAL RESPONSIBILITY

Formal Opinion 483

October 17, 2018

Lawyers' Obligations After an Electronic Data Breach or Cyberattack

Model Rule 1.4 requires lawyers to keep clients “reasonably informed” about the status of a matter and to explain matters “to the extent reasonably necessary to permit a client to make an informed decision regarding the representation.” Model Rules 1.1, 1.6, 5.1 and 5.3, as amended in 2012, address the risks that accompany the benefits of the use of technology by lawyers. When a data breach occurs involving, or having a substantial likelihood of involving, material client information, lawyers have a duty to notify clients of the breach and to take other reasonable steps consistent with their obligations under these Model Rules.

Introduction¹

Data breaches and cyber threats involving or targeting lawyers and law firms are a major professional responsibility and liability threat facing the legal profession. As custodians of highly sensitive information, law firms are inviting targets for hackers.² In one highly publicized incident, hackers infiltrated the computer networks at some of the country’s most well-known law firms, likely looking for confidential information to exploit through insider trading schemes.³ Indeed, the data security threat is so high that law enforcement officials regularly divide business entities into two categories: those that have been hacked and those that will be.⁴

In Formal Opinion 477R, this Committee explained a lawyer’s ethical responsibility to use reasonable efforts when communicating client confidential information using the Internet.⁵ This

¹ This opinion is based on the ABA Model Rules of Professional Conduct as amended by the ABA House of Delegates through August 2018. The laws, court rules, regulations, rules of professional conduct and opinions promulgated in individual jurisdictions are controlling.

² See, e.g., Dan Steiner, *Hackers Are Aggressively Targeting Law Firms’ Data* (Aug. 3, 2017), <https://www.cio.com> (explaining that “[f]rom patent disputes to employment contracts, law firms have a lot of exposure to sensitive information. Because of their involvement, confidential information is stored on the enterprise systems that law firms use. . . . This makes them a juicy target for hackers that want to steal consumer information and corporate intelligence.”); See also *Criminal-Seeking-Hacker’ Requests Network Breach for Insider Trading*, Private Industry Notification 160304-01, FBI, CYBER DIVISION (Mar. 4, 2016).

³ Nicole Hong & Robin Sidel, *Hackers Breach Law Firms, Including Cravath and Weil Gotshal*, WALL ST. J. (Mar. 29, 2016), <https://www.wsj.com/articles/hackers-breach-cravath-swaine-other-big-law-firms-1459293504>.

⁴ Robert S. Mueller, III, *Combatting Threats in the Cyber World Outsmarting Terrorists, Hackers and Spies*, FBI (Mar. 1, 2012), <https://archives.fbi.gov/archives/news/speeches/combating-threats-in-the-cyber-world-outsmarting-terrorists-hackers-and-spies>.

⁵ ABA Comm. on Ethics & Prof’l Responsibility, Formal Op. 477R (2017) (“Securing Communication of Protected Client Information”).

opinion picks up where Opinion 477R left off, and discusses an attorney's ethical obligations when a data breach exposes client confidential information. This opinion focuses on an attorney's ethical obligations after a data breach,⁶ and it addresses only data breaches that involve information relating to the representation of a client. It does not address other laws that may impose post-breach obligations, such as privacy laws or other statutory schemes that law firm data breaches might also implicate. Each statutory scheme may have different post-breach obligations, including different notice triggers and different response obligations. Both the triggers and obligations in those statutory schemes may overlap with the ethical obligations discussed in this opinion. And, as a matter of best practices, attorneys who have experienced a data breach should review all potentially applicable legal response obligations. However, compliance with statutes such as state breach notification laws, HIPAA, or the Gramm-Leach-Bliley Act does not necessarily achieve compliance with ethics obligations. Nor does compliance with lawyer regulatory rules *per se* represent compliance with breach response laws. As a matter of best practices, lawyers who have suffered a data breach should analyze compliance separately under every applicable law or rule.

Compliance with the obligations imposed by the Model Rules of Professional Conduct, as set forth in this opinion, depends on the nature of the cyber incident, the ability of the attorney to know about the facts and circumstances surrounding the cyber incident, and the attorney's roles, level of authority, and responsibility in the law firm's operations.⁷

⁶ The Committee recognizes that lawyers provide legal services to clients under a myriad of organizational structures and circumstances. The Model Rules of Professional Conduct refer to the various structures as a "firm." A "firm" is defined in Rule 1.0(c) as "a lawyer or lawyers in a law partnership, professional corporation, sole proprietorship or other association authorized to practice law; or lawyers employed in a legal services organization or the legal department of a corporation or other organization." How a lawyer complies with the obligations discussed in this opinion will vary depending on the size and structure of the firm in which a lawyer is providing client representation and the lawyer's position in the firm. *See* MODEL RULES OF PROF'L CONDUCT R. 5.1 (2018) (Responsibilities of Partners, Managers, and Supervisory Lawyers); MODEL RULES OF PROF'L CONDUCT R. 5.2 (2018) (Responsibility of a Subordinate Lawyers); and MODEL RULES OF PROF'L CONDUCT R. 5.3 (2018) (Responsibility Regarding Nonlawyer Assistance).

⁷ In analyzing how to implement the professional responsibility obligations set forth in this opinion, lawyers may wish to consider obtaining technical advice from cyber experts. ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 477R (2017) ("Any lack of individual competence by a lawyer to evaluate and employ safeguards to protect client confidences may be addressed through association with another lawyer or expert, or by education.") *See also, e.g., Cybersecurity Resources*, ABA Task Force on Cybersecurity, <https://www.americanbar.org/groups/cybersecurity/resources.html> (last visited Oct. 5, 2018).

I. Analysis

A. Duty of Competence

Model Rule 1.1 requires that “A lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation.”⁸ The scope of this requirement was clarified in 2012, when the ABA recognized the increasing impact of technology on the practice of law and the obligation of lawyers to develop an understanding of that technology. Comment [8] to Rule 1.1 was modified in 2012 to read:

To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, *including the benefits and risks associated with relevant technology*, engage in continuing study and education and comply with all continuing legal education requirements to which the lawyer is subject. (Emphasis added.)⁹

In recommending the change to Rule 1.1’s Comment, the ABA Commission on Ethics 20/20 explained:

Model Rule 1.1 requires a lawyer to provide competent representation, and Comment [6] [renumbered as Comment [8]] specifies that, to remain competent, lawyers need to ‘keep abreast of changes in the law and its practice.’ The Commission concluded that, in order to keep abreast of changes in law practice in a digital age, lawyers necessarily need to understand basic features of relevant technology and that this aspect of competence should be expressed in the Comment. For example, a lawyer would have difficulty providing competent legal services in today’s environment without knowing how to use email or create an electronic document.¹⁰

⁸ MODEL RULES OF PROF’L CONDUCT R. 1.1 (2018).

⁹ A LEGISLATIVE HISTORY: THE DEVELOPMENT OF THE ABA MODEL RULES OF PROFESSIONAL CONDUCT, 1982-2013, at 43 (Art Garwin ed., 2013).

¹⁰ ABA COMMISSION ON ETHICS 20/20 REPORT 105A (Aug. 2012), http://www.americanbar.org/content/dam/aba/administrative/ethics_2020/20120808_revised_resolution_105a_as_a_mended_authcheckdam.pdf. The 20/20 Commission also noted that modification of Comment [6] did not change the lawyer’s substantive duty of competence: “Comment [6] already encompasses an obligation to remain aware of changes in technology that affect law practice, but the Commission concluded that making this explicit, by addition of the phrase ‘including the benefits and risks associated with relevant technology,’ would offer greater clarity in this area and emphasize the importance of technology to modern law practice. The proposed amendment, which appears in a Comment, does not impose any new obligations on lawyers. Rather, the amendment is intended to serve as a reminder to lawyers that they should remain aware of technology, including the benefits and risks associated with it, as part of a lawyer’s general ethical duty to remain competent.”

In the context of a lawyer's post-breach responsibilities, both Comment [8] to Rule 1.1 and the 20/20 Commission's thinking behind it require lawyers to understand technologies that are being used to deliver legal services to their clients. Once those technologies are understood, a competent lawyer must use and maintain those technologies in a manner that will reasonably safeguard property and information that has been entrusted to the lawyer. A lawyer's competency in this regard may be satisfied either through the lawyer's own study and investigation or by employing or retaining qualified lawyer and nonlawyer assistants.¹¹

1. Obligation to Monitor for a Data Breach

Not every cyber episode experienced by a lawyer is a data breach that triggers the obligations described in this opinion. A data breach for the purposes of this opinion means a data event where material client confidential information is misappropriated, destroyed or otherwise compromised, or where a lawyer's ability to perform the legal services for which the lawyer is hired is significantly impaired by the episode.

Many cyber events occur daily in lawyers' offices, but they are not a data breach because they do not result in actual compromise of material client confidential information. Other episodes rise to the level of a data breach, either through exfiltration/theft of client confidential information or through ransomware, where no client information is actually accessed or lost, but where the information is blocked and rendered inaccessible until a ransom is paid. Still other compromises involve an attack on a lawyer's systems, destroying the lawyer's infrastructure on which confidential information resides and incapacitating the attorney's ability to use that infrastructure to perform legal services.

Model Rules 5.1 and 5.3 impose upon lawyers the obligation to ensure that the firm has in effect measures giving reasonable assurance that all lawyers and staff in the firm conform to the Rules of Professional Conduct. Model Rule 5.1 Comment [2], and Model Rule 5.3 Comment [1] state that lawyers with managerial authority within a firm must make reasonable efforts to establish

¹¹ MODEL RULES OF PROF'L CONDUCT R. 5.3 (2018); ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 477R (2017); ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 08-451 (2018); *See also* JILL D. RHODES & ROBERT S. LITT, THE ABA CYBERSECURITY HANDBOOK: A RESOURCE FOR ATTORNEYS, LAW FIRMS, AND BUSINESS PROFESSIONALS 124 (2d ed. 2018) [hereinafter ABA CYBERSECURITY HANDBOOK].

internal policies and procedures designed to provide reasonable assurance that all lawyers and staff in the firm will conform to the Rules of Professional Conduct. Model Rule 5.1 Comment [2] further states that “such policies and procedures include those designed to detect and resolve conflicts of interest, identify dates by which actions must be taken in pending matters, account for client funds and property and ensure that inexperienced lawyers are properly supervised.”

Applying this reasoning, and based on lawyers’ obligations (i) to use technology competently to safeguard confidential information against unauthorized access or loss, and (ii) to supervise lawyers and staff, the Committee concludes that lawyers must employ reasonable efforts to monitor the technology and office resources connected to the internet, external data sources, and external vendors providing services relating to data¹² and the use of data. Without such a requirement, a lawyer’s recognition of any data breach could be relegated to happenstance --- and the lawyer might not identify whether a breach has occurred,¹³ whether further action is warranted,¹⁴ whether employees are adhering to the law firm’s cybersecurity policies and procedures so that the lawyers and the firm are in compliance with their ethical duties,¹⁵ and how and when the lawyer must take further action under other regulatory and legal provisions.¹⁶ Thus, just as lawyers must safeguard and monitor the security of paper files and actual client property, lawyers utilizing technology have the same obligation to safeguard and monitor the security of electronically stored client property and information.¹⁷

While lawyers must make reasonable efforts to monitor their technology resources to detect a breach, an ethical violation does not necessarily occur if a cyber-intrusion or loss of electronic information is not immediately detected, because cyber criminals might successfully hide their

¹² ABA Comm. on Ethics & Prof’l Responsibility, Formal Op. 08-451 (2008).

¹³ Fredric Greene, *Cybersecurity Detective Controls—Monitoring to Identify and Respond to Threats*, ISACA J., Vol. 5, 1025 (2015), available at <https://www.isaca.org/Journal/archives/2015/Volume-5/Pages/cybersecurity-detective-controls.aspx> (noting that “[d]etective controls are a key component of a cybersecurity program in providing visibility into malicious activity, breaches and attacks on an organization’s IT environment.”).

¹⁴ MODEL RULES OF PROF’L CONDUCT R. 1.6(c) (2018); MODEL RULES OF PROF’L CONDUCT R. 1.15 (2018).

¹⁵ See also MODEL RULES OF PROF’L CONDUCT R. 5.1 & 5.3 (2018).

¹⁶ The importance of monitoring to successful cybersecurity efforts is so critical that in 2015, Congress passed the Cybersecurity Information Sharing Act of 2015 (CISA) to authorize companies to monitor and implement defensive measures on their information systems, and to foreclose liability for such monitoring under CISA. AUTOMATED INDICATOR SHARING, <https://www.us-cert.gov/ais> (last visited Oct. 5, 2018); See also National Cyber Security Centre “Ten Steps to Cyber Security” [Step 8: Monitoring] (Aug. 9, 2016), <https://www.ncsc.gov.uk/guidance/10-steps-cyber-security>.

¹⁷ ABA Comm. on Ethics & Prof’l Responsibility, Formal Op. 477R (2017).

intrusion despite reasonable or even extraordinary efforts by the lawyer. Thus, as is more fully explained below, the potential for an ethical violation occurs when a lawyer does not undertake reasonable efforts to avoid data loss or to detect cyber-intrusion, and that lack of reasonable effort is the cause of the breach.

2. Stopping the Breach and Restoring Systems

When a breach of protected client information is either suspected or detected, Rule 1.1 requires that the lawyer act reasonably and promptly to stop the breach and mitigate damage resulting from the breach. How a lawyer does so in any particular circumstance is beyond the scope of this opinion. As a matter of preparation and best practices, however, lawyers should consider proactively developing an incident response plan with specific plans and procedures for responding to a data breach.¹⁸ The decision whether to adopt a plan, the content of any plan, and actions taken to train and prepare for implementation of the plan, should be made before a lawyer is swept up in an actual breach. “One of the benefits of having an incident response capability is that it supports responding to incidents systematically (i.e., following a consistent incident handling methodology) so that the appropriate actions are taken. Incident response plans help personnel to minimize loss or theft of information and disruption of services caused by incidents.”¹⁹ While every lawyer’s response plan should be tailored to the lawyer’s or the law firm’s specific practice, as a general matter incident response plans share common features:

The primary goal of any incident response plan is to have a process in place that will allow the firm to promptly respond in a coordinated manner to any type of security incident or cyber intrusion. The incident response process should promptly: identify and evaluate any potential network anomaly or intrusion; assess its nature and scope; determine if any data or information may have been accessed or compromised; quarantine the threat or malware; prevent the exfiltration of information from the firm; eradicate the malware, and restore the integrity of the firm’s network.

Incident response plans should identify the team members and their backups; provide the means to reach team members at any time an intrusion is reported, and

¹⁸ See ABA CYBERSECURITY HANDBOOK, *supra* note 11, at 202 (explaining the utility of large law firms adopting “an incident response plan that details who has ownership of key decisions and the process to follow in the event of an incident.”).

¹⁹ NIST Computer Security Incident Handling Guide, at 6 (2012), <https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf>.

define the roles of each team member. The plan should outline the steps to be taken at each stage of the process, designate the team member(s) responsible for each of those steps, as well as the team member charged with overall responsibility for the response.²⁰

Whether or not the lawyer impacted by a data breach has an incident response plan in place, after taking prompt action to stop the breach, a competent lawyer must make all reasonable efforts to restore computer operations to be able again to service the needs of the lawyer's clients. The lawyer may do so either on her own, if qualified, or through association with experts. This restoration process provides the lawyer with an opportunity to evaluate what occurred and how to prevent a reoccurrence consistent with the obligation under Model Rule 1.6(c) that lawyers "make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of the client."²¹ These reasonable efforts could include (i) restoring the technology systems as practical, (ii) the implementation of new technology or new systems, or (iii) the use of no technology at all if the task does not require it, depending on the circumstances.

3. Determining What Occurred

The Model Rules do not impose greater or different obligations on a lawyer as a result of a breach involving client information, regardless of whether the breach occurs through electronic or physical means. Just as a lawyer would need to assess which paper files were stolen from the lawyer's office, so too lawyers must make reasonable attempts to determine whether electronic files were accessed, and if so, which ones. A competent attorney must make reasonable efforts to determine what occurred during the data breach. A post-breach investigation requires that the lawyer gather sufficient information to ensure the intrusion has been stopped and then, to the extent reasonably possible, evaluate the data lost or accessed. The information gathered in a post-breach investigation is necessary to understand the scope of the intrusion and to allow for accurate disclosure to the client consistent with the lawyer's duty of communication and honesty under

²⁰ Steven M. Puiszis, *Prevention and Response: A Two-Pronged Approach to Cyber Security and Incident Response Planning*, THE PROF'L LAWYER, Vol. 24, No. 3 (Nov. 2017).

²¹ We discuss Model Rule 1.6(c) further below. But in restoring computer operations, lawyers should consider whether the lawyer's computer systems need to be upgraded or otherwise modified to address vulnerabilities, and further, whether some information is too sensitive to continue to be stored electronically.

Model Rules 1.4 and 8.4(c).²² Again, how a lawyer actually makes this determination is beyond the scope of this opinion. Such protocols may be a part of an incident response plan.

B. Duty of Confidentiality

In 2012, amendments to Rule 1.6 modified both the Rule and the commentary about a lawyer's efforts that are required to preserve the confidentiality of information relating to the representation of a client. Model Rule 1.6(a) requires that "A lawyer shall not reveal information relating to the representation of a client" unless certain circumstances arise.²³ The 2012 modification added a duty in paragraph (c) that: "A lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client."²⁴

Amended Comment [18] explains:

Paragraph (c) requires a lawyer to act competently to safeguard information relating to the representation of a client against unauthorized access by third parties and against inadvertent or unauthorized disclosure by the lawyer or other persons who are participating in the representation of the client or who are subject to the lawyer's supervision. *See* Rules 1.1, 5.1 and 5.3. The unauthorized access to, or the inadvertent or unauthorized disclosure of, information relating to the representation of a client does not constitute a violation of paragraph (c) if the lawyer has made reasonable efforts to prevent the access or disclosure.

Recognizing the necessity of employing a fact-based analysis, Comment [18] to Model Rule 1.6(c) includes nonexclusive factors to guide lawyers in making a "reasonable efforts" determination. Those factors include:

- the sensitivity of the information,
- the likelihood of disclosure if additional safeguards are not employed,
- the cost of employing additional safeguards,
- the difficulty of implementing the safeguards, and

²² The rules against dishonesty and deceit may apply, for example, where the lawyer's failure to make an adequate disclosure --- or any disclosure at all --- amounts to deceit by silence. *See, e.g.*, MODEL RULES OF PROF'L CONDUCT R. 4.1 cmt. [1] (2018) ("Misrepresentations can also occur by partially true but misleading statements or omissions that are the equivalent of affirmative false statements.")

²³ MODEL RULES OF PROF'L CONDUCT R. 1.6(a) (2018).

²⁴ *Id.* at (c).

- the extent to which the safeguards adversely affect the lawyer’s ability to represent clients (e.g., by making a device or important piece of software excessively difficult to use).²⁵

As this Committee recognized in ABA Formal Opinion 477R:

At the intersection of a lawyer’s competence obligation to keep “abreast of knowledge of the benefits and risks associated with relevant technology,” and confidentiality obligation to make “reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client,” lawyers must exercise reasonable efforts when using technology in communicating about client matters. What constitutes reasonable efforts is not susceptible to a hard and fast rule, but rather is contingent upon a set of factors.

As discussed above and in Formal Opinion 477R, an attorney’s competence in preserving a client’s confidentiality is not a strict liability standard and does not require the lawyer to be invulnerable or impenetrable.²⁶ Rather, the obligation is one of reasonable efforts. Rule 1.6 is not violated even if data is lost or accessed if the lawyer has made reasonable efforts to prevent the loss or access.²⁷ As noted above, this obligation includes efforts to monitor for breaches of client confidentiality. The nature and scope of this standard is addressed in the ABA Cybersecurity Handbook:

Although security is relative, a legal standard for “reasonable” security is emerging. That standard rejects requirements for specific security measures (such as firewalls, passwords, or the like) and instead adopts a fact-specific approach to business security obligations that requires a “process” to assess risks, identify and implement appropriate security measures responsive to those risks, verify that the measures are effectively implemented, and ensure that they are continually updated in response to new developments.²⁸

²⁵ MODEL RULES OF PROF’L CONDUCT R. 1.6 cmt. [18] (2018). “The [Ethics 20/20] Commission examined the possibility of offering more detailed guidance about the measures that lawyers should employ. The Commission concluded, however, that technology is changing too rapidly to offer such guidance and that the particular measures lawyers should use will necessarily change as technology evolves and as new risks emerge and new security procedures become available.” ABA COMMISSION REPORT 105A, *supra* note 9, at 5.

²⁶ ABA CYBERSECURITY HANDBOOK, *supra* note 11, at 122.

²⁷ MODEL RULES OF PROF’L CONDUCT R. 1.6, cmt. [18] (2018) (“The unauthorized access to, or the inadvertent or unauthorized disclosure of, information relating to the representation of a client does not constitute a violation of paragraph (c) if the lawyer has made reasonable efforts to prevent the access or disclosure.”)

²⁸ ABA CYBERSECURITY HANDBOOK, *supra* note 11, at 73.

Finally, Model Rule 1.6 permits a lawyer to reveal information relating to the representation of a client if the disclosure is impliedly authorized in order to carry out the representation. Such disclosures are permitted if the lawyer reasonably believes that disclosure: (1) is impliedly authorized and will advance the interests of the client in the representation, and (2) will not affect a material interest of the client adversely.²⁹ In exercising this discretion to disclose information to law enforcement about the data breach, the lawyer must consider: (i) whether the client would object to the disclosure; (ii) whether the client would be harmed by the disclosure; and (iii) whether reporting the theft would benefit the client by assisting in ending the breach or recovering stolen information. Even then, without consent, the lawyer may disclose only such information as is reasonably necessary to assist in stopping the breach or recovering the stolen information.

C. Lawyer's Obligations to Provide Notice of Data Breach

When a lawyer knows or reasonably should know a data breach has occurred, the lawyer must evaluate notice obligations. Due to record retention requirements of Model Rule 1.15, information compromised by the data breach may belong or relate to the representation of a current client or former client.³⁰ We address each below.

1. Current Client

Communications between a lawyer and current client are addressed generally in Model Rule 1.4. Rule 1.4(a)(3) provides that a lawyer must “keep the client reasonably informed about the status of the matter.” Rule 1.4(b) provides: “A lawyer shall explain a matter to the extent reasonably necessary to permit the client to make informed decisions regarding the representation.” Under these provisions, an obligation exists for a lawyer to communicate with current clients about a data breach.³¹

²⁹ ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 01-421(2001) (disclosures to insurer in bills when lawyer representing insured).

³⁰ This opinion addresses only obligations to clients and former clients. Data breach, as used in this opinion, is limited to client confidential information. We do not address ethical duties, if any, to third parties.

³¹ Relying on Rule 1.4 generally, the New York State Bar Committee on Professional Ethics concluded that a lawyer must notify affected clients of information lost through an online data storage provider. N.Y. State Bar Ass'n Op. 842 (2010) (Question 10: “If the lawyer learns of any breach of confidentiality by the online storage provider, then the lawyer must investigate whether there has been any breach of his or her own clients' confidential information,

Our conclusion here is consistent with ABA Formal Ethics Opinion 95-398 where this Committee said that notice must be given to clients if a breach of confidentiality was committed by or through a third-party computer vendor or other service provider. There, the Committee concluded notice to the client of the breach may be required under 1.4(b) for a “serious breach.”³² The Committee advised:

Where the unauthorized release of confidential information could reasonably be viewed as a significant factor in the representation, for example where it is likely to affect the position of the client or the outcome of the client's legal matter, disclosure of the breach would be required under Rule 1.4(b).³³

A data breach under this opinion involves the misappropriation, destruction or compromise of client confidential information, or a situation where a lawyer’s ability to perform the legal services for which the lawyer was hired is significantly impaired by the event. Each of these scenarios is one where a client’s interests have a reasonable possibility of being negatively impacted. When a data breach occurs involving, or having a substantial likelihood of involving, material client confidential information a lawyer has a duty to notify the client of the breach. As noted in ABA Formal Opinion 95-398, a data breach requires notice to the client because such notice is an integral part of keeping a “client reasonably informed about the status of the matter” and the lawyer should provide information as would be “reasonably necessary to permit the client to make informed decisions regarding the representation” within the meaning of Model Rule 1.4.³⁴

The strong client protections mandated by Model Rule 1.1, 1.6, 5.1 and 5.3, particularly as they were amended in 2012 to account for risks associated with the use of technology, would be compromised if a lawyer who experiences a data breach that impacts client confidential information is permitted to hide those events from their clients. And in view of the duties imposed by these other Model Rules, Model Rule 1.4’s requirement to keep clients “reasonably informed about the status” of a matter would ring hollow if a data breach was somehow excepted from this responsibility to communicate.

notify any affected clients, and discontinue use of the service unless the lawyer receives assurances that any security issues have been sufficiently remediated.”) (*citations omitted*).

³² ABA Comm. on Ethics & Prof’l Responsibility, Formal Op. 95-398 (1995).

³³ *Id.*

³⁴ MODEL RULES OF PROF’L CONDUCT R. 1.4(b) (2018).

Model Rule 1.15(a) provides that a lawyer shall hold “property” of clients “in connection with a representation separate from the lawyer’s own property.” Funds must be kept in a separate account, and “[o]ther property shall be identified as such and appropriately safeguarded.” Model Rule 1.15(a) also provides that, “Complete records of such account funds and other property shall be kept by the lawyer” Comment [1] to Model Rule 1.15 states:

A lawyer should hold property of others with the care required of a professional fiduciary. Securities should be kept in a safe deposit box, except when some other form of safekeeping is warranted by special circumstances. All property that is the property of clients or third persons, including prospective clients, must be kept separate from the lawyer’s business and personal property.

An open question exists whether Model Rule 1.15’s reference to “property” includes information stored in electronic form. Comment [1] uses as examples “securities” and “property” that should be kept separate from the lawyer’s “business and personal property.” That language suggests Rule 1.15 is limited to tangible property which can be physically segregated. On the other hand, many courts have moved to electronic filing and law firms routinely use email and electronic document formats to image or transfer information. Reading Rule 1.15’s safeguarding obligation to apply to hard copy client files but not electronic client files is not a reasonable reading of the Rule.

Jurisdictions that have addressed the issue are in agreement. For example, Arizona Ethics Opinion 07-02 concluded that client files may be maintained in electronic form, with client consent, but that lawyers must take reasonable precautions to safeguard the data under the duty imposed in Rule 1.15. The District of Columbia Formal Ethics Opinion 357 concluded that, “Lawyers who maintain client records solely in electronic form should take reasonable steps (1) to ensure the continued availability of the electronic records in an accessible form during the period for which they must be retained and (2) to guard against the risk of unauthorized disclosure of client information.”

The Committee has engaged in considerable discussion over whether Model Rule 1.15 and, taken together, the technology amendments to Rules 1.1, 1.6, and 5.3 impliedly impose an obligation on a lawyer to notify a current client of a data breach. We do not have to decide that question in the absence of concrete facts. We reiterate, however, the obligation to inform the client does exist under Model Rule 1.4.

2. Former Client

Model Rule 1.9(c) requires that “A lawyer who has formerly represented a client in a matter or whose present or former firm has formerly represented a client in a matter shall not thereafter . . . reveal information relating to the representation except as these Rules would permit or require with respect to a client.”³⁵ When electronic “information relating to the representation” of a former client is subject to unauthorized access, disclosure, or destruction, the Model Rules provide no direct guidance on a lawyer’s obligation to notify the former client. Rule 1.9(c) provides that a lawyer “shall not . . . reveal” the former client’s information. It does not describe what steps, if any, a lawyer should take if such information is revealed. The Committee is unwilling to require notice to a former client as a matter of legal ethics in the absence of a black letter provision requiring such notice.³⁶

Nevertheless, we note that clients can make an informed waiver of the protections in Rule 1.9.³⁷ We also note that Rule 1.16(d) directs that lawyers should return “papers and property” to clients at the conclusion of the representation, which has commonly been understood to include the client’s file, in whatever form it is held. Rule 1.16(d) also has been interpreted as permitting lawyers to establish appropriate data destruction policies to avoid retaining client files and property indefinitely.³⁸ Therefore, as a matter of best practices, lawyers are encouraged to reach agreement with clients before conclusion, or at the termination, of the relationship about how to handle the client’s electronic information that is in the lawyer’s possession.

Absent an agreement with the former client lawyers are encouraged to adopt and follow a paper and electronic document retention schedule, which meets all applicable laws and rules, to reduce the amount of information relating to the representation of former clients that the lawyers retain. In addition, lawyers should recognize that in the event of a data breach involving former client information, data privacy laws, common law duties of care, or contractual arrangements with

³⁵ MODEL RULES OF PROF’L CONDUCT R. 1.9(c)(2) (2018).

³⁶ See *Discipline of Feland*, 2012 ND 174, ¶ 19, 820 N.W.2d 672 (Rejecting respondent’s argument that the court should engraft an additional element of proof in a disciplinary charge because “such a result would go beyond the clear language of the rule and constitute amendatory rulemaking within an ongoing disciplinary proceeding.”).

³⁷ See MODEL RULES OF PROF’L CONDUCT R. 1.9, cmt. [9] (2018).

³⁸ See ABA Ethics Search Materials on Client File Retention, https://www.americanbar.org/content/dam/aba/administrative/professional_responsibility/piles_of_files_2008.pdf (last visited Oct. 15, 2018).

the former client relating to records retention, may mandate notice to former clients of a data breach. A prudent lawyer will consider such issues in evaluating the response to the data breach in relation to former clients.³⁹

3. Breach Notification Requirements

The nature and extent of the lawyer's communication will depend on the type of breach that occurs and the nature of the data compromised by the breach. Unlike the "safe harbor" provisions of Comment [18] to Model Rule 1.6, if a post-breach obligation to notify is triggered, a lawyer must make the disclosure irrespective of what type of security efforts were implemented prior to the breach. For example, no notification is required if the lawyer's office file server was subject to a ransomware attack but no information relating to the representation of a client was inaccessible for any material amount of time, or was not accessed by or disclosed to unauthorized persons. Conversely, disclosure will be required if material client information was actually or reasonably suspected to have been accessed, disclosed or lost in a breach.

The disclosure must be sufficient to provide enough information for the client to make an informed decision as to what to do next, if anything. In a data breach scenario, the minimum disclosure required to all affected clients under Rule 1.4 is that there has been unauthorized access to or disclosure of their information, or that unauthorized access or disclosure is reasonably suspected of having occurred. Lawyers must advise clients of the known or reasonably ascertainable extent to which client information was accessed or disclosed. If the lawyer has made reasonable efforts to ascertain the extent of information affected by the breach but cannot do so, the client must be advised of that fact.

In addition, and as a matter of best practices, a lawyer also should inform the client of the lawyer's plan to respond to the data breach, from efforts to recover information (if feasible) to steps being taken to increase data security.

The Committee concludes that lawyers have a continuing duty to keep clients reasonably apprised of material developments in post-breach investigations affecting the clients'

³⁹ Cf. ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 482 (2018), at 8-10 (discussing obligations regarding client files lost or destroyed during disasters like hurricanes, floods, tornadoes, and fires).

information.⁴⁰ Again, specific advice on the nature and extent of follow up communications cannot be provided in this opinion due to the infinite number of variable scenarios.

If personally identifiable information of clients or others is compromised as a result of a data breach, the lawyer should evaluate the lawyer's obligations under state and federal law. All fifty states, the District of Columbia, Guam, Puerto Rico, and the Virgin Islands have statutory breach notification laws.⁴¹ Those statutes require that private or governmental entities notify individuals of breaches involving loss or disclosure of personally identifiable information.⁴² Most breach notification laws specify who must comply with the law, define "personal information," define what constitutes a breach, and provide requirements for notice.⁴³ Many federal and state agencies also have confidentiality and breach notification requirements.⁴⁴ These regulatory schemes have the potential to cover individuals who meet particular statutory notice triggers, irrespective of the individual's relationship with the lawyer. Thus, beyond a Rule 1.4 obligation, lawyers should evaluate whether they must provide a statutory or regulatory data breach notification to clients or others based upon the nature of the information in the lawyer's possession that was accessed by an unauthorized user.⁴⁵

III. Conclusion

Even lawyers who, (i) under Model Rule 1.6(c), make "reasonable efforts to prevent the . . . unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client," (ii) under Model Rule 1.1, stay abreast of changes in technology, and (iii) under Model Rules 5.1 and 5.3, properly supervise other lawyers and third-party electronic-information storage vendors, may suffer a data breach. When they do, they have a duty to notify clients of the data

⁴⁰ State Bar of Mich. Op. RI-09 (1991).

⁴¹ National Conference of State Legislatures, *Security Breach Notification Laws* (Sept. 29, 2018), <http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx>.

⁴² *Id.*

⁴³ *Id.*

⁴⁴ ABA CYBERSECURITY HANDBOOK, *supra* note 11, at 65.

⁴⁵ Given the broad scope of statutory duties to notify, lawyers would be well served to actively manage the amount of confidential and or personally identifiable information they store beyond any ethical, statutory, or other legal obligation to do so. Lawyers should implement, and follow, a document retention policy that comports with Model Rule 1.15 and evaluate ways to limit receipt, possession and/or retention of confidential or personally identifiable information during or after an engagement.

breach under Model Rule 1.4 in sufficient detail to keep clients “reasonably informed” and with an explanation “to the extent necessary to permit the client to make informed decisions regarding the representation.”

AMERICAN BAR ASSOCIATION STANDING COMMITTEE ON ETHICS AND PROFESSIONAL RESPONSIBILITY

321 N. Clark Street, Chicago, Illinois 60654-4714 Telephone (312) 988-5328

CHAIR: Barbara S. Gillers, New York, NY ■ John M. Barkett, Miami, FL ■ Wendy Wen Yun Chang, Los Angeles, CA ■ Hon. Daniel J. Crothers, Bismarck, ND ■ Keith R. Fisher, Arlington, VA ■ Douglas R. Richmond, Chicago, IL ■ Michael H. Rubin, Baton Rouge, LA ■ Lynda Shely, Scottsdale, AZ ■ Elizabeth C. Tarbert, Tallahassee, FL. ■ Allison Wood, Chicago, IL

CENTER FOR PROFESSIONAL RESPONSIBILITY: Dennis A. Rendleman, Ethics Counsel

©2018 by the American Bar Association. All rights reserved.

Outside Counsel

Expert Analysis

Strategies for Navigating Business-to-Business Data Breaches

There is no shortage of attention in the media to data breaches affecting consumers in the United States—so called “business to consumer,” or “B2C” data breaches. And rightfully so—the Identity Theft Resource Center, which has been tracking data breaches in the United States since 2005, released a report in January 2015 which showed that U.S. B2C data breaches hit a record high of 783 in 2014.¹ This number represents an increase of 27.5 percent over similar breaches reported in 2013, and pushes the total number of U.S. data breach incidents tracked since 2005 to 5,029 reported incidents involving over 675 million estimated records.²

For example, in January 2014, Target revealed that it had been the victim of a computer hack through which the contact information of 70 million individuals and information relating to 40 million credit and debit card accounts were stolen.³ In early 2015, Anthem announced that a cyberattack had compromised the personal information of almost 80 million individuals, including names, dates of birth, Social Security numbers, health care ID numbers, home addresses, email addresses, and employment information.⁴

In large part, it is the number of consumers affected that has led to the increased media onslaught that follows these types of B2C breaches, as well as the call to arms for legislative changes to address these security issues across industries. It is no coincidence that the Obama Administration has made consumer data protection a priority with its proposed data protection act, which will, among other things, require companies to publicly disclose a data compromise within 30 days of it occurring.⁵

In the midst of all this focus on consumer data protection and B2C breaches, however, the media and the Legislature have largely ignored



By
**Joseph V.
DeMarco**

And
**Urvashi
Sen**

data privacy breaches that are not directly consumer-facing privacy concerns—so-called “business to business,” or “B2B” breaches. Such breaches tend to occur quietly, for two main reasons: (1) there are currently no overarching statutory obligations to report data breaches that do not involve statutorily defined categories of personally identifiable information (PII) belonging to consumers; and (2) it is in a company’s best interest to keep breaches of this nature (really, any breaches at all) quiet, so as to prevent the public airing of their potential security flaws.

It is also for these reasons that companies tend not to focus their attention, and their resources, on B2B breach scenarios. It is easy to understand why a B2C breach, which can so directly affect a company’s bottom line in a much clearer and more quantifiable manner through public notification and media involvement, is generally where companies put their best thinking and resources. However, to ignore the potential damage that B2B breaches can cause would be a huge mistake. Indeed, companies can go a long way toward protecting themselves from B2B data breach incidents by implementing two simple, yet critical, measures: (1) retaining expert privacy counsel to perform due diligence on potential business partners and vendors, and (2) ensuring that vendor and other business contracts contain key clauses addressing potential cybersecurity incidents—in particular, arbitration clauses that cover data breaches.

B2B Breaches

While it is certainly in neither party’s interest in a B2B data breach to air its grievances publicly,

this does not mean that such situations are simple affairs that are quickly and painlessly resolved. In fact, the opposite is most likely the case—without regulatory or statutory parameters to inform the discussion, and without a direct public fallout to steer companies in the right direction, these types of “quiet” breaches can result in very contentious disputes that may drag on and become difficult to resolve.

In one public example of just how far the fallout from a B2B breach can extend, it was reported in March 2014 that a security breach had impacted the e-commerce platform of Createthe Group (CTG), a digital luxury agency that provides e-commerce solutions to a number of recognizable brands in the retail and fashion space, including Calvin Klein, H&M, Hugo Boss, Louis Vuitton, and many more.⁶ CTG ultimately retired its e-commerce platform and exited the e-commerce space altogether (although the security breach was not cited specifically by CTG as a reason for this decision).⁷ Notably, in this case the security breach resulted in the alleged compromise of credit card numbers belonging to customers of the various brands CTG represented,⁸ no doubt one of the reasons why the breach was reported in the press at all.

Even without a public media backlash, however, it is not difficult to imagine how damaging a B2B data breach incident can be to a company. A compromise of a company’s systems, whether through malware received from a vendor or business partner, or through a breach of such a third party’s own security systems, consumes the time, energy, and resources of an organization. Even if no consumer data is impacted by the breach,⁹ the impact of a B2B breach can result in tremendous losses to a company, including the costs involved in assessing the breach itself, which often can encompass its impact on the company’s systems and data, determining and implementing solutions necessary to prevent such an incident to future, spending employee and attorney (in most cases, outside counsel) hours interfacing with the third party responsible for the breach, and managing any reputational damage that may have occurred.

JOSEPH V. DEMARCO is a partner at DeVore & DeMarco and previously served as an assistant U.S. attorney for the Southern District of New York, where he founded and headed the Computer Hacking and Intellectual Property Program. URVASHI SEN is counsel at DeVore & DeMarco.

Pre-Contract Due Diligence

One important step a company should take prior to entering into an agreement with a business partner or vendor is to ensure that these third parties follow robust, industry-appropriate security and privacy protocols. What these protocols should be will vary greatly depending on the industry and the size of the third party in question. As such, it is essential that each company contemplating a third-party business relationship retain outside, expert counsel to guide them in this process. The amount of money at stake in each business relationship and the level of data connectivity that will result between the company and the third party will determine how much due diligence is necessary prior to entering into a contractual relationship.

Smaller, simpler associations may only require a basic review of the third party's policies and procedures, whereas for more complex and long-term relationships, a more robust vetting of the third party's cybersecurity policies and protocols may be appropriate. In all cases, the vetting should be done under counsel privilege to the maximum degree permitted by law.

While such due diligence may, on its face, appear arduous, in fact this type of "pre-screening" not only goes a long way toward preventing a potential external security breach that may affect the company, but also sends a very clear message about the level of importance the company places on cybersecurity matters. This can often be a critical deterrent to a third party that may ordinarily choose to play fast and loose with cybersecurity best practices.¹⁰

Contracts and Arbitration

Another key strategy companies can employ in protecting themselves from potential B2B data breaches is to ensure that contracts with vendors and business partners specifically address cybersecurity matters, from preventative measures, to risk allocation and dispute resolution in the event of a data security breach.

As a preliminary matter, contracts should outline the data security procedures and protocols that the third party agrees to comply with. What these procedures should be will, ideally, become clear in the due diligence phase discussed above. Contracts should also address the procedures that should be followed in the event of a security breach and how risk in that context should be allocated.

Specifically, companies should ensure that (1) the third party is contractually obligated to report any security incidents in a reasonably prompt manner to the company; (2) the contract includes a clause allocating risk for certain basic types of data breach incidents; (3) the contract addresses indemnification in the data breach context; and (4) the contract includes a broad-form arbitration clause covering all disputes, including disputes relating to data security and privacy matters, and data breaches in particular.¹¹

An arbitration clause is, in our view, a critical component to handling data security breaches in B2B relationships. There are undoubtedly numerous advantages to companies across various industries that choose to arbitrate, rather than litigate, their contractual disputes, regardless of the subject matter of the dispute itself. However, B2B data breach incidents actually present what appears to be the perfect case for the use of arbitration clauses.

First, arbitrating a B2B security incident is more likely to result in a speedier, more efficient, and less costly resolution, not least of all because the evidentiary hearing can proceed uninterrupted, hour-to-hour, on sequential days as needed, as opposed to courtroom proceedings with myriad interruptions and off-days. Additionally, pre-hearing procedures such as discovery and motion practice are streamlined. This frees up company resources to address and rectify the root problems that resulted in the breach, particularly when preceded by mediation, as is generally recommended by the various arbitration associations.¹²

Notably, the efficiency of an arbitration proceeding can be greatly increased by carefully negotiating contractual agreements between parties, such as including a "stepped" arbitration clause, which requires the parties to engage in meaningful mediation prior to entering into a formal arbitration proceeding, and an indemnification clause that covers various security incident scenarios. Here, too, having knowledgeable, expert data privacy counsel to review contracts with third parties for data security issues will go a long way in preventing long and messy disputes when breaches do occur.

Second, an arbitration not only can ensure that legitimate subject-matter expert arbitrators, with all the technical qualifications necessary to understand complex data security and privacy matters, will resolve the matter, but also eliminates the possibility that an emotional jury, panicking at the prospect of potential effects on consumers from the breach and ill-equipped to comprehend the technical nature of the subject matter, will be the ultimate decision-makers. Additionally, arbitration affords parties the ability to elect in advance whether to have the arbitrator (or arbitrators) issue a bare, standard award or a reasoned award, which has implications relating to delay, expense, and susceptibility to vacatur.

Third, arbitration proceedings can be kept confidential, whereas courtroom proceedings typically cannot be, even if a jury is not involved. This is a key factor for companies navigating a security breach incident, particularly in the current climate of intense scrutiny facing reported breaches. In many cases, it is a tremendous uphill battle to recover from the reputational damage that can result from the public revelation of a data breach, for both parties involved—so much so, that without the option of a confidential arbitration, companies may

choose to forgo dispute resolution, swallowing their losses instead. Arbitration provides an ideal environment to ensure that such situations do not arise.

Fourth, arbitration affords far greater finality of decision than court proceedings, where appellate possibilities abound. In data breach disputes, this finality allows both parties to put the dispute behind them quickly, and focus their energies on rectifying the breach and working toward preventing future incidents.

Top of the Agenda

Ultimately, in this current environment of record-high breaches and, undoubtedly, record-high scrutiny of companies impacted by breaches, it is in each company's best interest to put cybersecurity at the top of the agenda, regardless of whether or not consumer data is likely to be implicated in a security incident. Preventive and protective measures can go a long way toward saving a company from catastrophic losses, both financial and reputational.

Endnotes:

1. See "Data Breach Reports, Dec. 31, 2014," Dec. 31, 2014, available at http://www.idtheftcenter.org/images/Breach/DataBreachReports_2014.pdf.

2. "Identity Theft Resource Center Breach Report Hits Record High in 2014," Jan. 12, 2015, available at <http://www.idtheftcenter.org/ITRC-Surveys-Studies/2014databreaches.html>.

3. See "Data Breach FAQ," <https://corporate.target.com/about/shopping-experience/payment-card-issue-faq>.

4. See "Anthem Facts," last updated May 8, 2015, <https://www.anthemfacts.com/>; see also "State Breakdowns: Anthem Breach by the Numbers," Feb. 26, 2015, available at <http://www.scmagazine.com/victims-of-the-anthem-breach-stretch-across-multiple-states/article/400489/>.

5. "Fact Sheet: Safeguarding American Consumers and Families," Jan. 12, 2015, available at <https://www.whitehouse.gov/the-press-office/2015/01/12/fact-sheet-safeguarding-american-consumers-families>.

6. "American Express Customers Receiving New Breach Notifications," June 20, 2014, <http://www.csoonline.com/article/2365803/data-protection/american-express-customers-receiving-new-breach-notifications.html>.

7. "Fashion Firms Probing Alleged Data Breach," March 26, 2014, http://www.zeeereport.com/breaking_news/4023-Fashion_Firms_Probing_Alleged_Data_Breach.html.

8. "American Express Customers Receiving New Breach Notifications," supra note 6.

9. Notably, it is also possible that a B2B or other type of breach will impact certain customer data, but not the types of data that trigger reporting obligations. For example, in New York (and many other states), name, date of birth, and address information, although considered "personal information," are not, standing alone, "private information" that, if compromised, requires notification of either individuals impacted or governmental agencies. See N.Y. GBS, Law §899-aa.

10. Of course, it is also crucial for companies to ensure they have appropriate cybersecurity insurance coverage that will protect them from security incidents prior to entering into contracts with third parties. This is not an easy task—all too often companies purchase expensive products that are peppered with loopholes, either rendering the coverage ineffective even in some of the most basic breach scenarios, or requiring policy modifications in order to become effective. Legal expertise, through outside data privacy counsel, can be critical here to ensure that the most cost-effective, robust policy is purchased, and that it appropriately covers B2B data breaches.

11. There are a range of reasons why arbitration clauses may be beneficial for all business-to-business matters. While a discussion of those reasons is beyond the scope of this article, we note that broad-form arbitration clauses are, at the very least, procedurally preferable. This is because carving up disputes into different silos for different treatment can be incredibly problematic and inefficient, particularly if parties are forced to arbitrate certain claims and litigate others (and, indeed, to go to court to determine what disputes are covered by the scope of the arbitration clause).

12. For example, under the American Arbitration Association Rules, parties must mediate disputes for claims in excess of \$75,000 unless one of them actively opts out of the mediation process. See American Arbitration Association's Commercial Rules and Mediation Procedures, Rule 9.