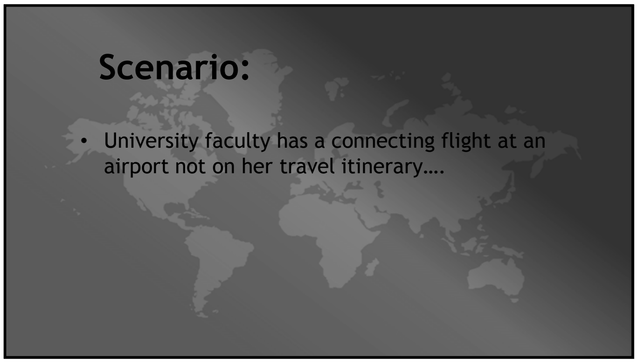
Encryption Fails

…and other Tales

International Travel, Borders & Mobile Devices

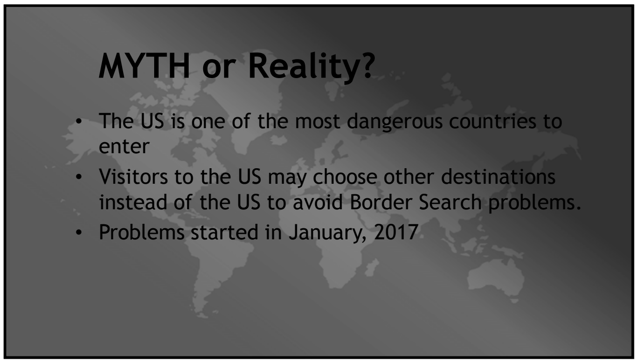
June 4th, 2018

Austin, Texas



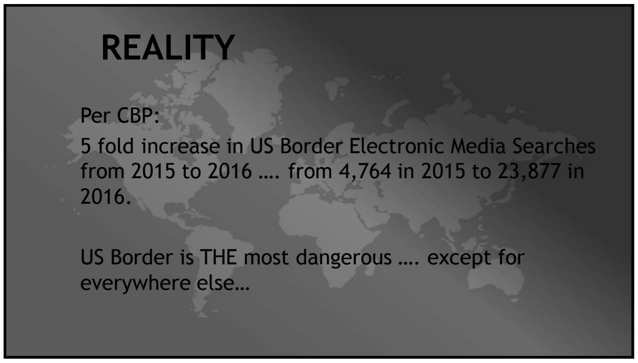
Scenario:

- University faculty has a connecting flight at an airport not on her travel itinerary….



MYTH or Reality?

- The US is one of the most dangerous countries to enter
- Visitors to the US may choose other destinations instead of the US to avoid Border Search problems.
- Problems started in January, 2017

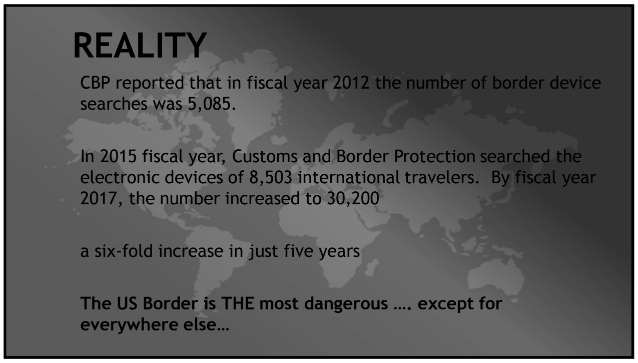


REALITY

Per CBP:

5 fold increase in US Border Electronic Media Searches from 2015 to 2016 …. from 4,764 in 2015 to 23,877 in 2016.

US Border is THE most dangerous …. except for everywhere else…



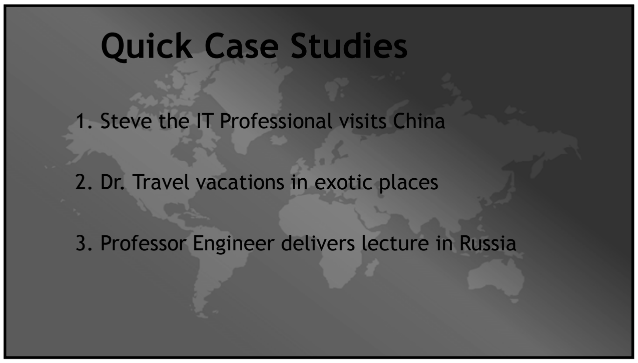
REALITY

CBP reported that in fiscal year 2012 the number of border device searches was 5,085.

In 2015 fiscal year, Customs and Border Protection searched the electronic devices of 8,503 international travelers. By fiscal year 2017, the number increased to 30,200

a six-fold increase in just five years

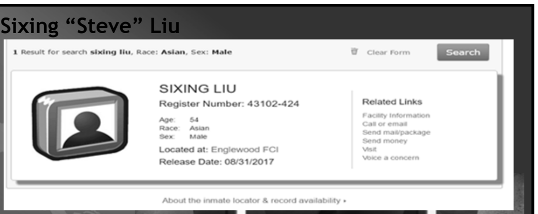
The US Border is THE most dangerous …. except for everywhere else…



Quick Case Studies

1. Steve the IT Professional visits China
2. Dr. Travel vacations in exotic places
3. Professor Engineer delivers lecture in Russia

Sixing “Steve” Liu


1 Result for search **sixing liu**, Race: **Asian**, Sex: **Male**

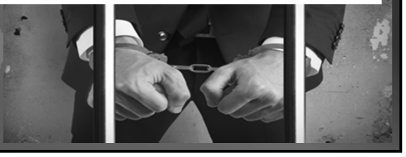
SIXING LIU

Register Number: 43102-424

Age: 54
Race: Asian
Sex: Male

Located at: Englewood FCI

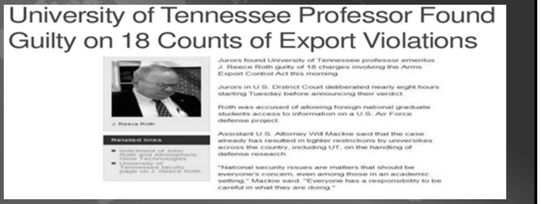
Release Date: 08/31/2017



In the news… Sept. 26, 2012:

A federal jury in Newark found Steve Liu guilty on nine counts, including exporting defense-related data without a license, possessing stolen trade secrets and lying to federal agents.

The case began when he returned with his laptop to Newark Airport on his return from China.


University of Tennessee Professor Found Guilty on 18 Counts of Export Violations

J. Reece Roth

Jurors found University of Tennessee professor emeritus J. Reece Roth guilty of 18 charges involving the Arms Export Control Act this morning.

Jurors in U.S. District Court deliberated nearly eight hours starting Tuesday before announcing their verdict.

Roth was accused of allowing foreign national graduate students access to information on a U.S. Air Force defense project.

Assistant U.S. Attorney Will Mackie said that the case already has resulted in tighter restrictions by universities across the country, including UT, on the handling of defense research.

"National security issues are matters that should be everyone's concern, even among those in an academic setting," Mackie said. "Everyone has a responsibility to be careful in what they are doing."

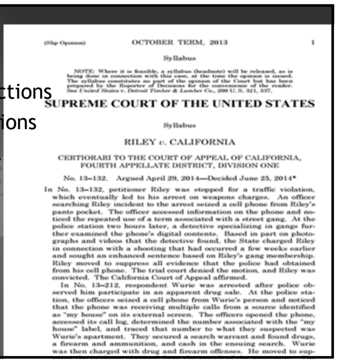
Related links
Indictment of John Roth and Atmospheric Glow Technologies
University of Tennessee faculty page on J. Reece Roth

Hot Zones

1. US Domestic
2. US Border Zone
3. International Border Crossings
4. Non-Embargoed Countries
5. Russia and China
6. Embargoed Countries

US Domestic

1. Constitutional Protections
2. Known rules/regulations
3. Encryption is critical
4. Limits on searches



(Slip Opinion) OCTOBER TERM, 2013 1

Syllabus

NOTE: Where it is feasible, a syllabus (headnote) will be released, as is being done in connection with this case, at the time the opinion is issued. The syllabus constitutes no part of the opinion of the Court but has been prepared by the Reporter of Decisions for the convenience of the reader. See *United States* v. *Detroit Timber & Lumber Co.*, 200 U. S. 321, 337.

SUPREME COURT OF THE UNITED STATES

Syllabus

RILEY *v.* CALIFORNIA

CERTIORARI TO THE COURT OF APPEAL OF CALIFORNIA, FOURTH APPELLATE DISTRICT, DIVISION ONE

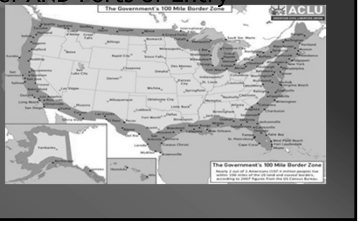
No. 13–132. Argued April 29, 2014—Decided June 25, 2014*

In No. 13–132, petitioner Riley was stopped for a traffic violation, which eventually led to his arrest on weapons charges. An officer searching Riley incident to the arrest seized a cell phone from Riley's pants pocket. The officer accessed information on the phone and noticed the repeated use of a term associated with a street gang. At the police station two hours later, a detective specializing in gangs further examined the phone's digital contents. Based in part on photographs and videos that the detective found, the State charged Riley in connection with a shooting that had occurred a few weeks earlier and sought an enhanced sentence based on Riley's gang membership. Riley moved to suppress all evidence that the police had obtained from his cell phone. The trial court denied the motion, and Riley was convicted. The California Court of Appeal affirmed.

In No. 13–212, respondent Wurie was arrested after police observed him participate in an apparent drug sale. At the police station, the officers seized a cell phone from Wurie's person and noticed that the phone was receiving multiple calls from a source identified as "my house" on its external screen. The officers opened the phone, accessed its call log, determined the number associated with the "my house" label, and traced that number to what they suspected was Wurie's apartment. They secured a search warrant and found drugs, a firearm and ammunition, and cash in the ensuing search. Wurie was then charged with drug and firearm offenses. He moved to sup-

What IS the US Border?

1. Constitutional limits
2. 100 miles off border AND Ports of Entry including Airports


The Government's 100 Mile Border Zone
ACLU
The Government's 100 Mile Border Zone
Nearly 2 out of 3 Americans (197.4 million people) live within 100 miles of the US land and coastal borders, according to 2007 figures from the US Census Bureau.

US Border

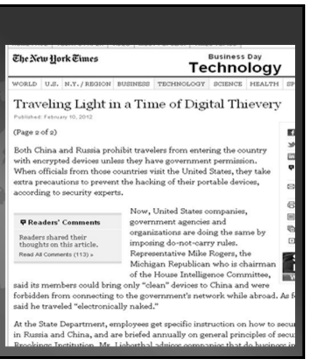
1. US Domestic
2. US Border Zone
3. International Border Crossings
4. Non-Embargoed Countries
5. Embargoed Countries

Hot Zone or Friendly?

Great Britain
Australia
Canada

International Travel:

The Data Breach Zone!



Traveling Light in a Time of Digital Thievery

Published: February 10, 2012

(Page 2 of 2)

Both China and Russia prohibit travelers from entering the country with encrypted devices unless they have government permission. When officials from those countries visit the United States, they take extra precautions to prevent the hacking of their portable devices, according to security experts.

Readers' Comments

Readers shared their thoughts on this article.

Read All Comments (113) »

Now, United States companies, government agencies and organizations are doing the same by imposing do-not-carry rules. Representative Mike Rogers, the Michigan Republican who is chairman of the House Intelligence Committee, said its members could bring only "clean" devices to China and were forbidden from connecting to the government's network while abroad. As f said he traveled "electronically naked."

At the State Department, employees get specific instruction on how to secu in Russia and China, and are briefed annually on general principles of secu Brookings Institution. Mr. Lieberthal advises companies that do business in

Hotel Room Incursions

Hotel Room Incursion.mp4

Hypothetical Question…

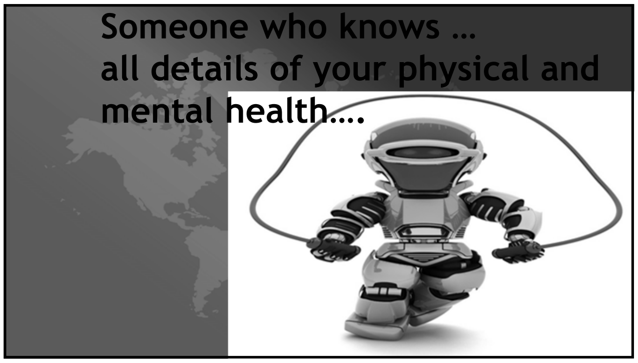
Who knows you best?

Best friend?

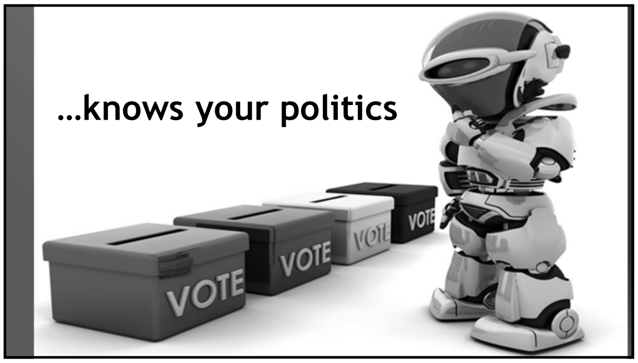
Significant other?

What if…

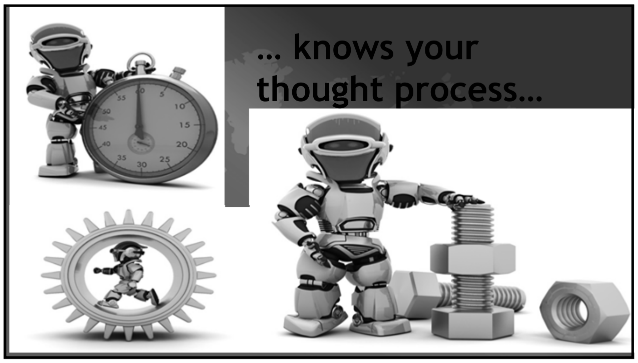
there was someone else?



Someone who knows …
all details of your physical and mental health….



…knows your politics



… knows your thought process…

…has full access to all your files…

…knows your finances…

…knows your online accounts…

…knows your passwords…

…knows who you communicate with…

…knows your search history…

…knows where you've been…

…knows your upcoming plans…

…knows intimate secrets…

…has access to your images…

…logs all of your ONLINE activities

…fits in your hand and travels everywhere with you…

…knows EVERYTHING about you AND holds ALL your data….

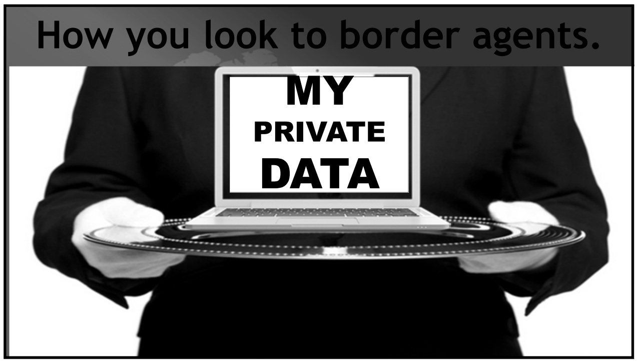
…and will generously share all your secrets when properly asked!

I.T. Security prepares for…

Instead of…

What time is it when you arrive?

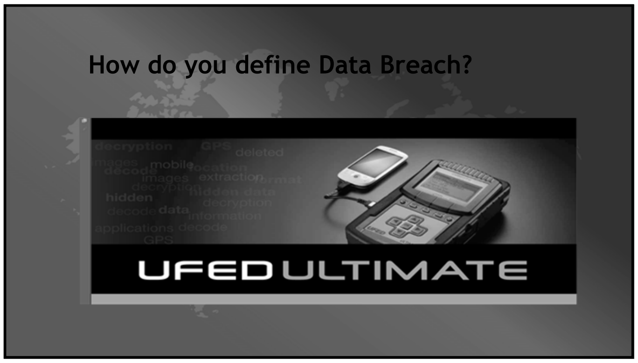
Time to Harvest the Data



How you look to border agents.

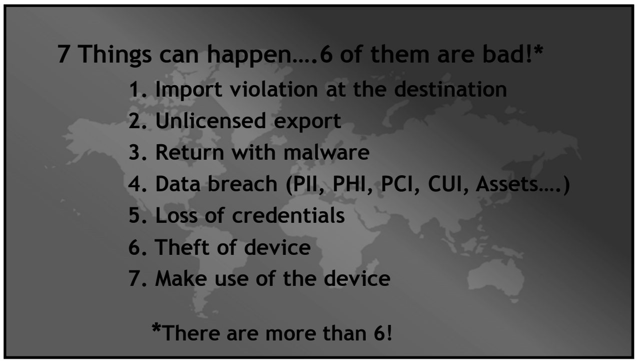
Just a mobile device?

Or something more?



How do you define Data Breach?

decryption
GPS
deleted
mobile
location
extraction
hidden
data
decode
applications
UFED ULTIMATE

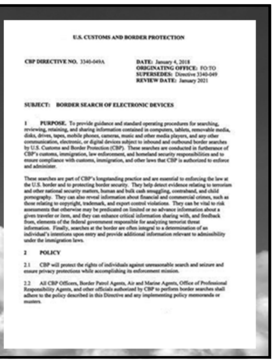


7 Things can happen….6 of them are bad!*

1. Import violation at the destination
2. Unlicensed export
3. Return with malware
4. Data breach (PII, PHI, PCI, CUI, Assets….)
5. Loss of credentials
6. Theft of device
7. Make use of the device

*There are more than 6!

“It’s OK…the data is encrypted ….right?”



U.S. CUSTOMS AND BORDER PROTECTION

CBP DIRECTIVE NO. 3340-049A

DATE: January 4, 2018
ORIGINATING OFFICE: FO:TO
SUPERSEDES: Directive 3340-049
REVIEW DATE: January 2021

SUBJECT: BORDER SEARCH OF ELECTRONIC DEVICES

1 **PURPOSE.** To provide guidance and standard operating procedures for searching, reviewing, retaining, and sharing information contained in computers, tablets, removable media, disks, drives, tapes, mobile phones, cameras, music and other media players, and any other communication, electronic, or digital devices subject to inbound and outbound border searches by U.S. Customs and Border Protection (CBP). These searches are conducted in furtherance of CBP's customs, immigration, law enforcement, and homeland security responsibilities and to ensure compliance with customs, immigration, and other laws that CBP is authorized to enforce and administer.

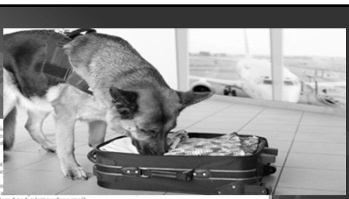
These searches are part of CBP's longstanding practice and are essential to enforcing the law at the U.S. border and to protecting border security. They help detect evidence relating to terrorism and other national security matters, human and bulk cash smuggling, contraband, and child pornography. They can also reveal information about financial and commercial crimes, such as those relating to copyright, trademark, and export control violations. They can be vital to risk assessments that otherwise may be predicated on limited or no advance information about a given traveler or item, and they can enhance critical information sharing with, and feedback from, elements of the federal government responsible for analyzing terrorist threat information. Finally, searches at the border are often integral to a determination of an individual's intentions upon entry and provide additional information relevant to admissibility under the immigration laws.

2 **POLICY**

2.1 CBP will protect the rights of individuals against unreasonable search and seizure and ensure privacy protections while accomplishing its enforcement mission.

2.2 All CBP Officers, Border Patrol Agents, Air and Marine Agents, Office of Professional Responsibility Agents, and other officials authorized by CBP to perform border searches shall adhere to the policy described in this Directive and any implementing policy memoranda or musters.

ICE Policy



5.3 **Electronic Media.** Any devi
Examples include: hard drive
portable music players, cell p
disks.

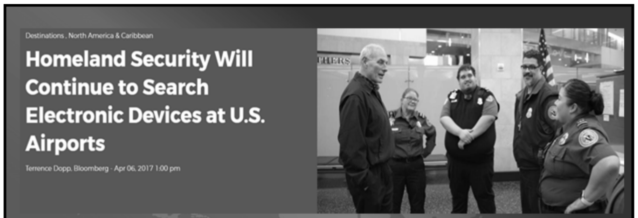
5.4 **Letter Class Mail.** U.S. first
postcards, aerogrammes, lette
class or category of postage.
in the U.S. postal system. On
deemed "mail," even if they a
or in baggage, are not considered to be letter class mail.

6. **POLICY.** ICE Special Agents acting under border search authority may search, detain, seize, retain, and share documents and electronic media consistent with the guidelines and applicable laws set forth herein. In the course of a border search, and absent individualized suspicion, officers can review the information transported by any individual attempting to enter, reenter, depart, pass through, or reside in the United States, subject to the requirements and limitations provided herein. Assistance to complete a thorough border search may be sought from outside agencies and entities, on a case by case basis, as appropriate.

NOTE: Nothing in this policy limits the authority of ICE Special Agents to make written notes or reports or to document impressions relating to a border encounter.

7. **RESPONSIBILITIES.**

7.1 The Directors of OI, OPR, and OIA have oversight over the implementation of the provisions of this Directive.



Destinations , North America & Caribbean

Homeland Security Will Continue to Search Electronic Devices at U.S. Airports

Terrence Dopp. Bloomberg - Apr 06. 2017 1:00 pm

Border Search Exception to the 4th Amend.

Searches conducted at the United States border or the equivalent of the border (such as an international airport) may be conducted without a warrant or probable cause subject to the "border-search" exception

Laptop Rule:

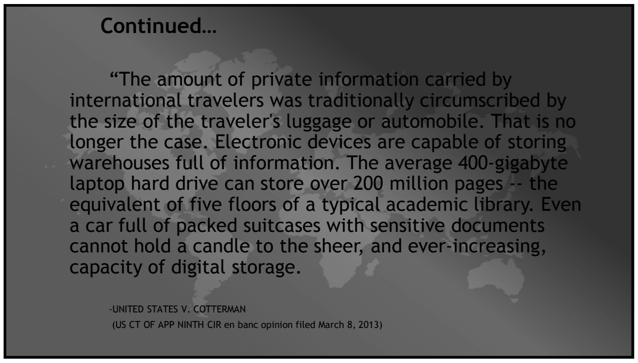
The U.S. Courts of Appeals for the Fourth and Ninth circuits have ruled that information on a traveler's electronic materials, including personal files on a laptop computer, may be searched at random, without suspicion

(US v. Ickes, 393 F.3d 501 (4th Cir., 2005) & US v. Arnold, 523 F.3d 941 (9th Cir. 2008)

US v. Cotterman….

The Courts…

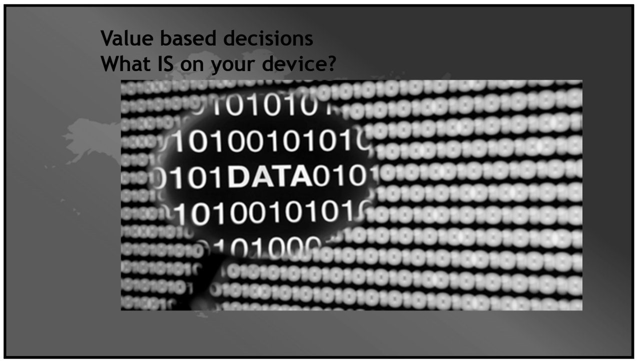
"Every day more than a million people cross American borders, from the physical borders with Mexico and Canada to functional borders at airports such as Los Angeles (LAX), Honolulu (HNL), New York (JFK, LGA), and Chicago (ORD, MDW). As denizens of a digital world, they carry with them laptop computers, iPhones, iPads, iPods, Kindles, Nooks, Surfaces, tablets, Blackberries, cell phones, digital cameras, and more. These devices often contain private and sensitive information ranging from personal, financial, and medical data to corporate trade secrets."



Continued…

“The amount of private information carried by international travelers was traditionally circumscribed by the size of the traveler's luggage or automobile. That is no longer the case. Electronic devices are capable of storing warehouses full of information. The average 400-gigabyte laptop hard drive can store over 200 million pages -- the equivalent of five floors of a typical academic library. Even a car full of packed suitcases with sensitive documents cannot hold a candle to the sheer, and ever-increasing, capacity of digital storage.

-UNITED STATES V. COTTERMAN
(US CT OF APP NINTH CIR en banc opinion filed March 8, 2013)



Value based decisions
What IS on your device?

101DATA010

International Borders:

Different Rules

Risk assessment:
Country specific decisions

Reality Check:

Travellers are exporters

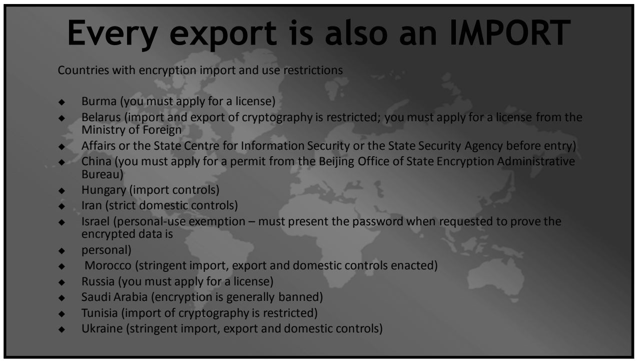
Your travel activities may legally constitute an export

Hand-carry travel items such as your laptop, smart phone, and software are subject to export controls and many other regulations.

Exports may requires a License

Taking certain items outside the US “may” require a license, for exam

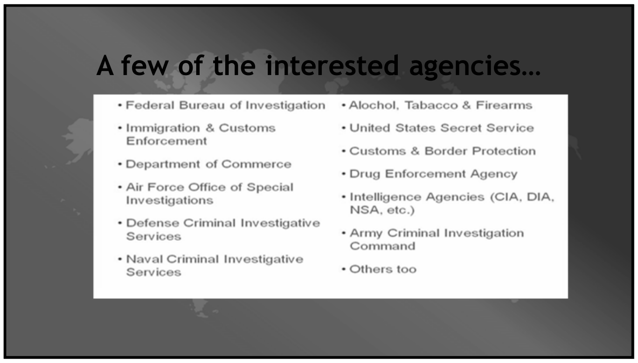
- Controlled technology
- Controlled hardware
- Data, technology
- Blueprints, schematics



Every export is also an IMPORT

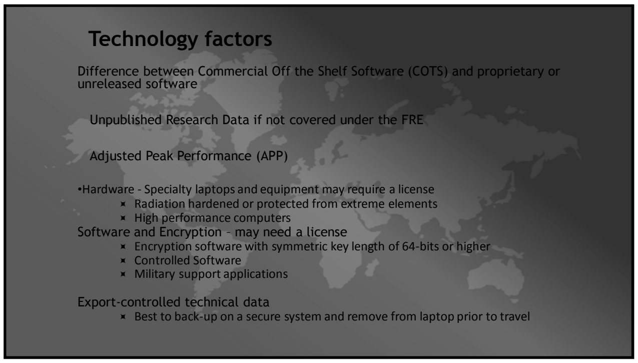
Countries with encryption import and use restrictions

- Burma (you must apply for a license)
- Belarus (import and export of cryptography is restricted; you must apply for a license from the Ministry of Foreign
- Affairs or the State Centre for Information Security or the State Security Agency before entry)
- China (you must apply for a permit from the Beijing Office of State Encryption Administrative Bureau)
- Hungary (import controls)
- Iran (strict domestic controls)
- Israel (personal-use exemption – must present the password when requested to prove the encrypted data is
- personal)
- Morocco (stringent import, export and domestic controls enacted)
- Russia (you must apply for a license)
- Saudi Arabia (encryption is generally banned)
- Tunisia (import of cryptography is restricted)
- Ukraine (stringent import, export and domestic controls)



A few of the interested agencies…

- Federal Bureau of Investigation
- Immigration & Customs Enforcement
- Department of Commerce
- Air Force Office of Special Investigations
- Defense Criminal Investigative Services
- Naval Criminal Investigative Services
- Alochol, Tabacco & Firearms
- United States Secret Service
- Customs & Border Protection
- Drug Enforcement Agency
- Intelligence Agencies (CIA, DIA, NSA, etc.)
- Army Criminal Investigation Command
- Others too



Technology factors

Difference between Commercial Off the Shelf Software (COTS) and proprietary or unreleased software

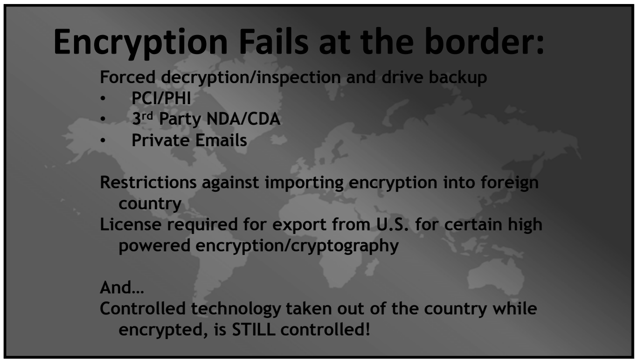
Unpublished Research Data if not covered under the FRE

Adjusted Peak Performance (APP)

•Hardware - Specialty laptops and equipment may require a license
- Radiation hardened or protected from extreme elements
- High performance computers

Software and Encryption - may need a license
- Encryption software with symmetric key length of 64-bits or higher
- Controlled Software
- Military support applications

Export-controlled technical data
- Best to back-up on a secure system and remove from laptop prior to travel



Encryption Fails at the border:

Forced decryption/inspection and drive backup

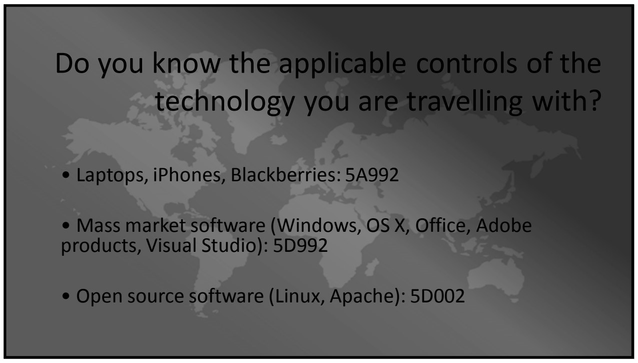
- PCI/PHI
- 3rd Party NDA/CDA
- Private Emails

Restrictions against importing encryption into foreign country

License required for export from U.S. for certain high powered encryption/cryptography

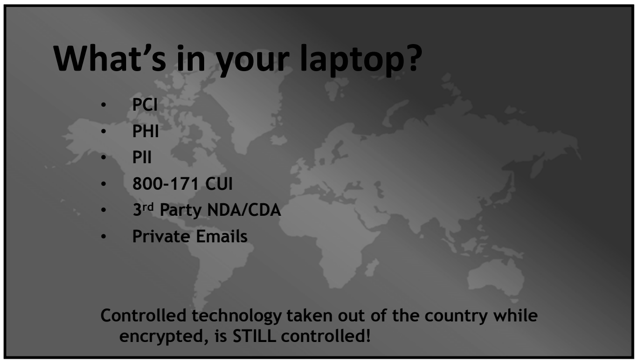
And…

Controlled technology taken out of the country while encrypted, is STILL controlled!



Do you know the applicable controls of the technology you are travelling with?

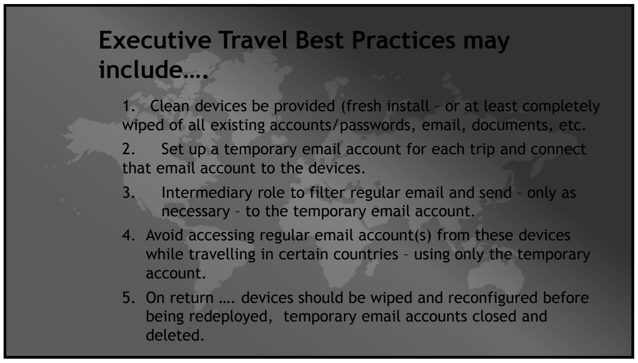
- Laptops, iPhones, Blackberries: 5A992
- Mass market software (Windows, OS X, Office, Adobe products, Visual Studio): 5D992
- Open source software (Linux, Apache): 5D002



What's in your laptop?

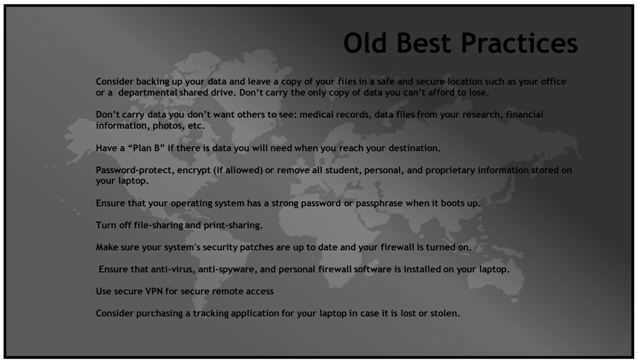
- PCI
- PHI
- PII
- 800-171 CUI
- 3rd Party NDA/CDA
- Private Emails

Controlled technology taken out of the country while encrypted, is STILL controlled!



Executive Travel Best Practices may include….

1. Clean devices be provided (fresh install – or at least completely wiped of all existing accounts/passwords, email, documents, etc.
2. Set up a temporary email account for each trip and connect that email account to the devices.
3. Intermediary role to filter regular email and send – only as necessary – to the temporary email account.
4. Avoid accessing regular email account(s) from these devices while travelling in certain countries – using only the temporary account.
5. On return …. devices should be wiped and reconfigured before being redeployed, temporary email accounts closed and deleted.



Old Best Practices

Consider backing up your data and leave a copy of your files in a safe and secure location such as your office or a departmental shared drive. Don't carry the only copy of data you can't afford to lose.

Don't carry data you don't want others to see: medical records, data files from your research, financial information, photos, etc.

Have a "Plan B" if there is data you will need when you reach your destination.

Password-protect, encrypt (if allowed) or remove all student, personal, and proprietary information stored on your laptop.

Ensure that your operating system has a strong password or passphrase when it boots up.

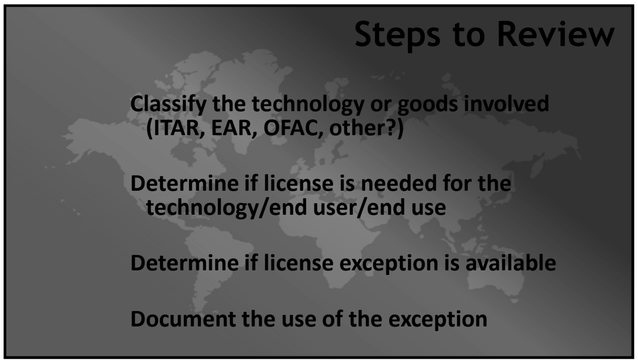
Turn off file-sharing and print-sharing.

Make sure your system's security patches are up to date and your firewall is turned on.

Ensure that anti-virus, anti-spyware, and personal firewall software is installed on your laptop.

Use secure VPN for secure remote access

Consider purchasing a tracking application for your laptop in case it is lost or stolen.



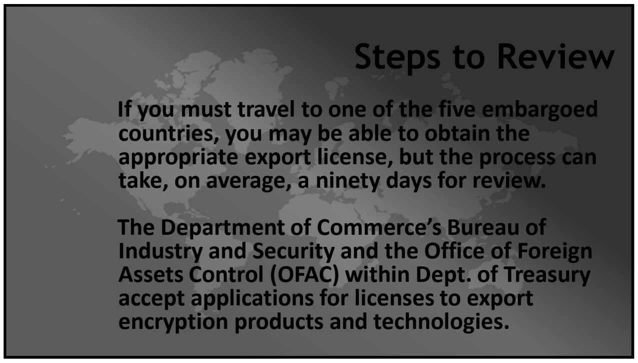
Steps to Review

Classify the technology or goods involved (ITAR, EAR, OFAC, other?)

Determine if license is needed for the technology/end user/end use

Determine if license exception is available

Document the use of the exception



Steps to Review

If you must travel to one of the five embargoed countries, you may be able to obtain the appropriate export license, but the process can take, on average, a ninety days for review.

The Department of Commerce's Bureau of Industry and Security and the Office of Foreign Assets Control (OFAC) within Dept. of Treasury accept applications for licenses to export encryption products and technologies.

Predicting the future…

What is NOW the minimum needed for international travel?

Former best practices?

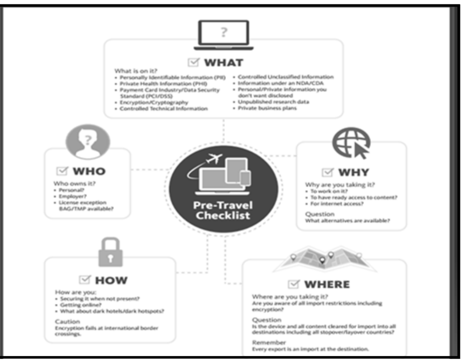
Exercise reasonable care when hand-carrying a laptop computer to a foreign country

The laptop:

- MUST remain in reasonable control of the person(s) responsible for it at all times
- MUST not be used by anyone in the foreign country
- MUST not be left behind (upon your return), given away, or out of the US more than 1 year.

Consider taking a minimal “Wiped” device

Plan ahead…



☑ WHAT

What is on it?

- Personally Identifiable Information (PII)
- Private Health Information (PHI)
- Payment Card Industry/Data Security Standard (PCI/DSS)
- Encryption/Cryptography
- Controlled Technical Information
- Controlled Unclassified Information
- Information under an NDA/CDA
- Personal/Private information you don't want disclosed
- Unpublished research data
- Private business plans

☑ WHO

Who owns it?

- Personal?
- Employer?
- License exception BAG/TMP available?

Pre-Travel Checklist

☑ WHY

Why are you taking it?

- To work on it?
- To have ready access to content?
- For internet access?

Question

What alternatives are available?

☑ HOW

How are you:

- Securing it when not present?
- Getting online?
- What about dark hotels/dark hotspots?

Caution

Encryption fails at international border crossings.

☑ WHERE

Where are you taking it?

Are you aware of all import restrictions including encryption?

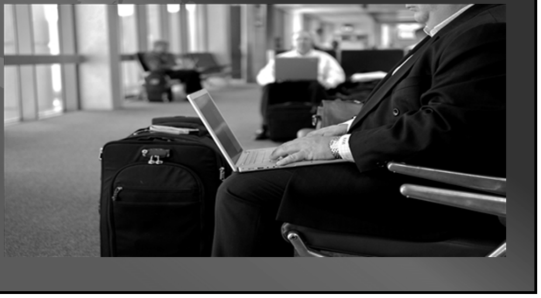
Question

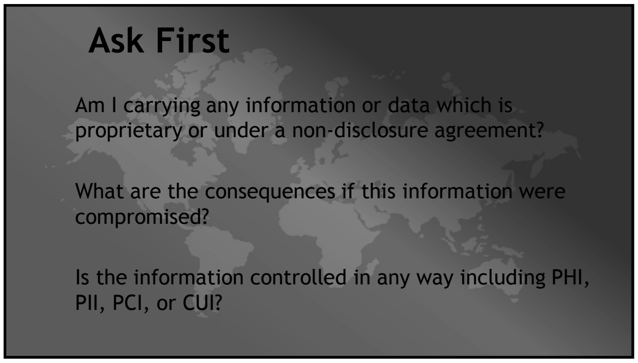
Is the device and all content cleared for import into all destinations including all stopover/layover countries?

Remember

Every export is an import at the destination.

Million dollar question: Is the data on your device worth more than the device itself?



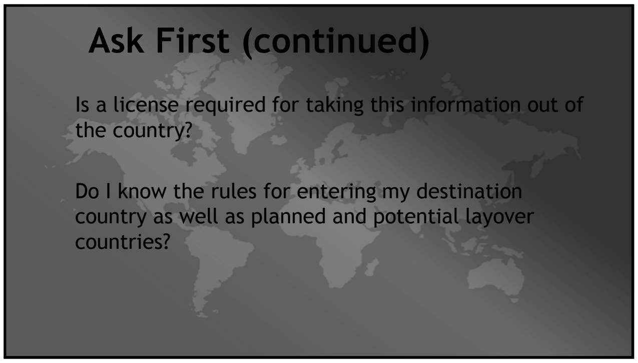


Ask First

Am I carrying any information or data which is proprietary or under a non-disclosure agreement?

What are the consequences if this information were compromised?

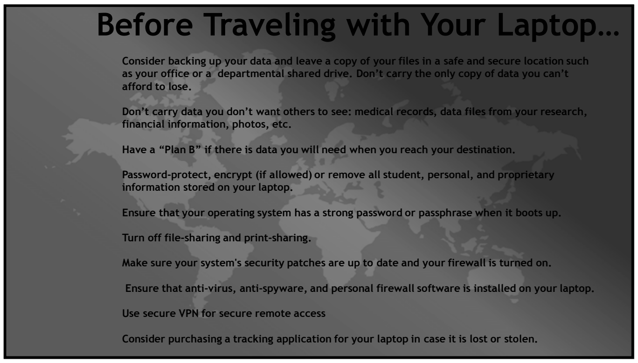
Is the information controlled in any way including PHI, PII, PCI, or CUI?



Ask First (continued)

Is a license required for taking this information out of the country?

Do I know the rules for entering my destination country as well as planned and potential layover countries?



Before Traveling with Your Laptop…

Consider backing up your data and leave a copy of your files in a safe and secure location such as your office or a departmental shared drive. Don't carry the only copy of data you can't afford to lose.

Don't carry data you don't want others to see: medical records, data files from your research, financial information, photos, etc.

Have a "Plan B" if there is data you will need when you reach your destination.

Password-protect, encrypt (if allowed) or remove all student, personal, and proprietary information stored on your laptop.

Ensure that your operating system has a strong password or passphrase when it boots up.

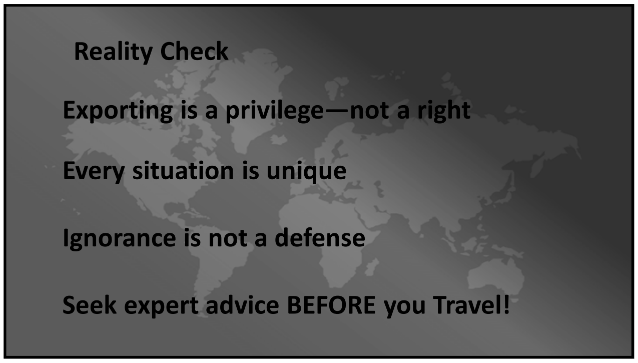
Turn off file-sharing and print-sharing.

Make sure your system's security patches are up to date and your firewall is turned on.

Ensure that anti-virus, anti-spyware, and personal firewall software is installed on your laptop.

Use secure VPN for secure remote access

Consider purchasing a tracking application for your laptop in case it is lost or stolen.



Reality Check

Exporting is a privilege—not a right

Every situation is unique

Ignorance is not a defense

Seek expert advice BEFORE you Travel!

No one size fits all solution

Plan ahead. Others are.

1

Questions?

Brian Mitchell Warshawsky
Brian.warshawsky@ucop.edu

(510) 987-0413