Frankie L. Trull
President, National Association for Biomedical Research

Frankie Trull is President of the National Association for Biomedical Research (NABR) and the Foundation for Biomedical Research. She also heads up Policy Directions, a Washington, DC- based government relations firm.

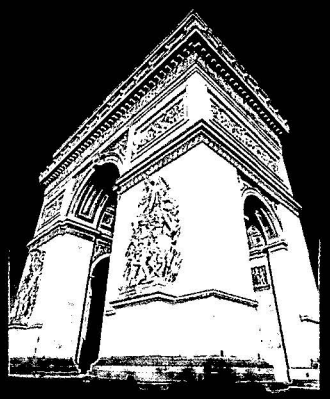
Ms. Trull has been involved in animal rights and animal extremist issues for more than 3 decades. She has been recognized for her work in representing the biomedical research community by receiving among others, the Presidential Award from the Society for Neuroscience, the Distinguished Leadership Award from The Endocrine Society, the Public Service Award from the American Association of Immunologists and the Association of American Medical Colleges Special Recognition Award.

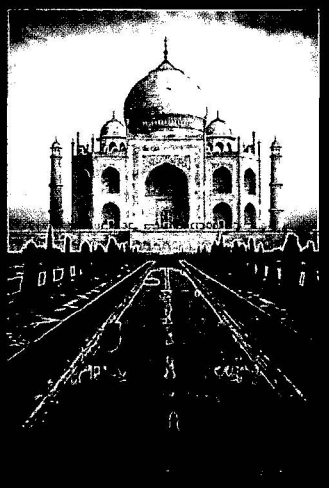
She has given more than 500 presentations and speeches in the US, Europe and Japan on biomedical research and government relations topics before medical professional societies, deans and university presidents groups, pharmaceutical and biotechnology companies, government agencies and scientific organizations. She has testified before Congress on numerous occasions on behalf of NABR's membership.

Frankie has served on the boards of both companies and foundations and is currently on the board of overseers of the Tufts University Cummings School of Veterinary Medicine.

A Massachusetts native, she received a BA from Boston University and an MA from Tufts University.

U.S. Department of Justice
Federal Bureau of Investigation






SAFETY AND SECURITY
for US Students Traveling Abroad

Living and studying in another country will be an enriching and rewarding experience, especially if you are prepared and take certain precautions. This brochure will introduce you to threats you may face and provide tips on avoiding unsafe situations. Following these precautions will reduce your risk of encountering problems.

Did You Know?

Groups of children and teens may swarm you and forcibly steal your personal belongings.

"Act Smart. Be Safe."

An ounce of prevention is worth a pound of cure.

Before You Go

Familiarize yourself with local laws and customs in the areas you plan to travel. You are expected to obey their laws, which may include dress standards, photography restrictions, telecommunication restrictions, curfews, etc.

Plan your wardrobe so that it does not offend the locals, nor draw unwanted attention to yourself. Americans are perceived as wealthy and are targeted for pick pocketing and other crimes. Do not wear expensive-looking jewelry and avoid wearing American team sports shirts or baseball caps that might indicate you are an American.

Make copies of your passport, airplane ticket, driver's license, and credit cards that you take with you. Keep one copy at home; carry a second copy with you but separate from the originals. This will help speed the replacement process if they are lost or stolen.

Do not take unnecessary identification or credit cards in case they are stolen. Take only what is necessary. Obtain traveler's checks if needed.

Establish points of contact for your family to contact and for your foreign hosts to contact in the event of an emergency. Register your trip with the State Department.

Take any necessary medications with you in their original containers and keep them in your carry-on luggage (not checked baggage) during the flight. Verify you have adequate medical insurance.

Obtain specific pre-travel country risk assessments for the country/countries you plan to visit from your study abroad program manager, the State Department, and/or the FBI. There may be specific issues you should be aware of and prepare for that will ensure your safety and peace of mind.

Useful websites:
State Department Students Abroad:
www.studentsabroad.state.gov
State Department travel website:
www.state.gov/travel
Center for Disease Control for Travelers' Health:
www.cdc.gov

During Your Stay

Protect your passport! Theft of American tourist passports is on the rise. It is recommended that you carry your passport in a front pants pocket or in a pouch hidden in your clothes, and that it remain with you at all times. Some hotels require you to leave it at the desk during your stay and they may use it to register you with the local police--a routine policy. Ask for a receipt and be sure to retrieve your passport before continuing your trip. If your passport is lost or stolen, report the situation immediately to the nearest US Embassy or Consulate.

Do not invite strangers into your room.

Be courteous and cooperative when processing through customs. Do not leave your bags unattended. Stay alert.

Use only authorized taxis. Passengers have been robbed or kidnapped when using "gypsy" taxis.

Avoid traveling alone, especially after dark. Be conscious of your surroundings and avoid areas you believe may put your personal safety at risk. Be wary of street vendors and innocent-looking youngsters. While one person has your attention, another may be picking your pocket.

Do not carry large amounts of cash. Always deal with reputable currency exchange officials or you run the risk of receiving counterfeit currency. Keep a record of your financial transactions.

Beware that theft from sleeping compartments on trains is common.

Do not leave drinks unattended – someone could slip a drug into it that causes amnesia and sleep.

Avoid long waits in lobbies and terminals, if possible. These areas may harbor pickpockets, thieves, and violent offenders. Laptop theft is especially common in airports.

In an international airport, a thief positioned himself to walk in front of a traveler who was walking with his roll bag. The thief stopped abruptly in front of the traveler causing the traveler to also stop. A second thief was following and quickly removed the traveler's laptop from his roll bag and disappeared.

Avoid civil disturbances and obey local laws. If you come upon a demonstration or rally, be careful; in the confusion you could be arrested or detained even though you are a bystander. Be mindful that in many countries, it is prohibited to speak derogatorily of the government and its leaders. It may be illegal to take photographs of train stations, government buildings, religious symbols, and military installations.

Avoid actions that are illegal, improper or indiscreet. Avoid offers of sexual companionship; they may lead to a room raid, photography, and blackmail. Do not attempt to keep up with your hosts in social drinking. Do not engage in black market activities. Do not sell your possessions. Do not bring in or purchase illegal drugs or pornography. Do not seek out political or religious dissidents. Do not accept packages or letters for delivery to another location.

An American was given a letter by a man he had never met. He tried to return the letter but the man ran away. That evening, national security officers visited the American, admonished him for taking the letter, and required him to sign a statement concerning the event.

If you are arrested for any reason, ask to notify the nearest US Embassy or Consulate. A consular officer cannot arrange for free legal aid or provide bail money, but they can assist you. Do not admit to wrongdoing or sign anything. Do not agree to help your detainer.

Keep a low profile and shun publicity. Do not discuss personal or family information with local news media, and as a general rule, be careful what information you share with foreigners. They may have been directed to obtain information about you for duplicitous purposes and may use what they learn to target or use against you.

Evade criminals and terrorists by being aware of your surroundings and alert to the possibility of surveillance. Take mental notes of anyone following you and promptly report it to the appropriate security officials and/or the US Embassy or Consulate. In general, criminals will strike when their target seems most vulnerable and lax about his/her security. If anyone grabs you, make a scene-- yell, fight and try to get away! If you are kidnapped, remain alert and establish a program of mental and physical activity for yourself; try to remain calm and non-threatening.

"Turkey drop" scam: a person drops money in front of a victim while an accomplice waits for the money to be picked up and suggests splitting it. The first person returns and accuses both of stealing the money. This usually results in the victim's money being stolen.

Beware of new acquaintances who probe for information about you or who attempt to get you involved in what could become a compromising situation.

Do not gossip about character flaws, financial problems, emotional relationships, or other difficulties of your fellow Americans or yourself. This information is eagerly sought by those who want to exploit you or your fellow travelers.

Beware that your conversations may not be private or secure. Unlike the United States, most other countries do not have legal restrictions against technical surveillance. Most foreign security services have various means of screening incoming visitors to identify persons of potential intelligence interest. They also have well established contacts with hotels and common hosts that can assist in various forms of monitoring you.

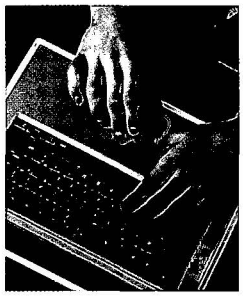
Two American students on study abroad talked privately about the lighting in their apartment. The next day, a light that had been out for weeks was working.

Telephone, Laptop & PDA Security

If you can do without the device, Do Not Take It!

Do not leave electronic devices unattended. Do not transport them (or anything valuable) in your checked baggage. Shield passwords from view. Avoid Wi-Fi networks if you can. In some countries they are controlled by security services; in all cases they are insecure.

Sanitize your laptop, telephone, & PDA, prior to travel and ensure no sensitive contact, research, or personal data is on them. Back-up all information you take and leave that at home. If feasible, use a different phone and a new email account while traveling.



Use up-to-date protections for antivirus, spyware, security patches, and firewalls. Don't use thumb drives given to you – they may be compromised.

During the Beijing Olympics, hotels were required to install software so law enforcement could monitor the Internet activity of hotel guests.

Clear your browser after each use: delete history files, caches, cookies, and temporary internet files.

In most countries, you have no expectation of privacy in Internet cafes, hotels, airplanes, offices, or public spaces. All information you send electronically (fax, computer, telephone) can be intercepted, especially wireless communications. If information might be valuable to another government, company or group, you should assume that it will be intercepted and retained. Security services and criminals can track your movements using your mobile phone and can turn on the microphone in your device even when you think it is turned off.

Beware of "phishing." Foreign security services and criminals are adept at pretending to be someone you trust in order to obtain personal or sensitive information.

If your device is stolen, report it immediately to the local US Embassy or Consulate.

Change all your passwords including your voicemail and check devices for malware when you return.

Cyber criminals from numerous countries buy and sell stolen financial information including credit card data and login credentials (user names and passwords).

Upon Your Return

Report any unusual circumstances or noteworthy incidents to your study abroad program manager and to the FBI. Notifying the FBI will help ensure that future travel advisories take into consideration the circumstances and incidents you encountered. It is not uncommon for foreigners to contact you after your return. The FBI may be able to help you determine if these contacts pose any risk to you.

Important Numbers

US Embassy/Consulate Phone & Address:

_____

_____

_____

POC in country: _____

_____

Reminder

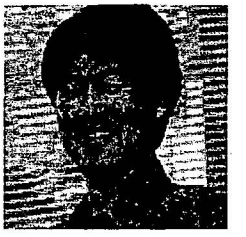
Our country will be judged by the impression you make. As an American abroad, you serve as a spokesperson for the United States.

Additional travel security tips and country threat assessments are available from the FBI upon request.

Your local FBI office #: _____

www.fbi.gov

Peter Lee



Peter Lee is the Head of the Computer Science Department at Carnegie Mellon University. He joined the faculty after completing his doctoral studies at the University of Michigan in 1987. Today he is a leading figure in computer science research, particularly in areas related to software security and reliability. An elected Fellow of the Association for Computing Machinery, several of his papers have received "test of time" awards for contributions that have demonstrated long-term impact. His work on "proof-carrying code" received the ACM SIGOPS Hall of Fame Award, for seminal contributions to computer systems research.

As the Head of the Computer Science Department, Peter Lee oversees one of the world's top research organizations, with over 80 faculty members (including two active Turing Award winners) and top-rated degree programs at both the doctoral and undergraduate levels. Prior to assuming his current position, Dr. Lee was briefly the Vice Provost for Research, where he provided administrative oversight and strategic guidance for the university's research activities, an enterprise that exceeds $450M in annual expenditures.

Peter Lee is called upon as an expert in diverse venues, including distinguished lectures at major universities, memberships on senior government advisory panels, and corporate advisory boards. Recently, he testified before the Science and Technology Committee off the U.S. House of Representatives. He is the incoming Chair of the Board of Directors of the Computing Research Association, member of the NRC Computer Science and Telecommunications Board and the Computing Community Consortium Council, and Vice-Chair of the Defense Advanced Research Projects Agency's Information Scienceand Technology Board.

Recent Significant Professional Activities:

Principal Investigator, Computing Innovation Fellows Project, May 2009 to present. Creating more than 100 research and higher education postdoctoral fellowships for new computing PhDs.
The National Academies, Computer Science and Telecommunications Board of the National Research Council (CSTB), September 2008 to present.
DARPA Information Science and Technology (ISAT) Board, September 2003 to present. Vice chair since August 2008.
Computing Research Association, March 2005 to present. Incoming Chair of the Board of Directors.
ACM SIGPLAN Executive Committee, 1997-1999, and again in 2005-present. Elected member.
DARPA Information Exploitation Office (IXO), Nov. 2003 to Aug. 2008. Member of the Senior Advisory Group.
Cedilla Systems Incorporated, Pittsburgh, November 1998 to December 2000. President and Co-founder (with George Necula). A security technology start-up.
Defense Science Board, March 2001 to September 2002. Co-chair, Technology Panel of the 2001 Summer Study on Defense Science and Technology.
Microsoft Corporation, December 1998 to March 2000. Expert Witness in the *Sun v. Microsoft* "Java lawsuit."

Assistant Director Marcus Thomas – Operational Technology Divisioin

Mr. Thomas was born in 1962 in Chattanooga, Tennessee, and earned his Bachelor of Science in Engineering degree in 1985 from the University of Tennessee. Before entering the FBI, Mr. Thomas worked as a designer within the Nuclear power industry.
Mr. Thomas entered on duty as a Special Agent with the FBI on April 21, 1986 and served as a Special Agent for more than 21 years. Upon completion of training at Quantico, he was assigned to the Washington Field Office, where he worked Domestic Terrorism, Criminal Investigations, and Foreign Counterintelligence.
In 1991, Mr. Thomas was appointed as a Supervisory Special Agent to the Technical Services Division, a precursor to the present-day Operational Technology Division. Since that time, Mr. Thomas has held a variety of positions and responsibilities associated with providing technical support to field office investigative operations. These positions include Unit Chief (1996), Advanced Telephony Unit, Section Chief (2000), Cyber Technology Section, and Deputy Assistant Director (2002) of the Operational Technology Division. In December, 2006, he was named Assistant Director, Operational Technology Division. Mr. Thomas can be reached during duty hours at [redacted] b6 b7C
or via enterprise e-mail at [redacted]
Mr. Thomas resides in [redacted]