Introduction to Information Security 14-741/18-631 Fall 2021 Unit 2 (Cryptography): Lecture 4: Policy Overview

Hanan Hibshi hhibshi@andrew

Today's Agenda

- **Basic policy overview**
  - Human traits and their effect on policy
  - Various aspect of information technology policy
  - Evidential issues
- **Objectives**
  - Expose you to some of the non-technical aspects of security
    - Awareness of "layer 8/9" issues is mandatory to properly design/manage a secure system
  - Expose you to the pervasiveness of information security
  - Lead you to be able to form opinions on the role of government in information security

Why Cryptosystems Fail Revisited

- **Major policy takeaway points?**
- **Security by obscurity rarely succeeds**
- **Incentives shape policies**
  - Contrast US, UK
    - Legal incentive (Truth in lending act)
    - No incentive (“blame the customer”)
- **“Information security is about power”**
  - Brings the question of the role of the government in security policy

Perceptions of Risk

- **Suppose I give you two alternatives:**
  - I give you $1 or
  - I flip a fair coin; if it’s tails, you get $2; heads, you get nothing
- **What do you choose?**

Perceptions of Risk

- **Suppose I give you two alternatives:**
  - I give you $10,000,000 or
  - I flip a fair coin; if it's tails, you get $20,000,000; heads, you get nothing
- **What do you choose?**

Perceptions of Risk

- **Suppose I give you two alternatives:**
  - I give you $10,000,000 or
  - I flip a fair coin; if it’s tails, you get $50,000,000; heads, you get nothing
- **What do you choose?**

Previous Findings

- **Humans generally risk-averse when it comes to gains (prefer fixed payoff even though reward potentially less)**
  - Risk aversion generally increases with the amount at stake (relative to the endowment)
- **Humans generally risk-seeking when it comes to losses**
  - Asian flu experiment (Kahneman and Tversky)

    Two courses of action have been suggested. If program A is adopted, ***400 will die****. If program B is adopted, there is a one-third probability that nobody will die and a two-thirds probability that 600 people will die. Which of the two programs do you favor?*

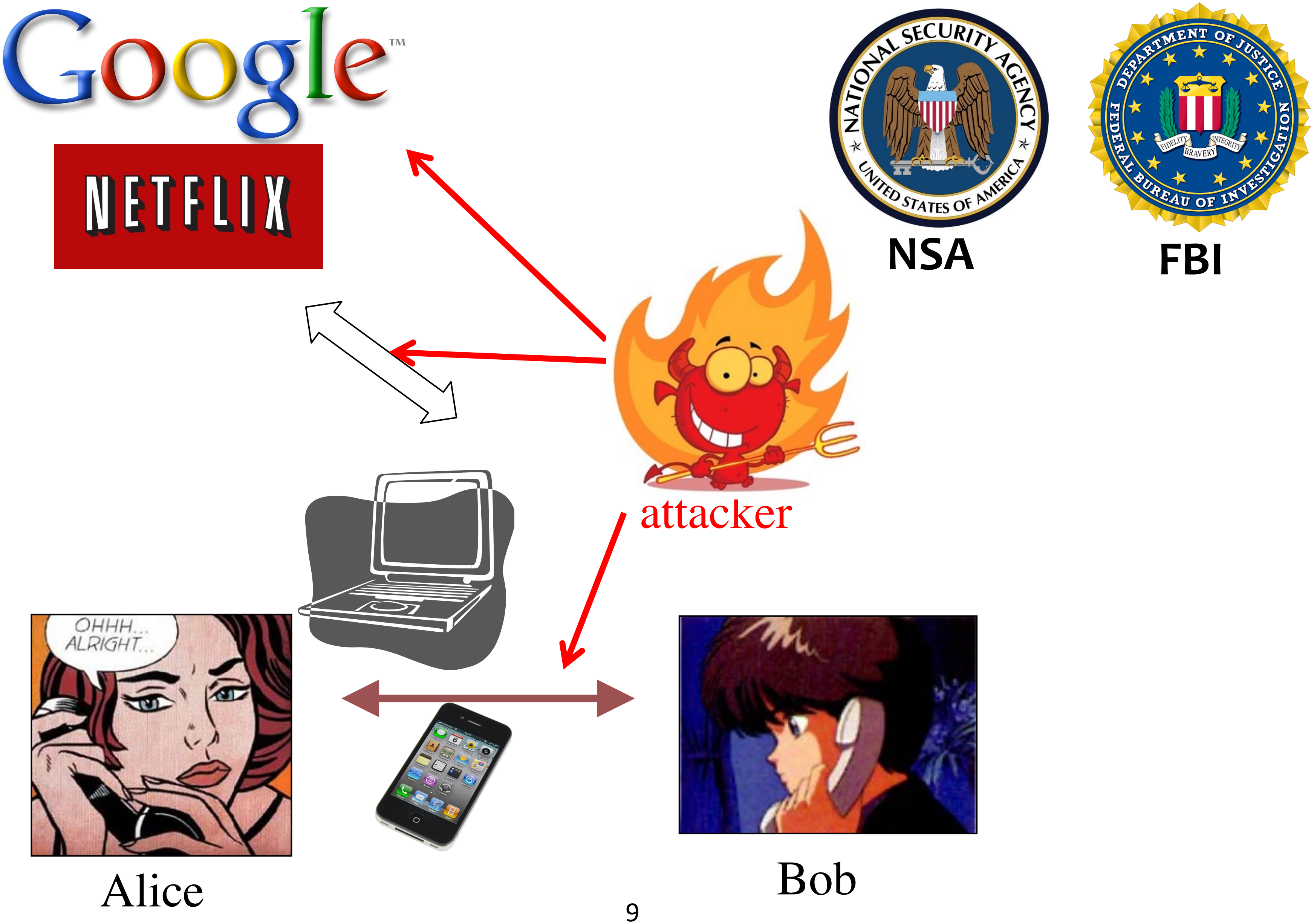
Impact on Public Policy

- **Rare, catastrophic, events have lasting impact**
  - E.g., 9/11, Fukushima nuclear accident…
- **Makes it easier for governments to pass laws**
  - Patriot Act: increase in surveillance operations
  - What's the most surprising about the recent revelations about NSA activities?
- **New twist: the prospect of a rare, catastrophic event may be sufficient**
  - Liquid ban on airplanes

Impact on Public Policy

- **Demands that government pass laws**
  - Even though they may be ineffective
  - Feeling that the government is doing something
- **Politicians are generally poor at providing social optima**
  - The socially optimum solution may actually make everybody unhappy – not a good recipe to win elections
- **Yields increased traffic surveillance + regulations**

Information Technology Policy



NSA

FBI

attacker

Alice

Bob

Information Technology Policy

Google

NETFLIX

facebook

Digital rights management policy

NSA

FBI

Data privacy policy

Government surveillance

Technology (crypto) policy

CFAA

Alice

Bob

Information Technology Policy

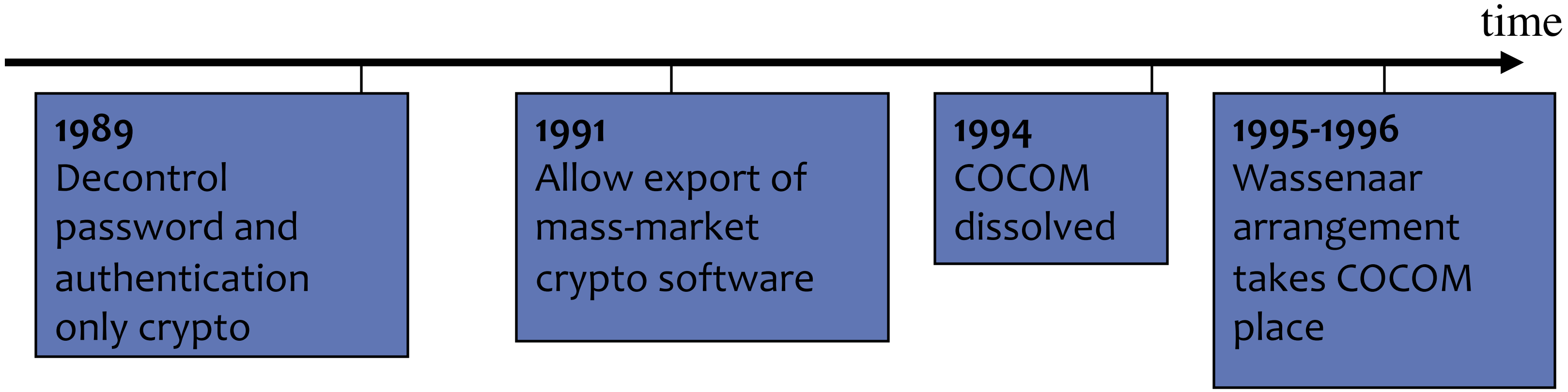
- **Crypto policy**
  - Export control
  - Domestic policy

Export Control

- **Cryptography considered as a weapon by vast majority of countries**
  - Military heritage
- **Don’t want strong crypto to fall into the hands of foreign powers**
  - Enigma (WWII) used to communicate with submarine operatives
  - “Dangerous states” (e.g., ~~Libya~~, Iraq?, Iran, North Korea)
- **Subject to laws very similar to weapons export**

COCOM

- Coordinating Committee for Multilateral Export Controls
- Large international organization for mutual control of export of strategic products from country members to proscribed destinations
- Maintained International Munitions List



1989
Decontrol password and authentication only crypto

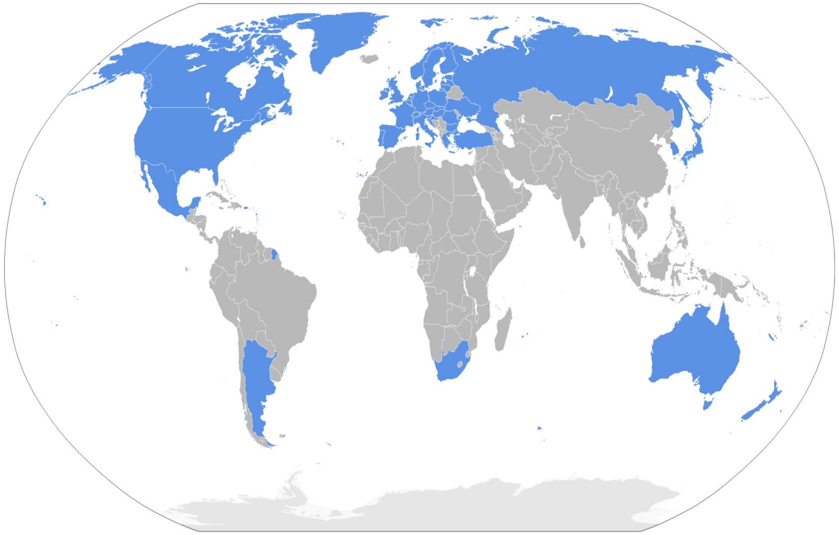
1991
Allow export of mass-market crypto software

1994
COCOM dissolved

1995-1996
Wassenaar arrangement takes COCOM place

Wassenaar

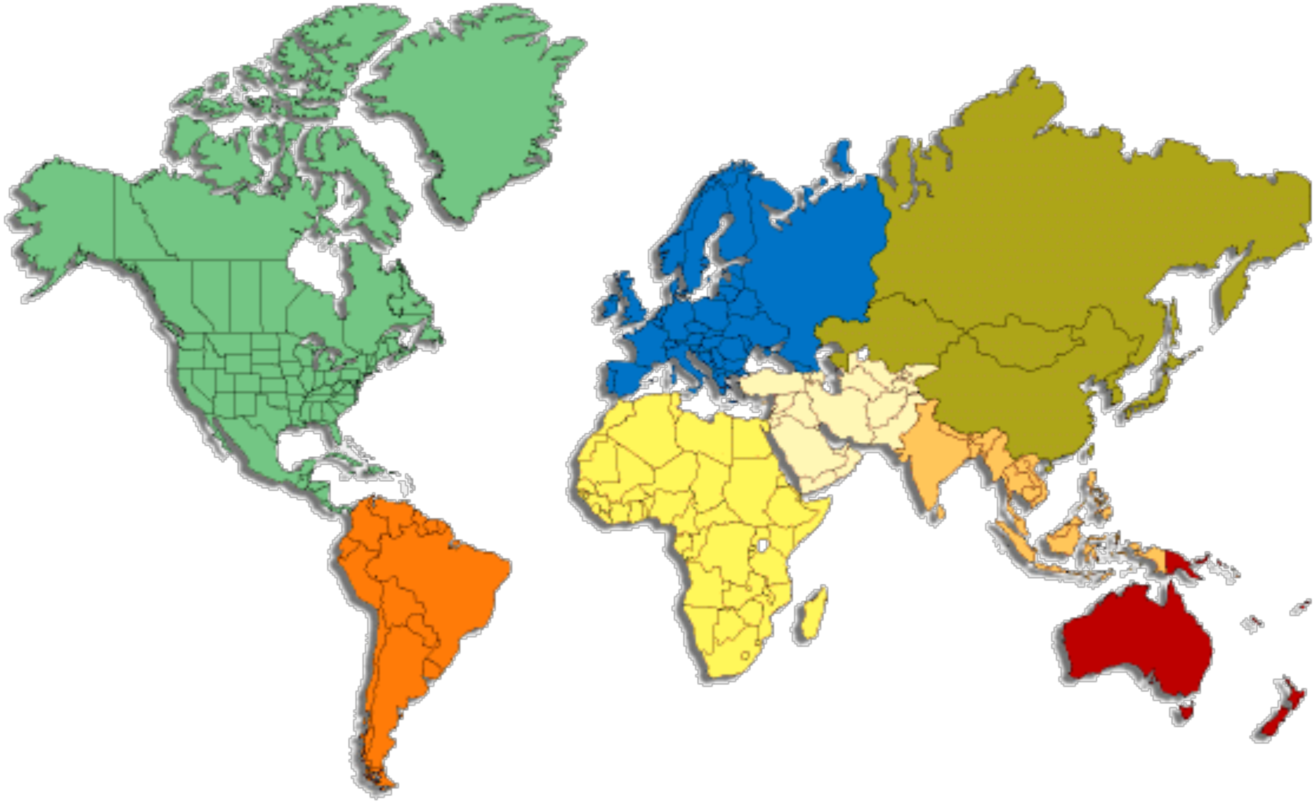
- Control export of weapons and dual use goods
- Dual use goods have both military and civilian applications
- Cryptography is a dual use good
- EU regulations also classify crypto as a dual use good



A Unified World?

Source: http://rechten.uvt.nl/koops/index.htm

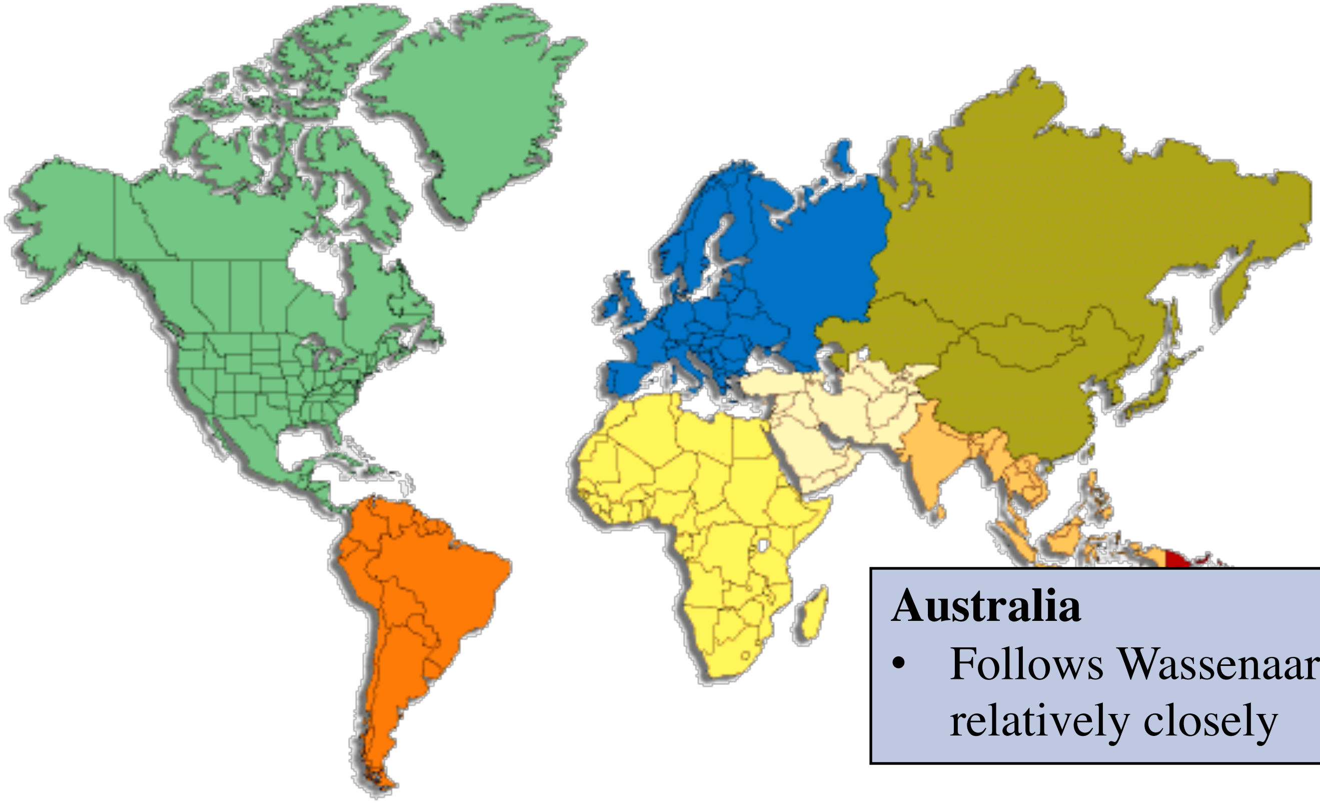
- **Countries essentially do what they want!**



A Unified World?

Source: http://rechten.uvt.nl/koops/index.htm

- **Countries essentially do what they want!**



Australia

- Follows Wassenaar relatively closely

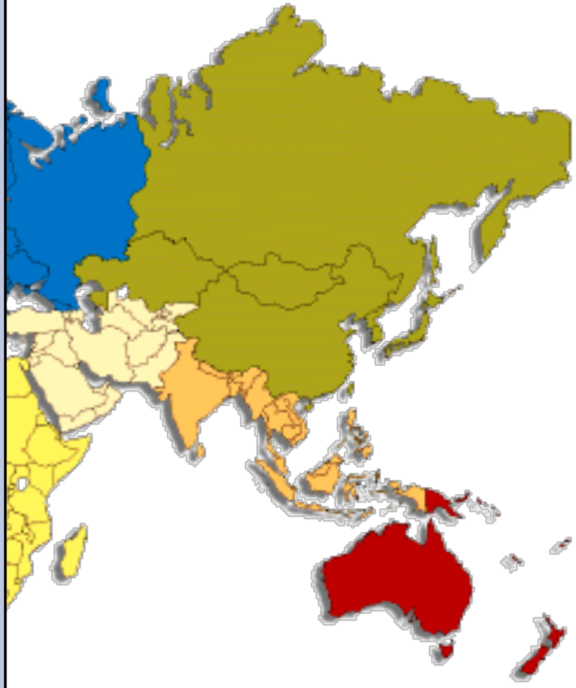
A Unified World?

Source: http://rechten.uvt.nl/koops/index.htm

- **Countries essentially do what they want!**

USA

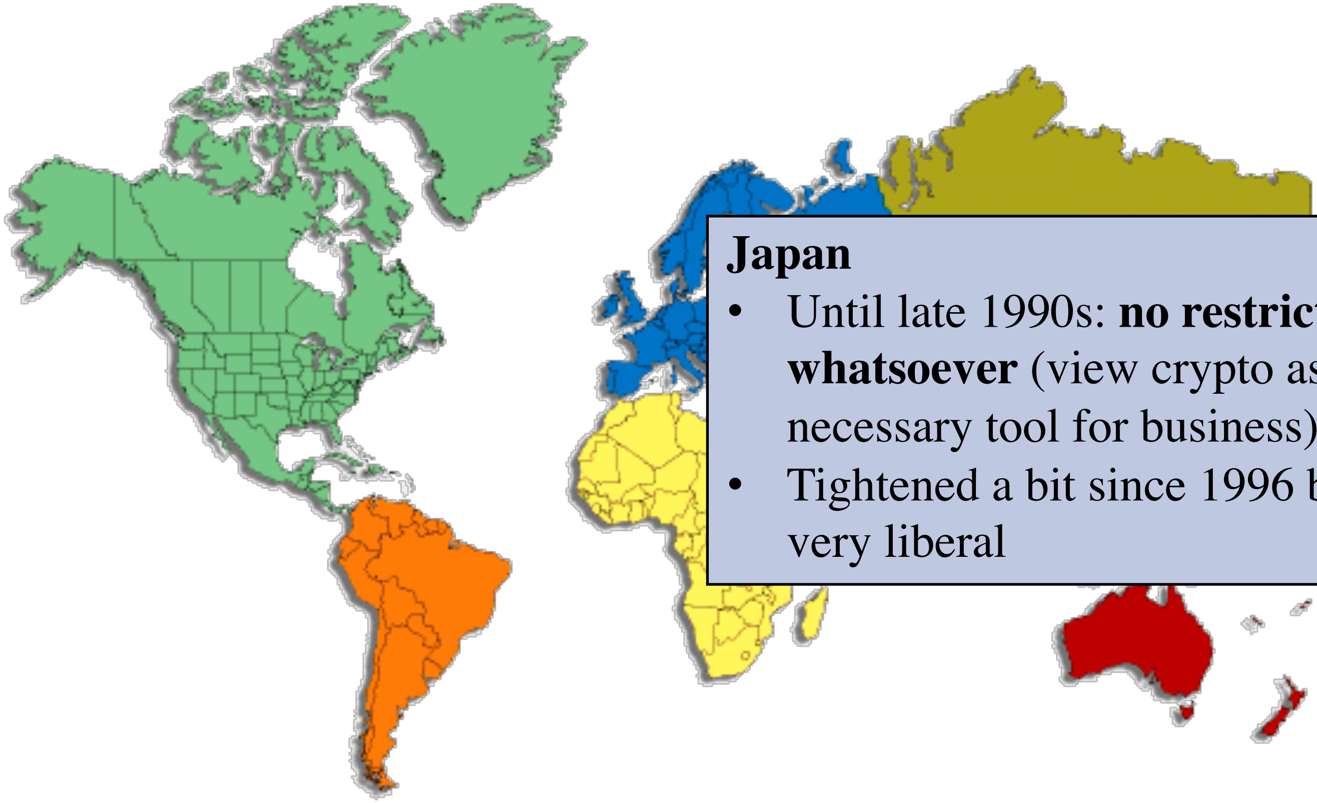
- Until 1998: used International Traffic in Arms Regulation rules for crypto (much stronger restrictions than COCOM)
- Weak (i.e., breakable) crypto can be exported
- Need export licenses for anything else…
- This is why some used to have domestic and international versions of Netscape, for instance
- One of the reasons why OpenBSD initially shipped from Canada
- Rules have been much relaxed since 1998



A Unified World?

Source: http://rechten.uvt.nl/koops/index.htm

- **Countries essentially do what they want!**



Japan

- Until late 1990s: **no restriction whatsoever** (view crypto as a necessary tool for business)
- Tightened a bit since 1996 but remains very liberal

A Unified World?

Source: http://rechten.uvt.nl/koops/index.htm

- **Countries essentially do what they want!**

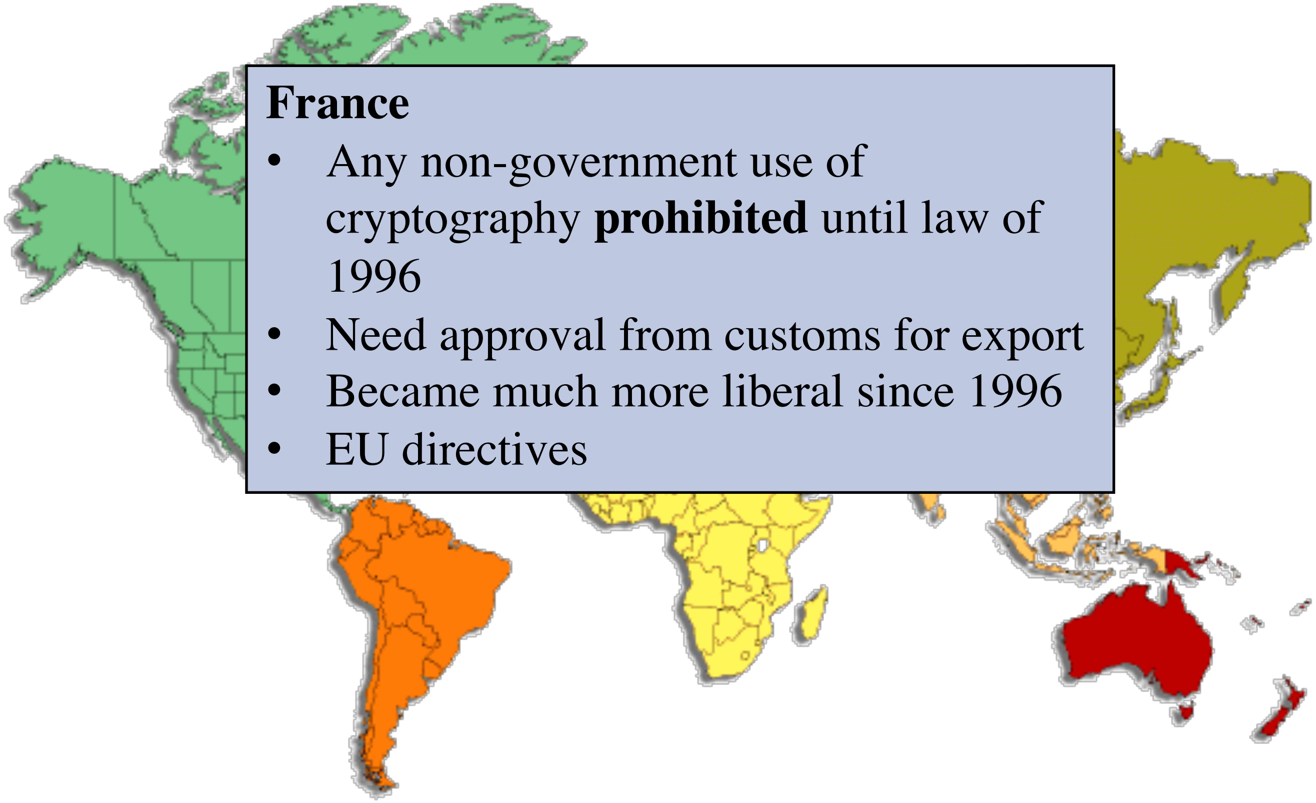
UK

- No restriction historically
- Became much stiffer in 2000 (Regulatory Investigatory Powers Act)
- All state sector keys are escrowed

A Unified World?

Source: http://rechten.uvt.nl/koops/index.htm

- **Countries essentially do what they want!**



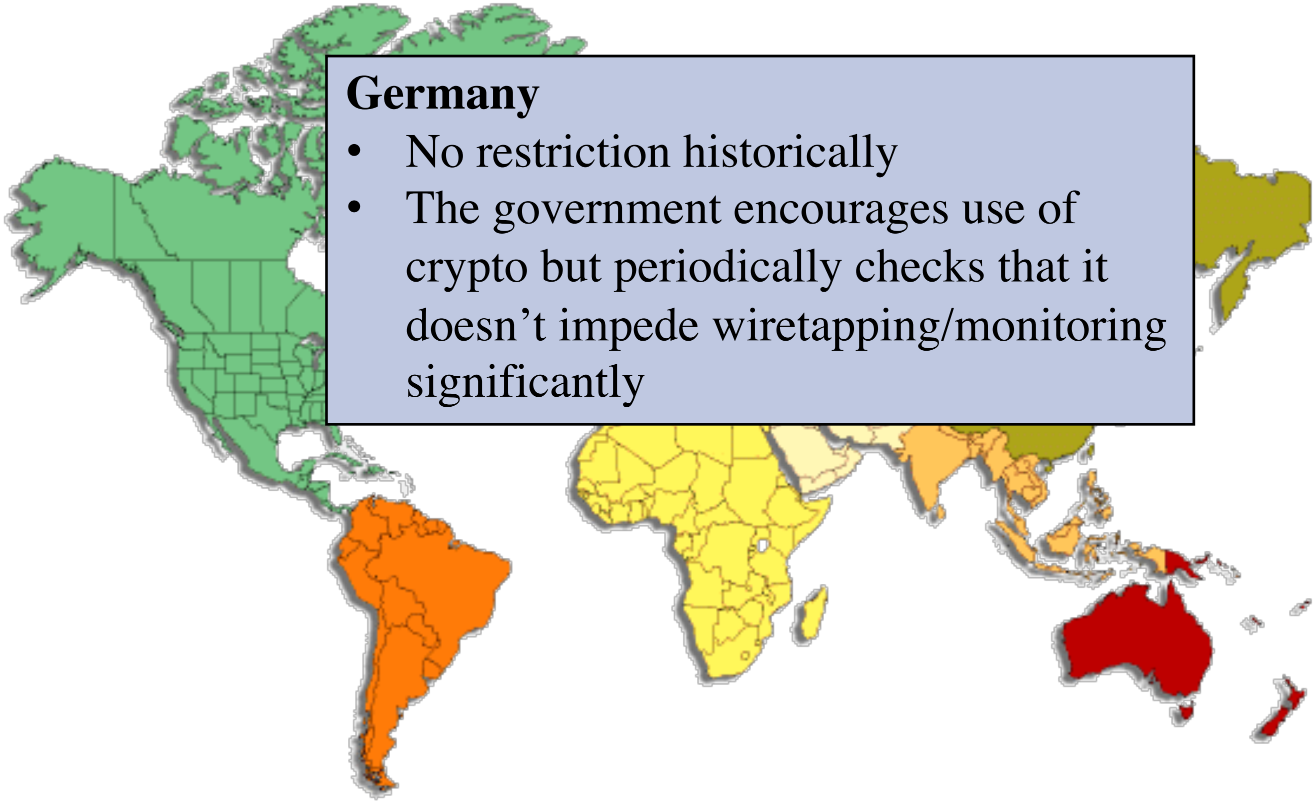
France

- Any non-government use of cryptography **prohibited** until law of 1996
- Need approval from customs for export
- Became much more liberal since 1996
- EU directives

A Unified World?

Source: http://rechten.uvt.nl/koops/index.htm

- **Countries essentially do what they want!**



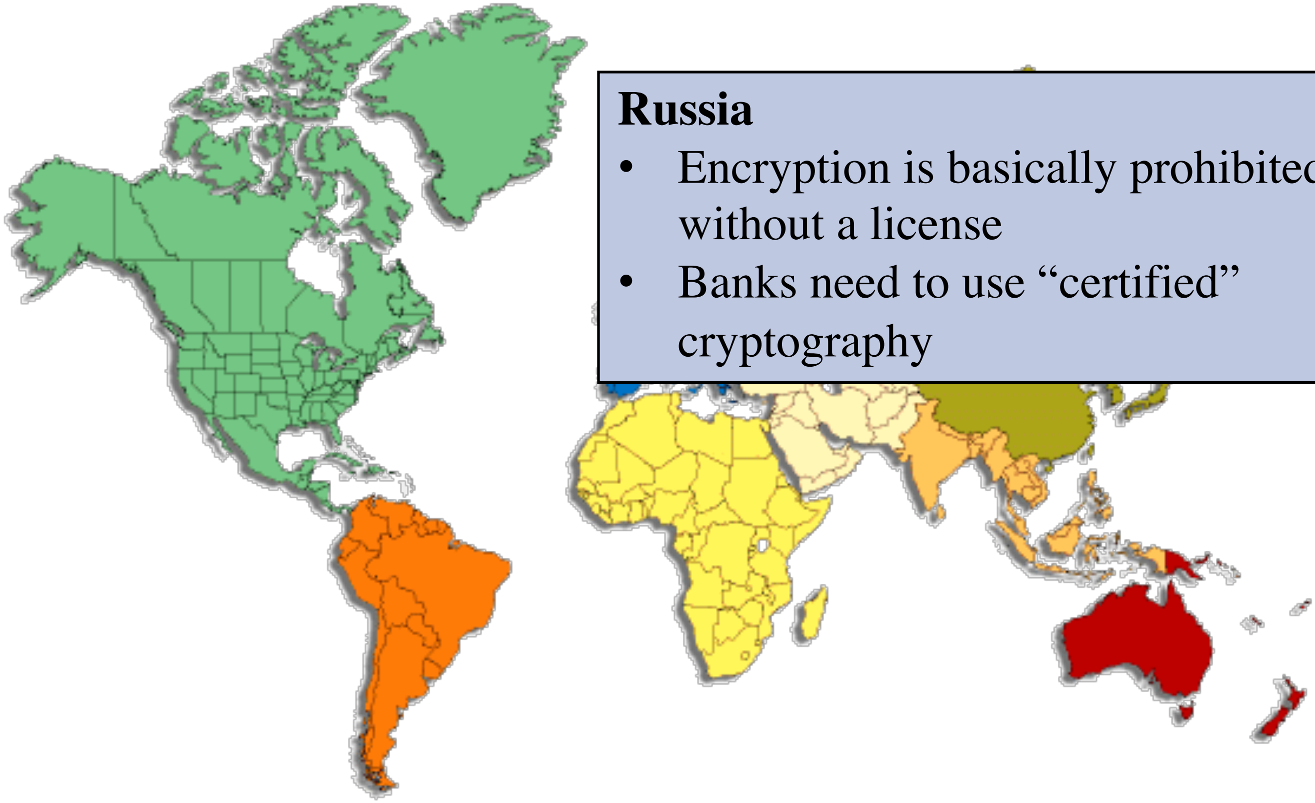
Germany

- No restriction historically
- The government encourages use of crypto but periodically checks that it doesn't impede wiretapping/monitoring significantly

A Unified World?

Source: http://rechten.uvt.nl/koops/index.htm

- **Countries essentially do what they want!**



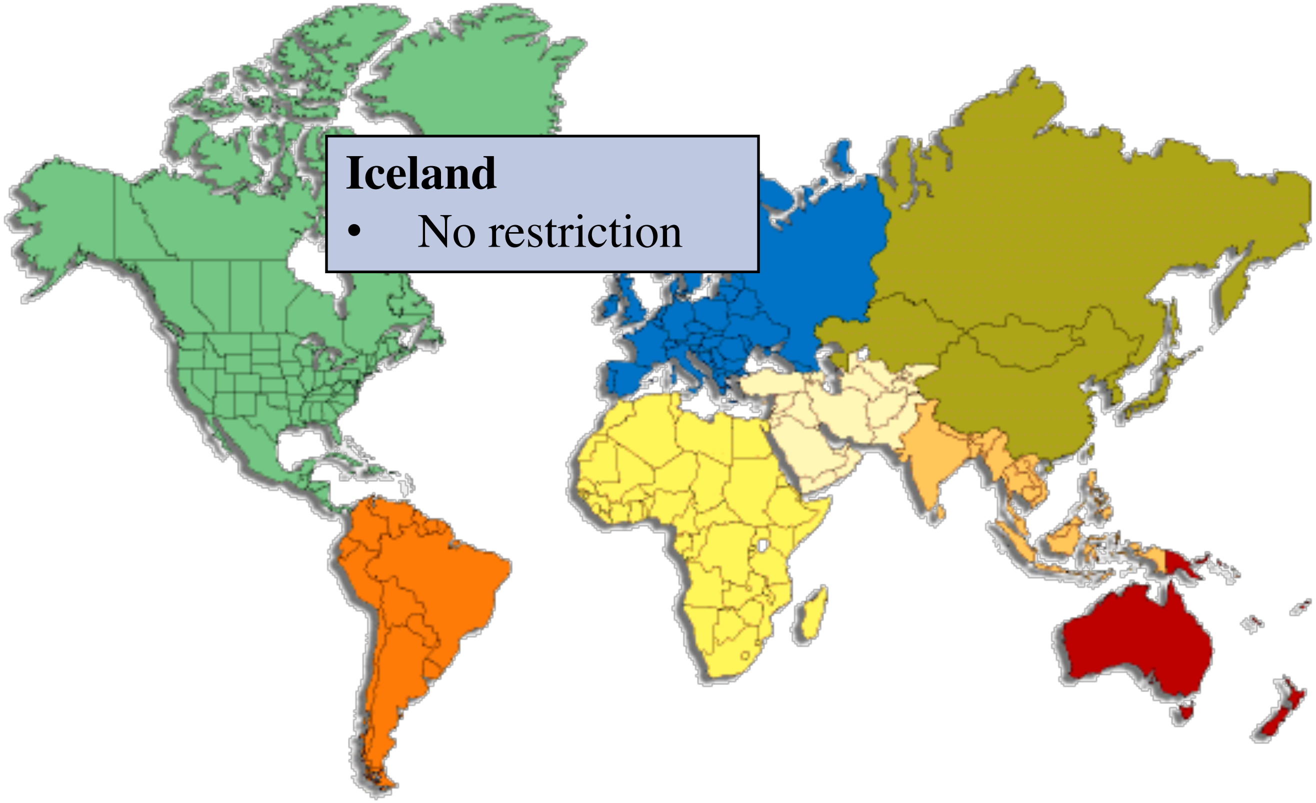
Russia

- Encryption is basically prohibited without a license
- Banks need to use “certified” cryptography

A Unified World?

Source: http://rechten.uvt.nl/koops/index.htm

- **Countries essentially do what they want!**



Iceland

- No restriction

Modifications to Wassenaar

- **Late 2013: add intrusion software to export-controlled goods**
  - The idea is to avoid export of surveillance technology to countries with history of human-rights abuse

- **How do you implement it?**

Modifications to Wassenaar

2013: added surveillance technology and intrusion software

- **Wassenaar text:**

  "Software" specially designed or modified to avoid detection by 'monitoring tools', or to defeat 'protective countermeasures', of a computer or network capable device, and performing any of the following:
  a. The extraction of data or information, from a computer or network capable device, or the modification of system or user data; or
  b. The modification of the standard execution path of a program or process in order to allow the execution of externally provided instructions.

- **BIS (US) proposal:**

  Systems, equipment, components and software specially designed for the generation, operation or delivery of, or communication with, intrusion software include network penetration testing products that use intrusion software to identify vulnerabilities of computers and network-capable devices.
  […] **Technology for the development of intrusion software includes proprietary research on the vulnerabilities and exploitation of computers and network-capable devices.**

1. **Why would governments want the addition?**
2. **Why would industry and research community strongly oppose to it?**

Cybersecurity is Leading Discussion!

What the Biden-Putin summit reveals about future of cyber attacks - and how to increase cybersecurity

Image: REUTERS/Denis Balibouse/Pool

What Does this Mean?

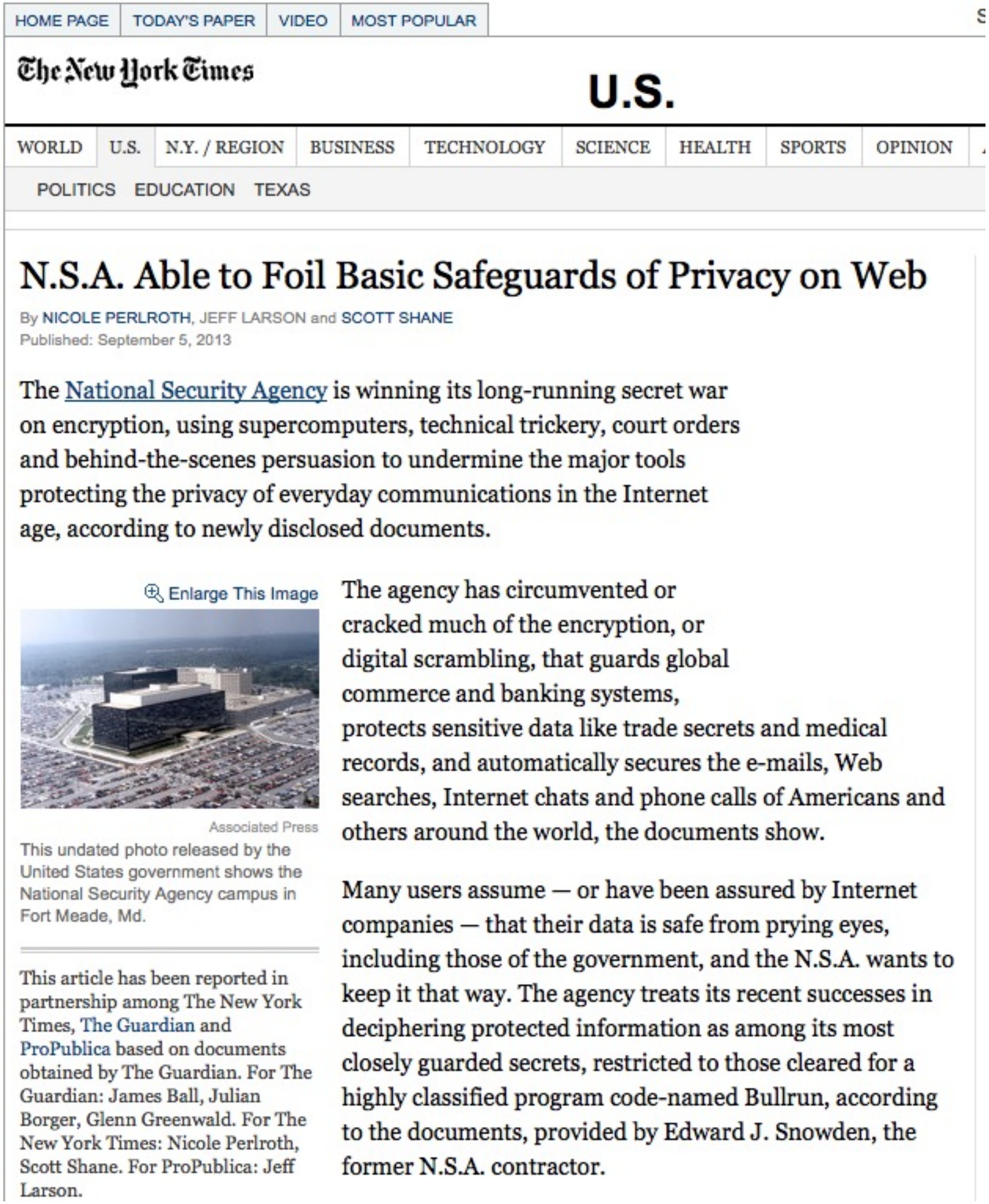
- **Is vulnerability research illegal?**
  - BIS says “no” but the text suggests “yes”

- **Are zero-days exploit exports illegal?**
  - Zero-days are only used by bad guys, right…?

- **But who develops them?**
  - What about the benevolent security researchers (a vast majority) that look for these vulnerabilities?

Cryptography Policy

- **In the US, crypto policy largely ignored by public until 1993**
- **Not much interest: mostly for military equipment and banks**
  - Did not seem to affect private citizens directly
- **Clipper chip**
  - Replacement for DES **with a backdoor** to allow government to monitor traffic
  - Goal is to make law enforcement agencies' wiretapping jobs easier
  - Civil groups and IT industry strongly opposed
  - Issue widely publicized



N.S.A. Able to Foil Basic Safeguards of Privacy on Web

By NICOLE PERLROTH, JEFF LARSON and SCOTT SHANE
Published: September 5, 2013

The National Security Agency is winning its long-running secret war on encryption, using supercomputers, technical trickery, court orders and behind-the-scenes persuasion to undermine the major tools protecting the privacy of everyday communications in the Internet age, according to newly disclosed documents.

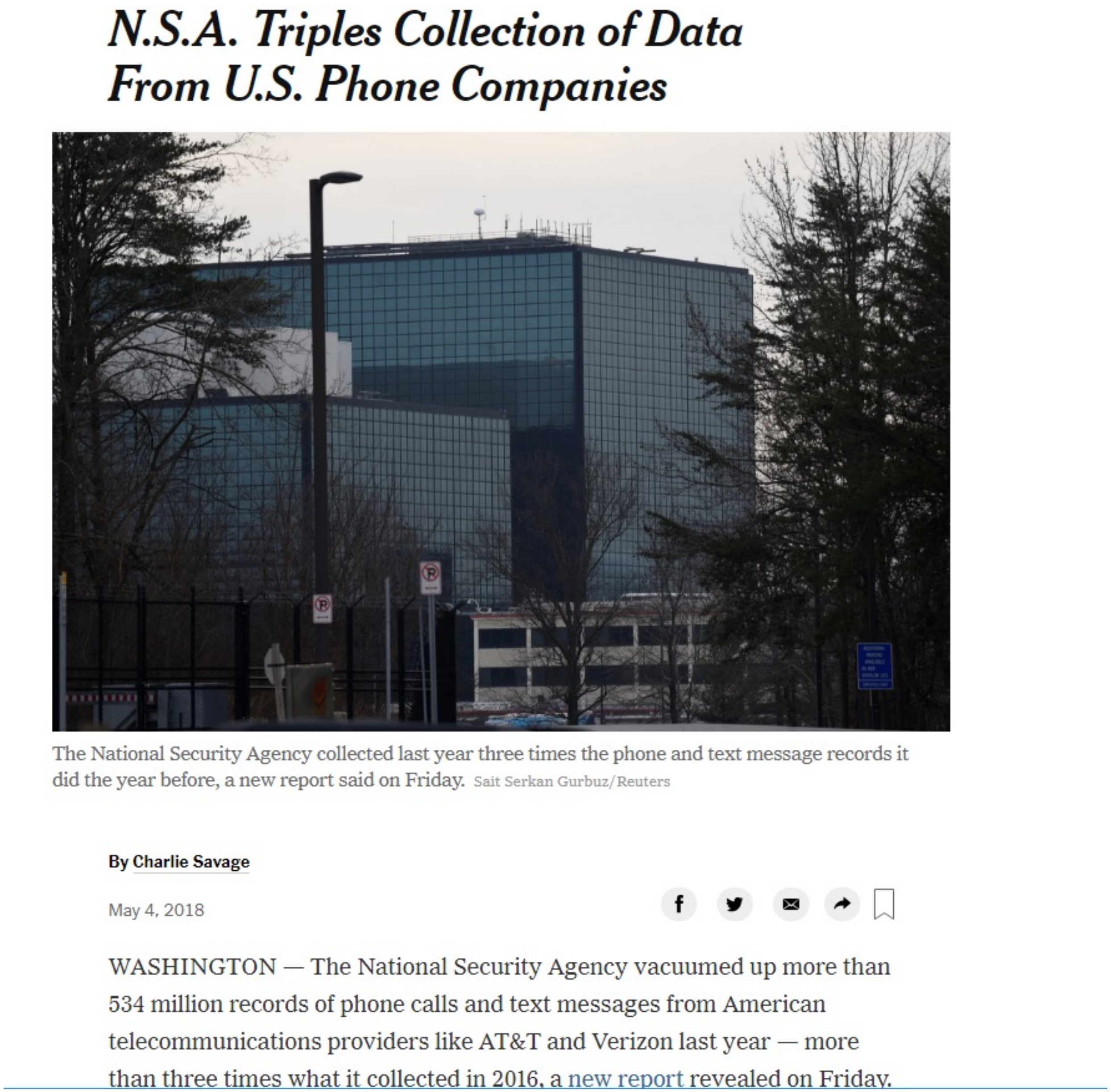
Associated Press

This undated photo released by the United States government shows the National Security Agency campus in Fort Meade, Md.

This article has been reported in partnership among The New York Times, The Guardian and ProPublica based on documents obtained by The Guardian. For The Guardian: James Ball, Julian Borger, Glenn Greenwald. For The New York Times: Nicole Perlroth, Scott Shane. For ProPublica: Jeff Larson.

The agency has circumvented or cracked much of the encryption, or digital scrambling, that guards global commerce and banking systems, protects sensitive data like trade secrets and medical records, and automatically secures the e-mails, Web searches, Internet chats and phone calls of Americans and others around the world, the documents show.

Many users assume — or have been assured by Internet companies — that their data is safe from prying eyes, including those of the government, and the N.S.A. wants to keep it that way. The agency treats its recent successes in deciphering protected information as among its most closely guarded secrets, restricted to those cleared for a highly classified program code-named Bullrun, according to the documents, provided by Edward J. Snowden, the former N.S.A. contractor.



N.S.A. Triples Collection of Data From U.S. Phone Companies

The National Security Agency collected last year three times the phone and text message records it did the year before, a new report said on Friday. Sait Serkan Gurbuz/Reuters

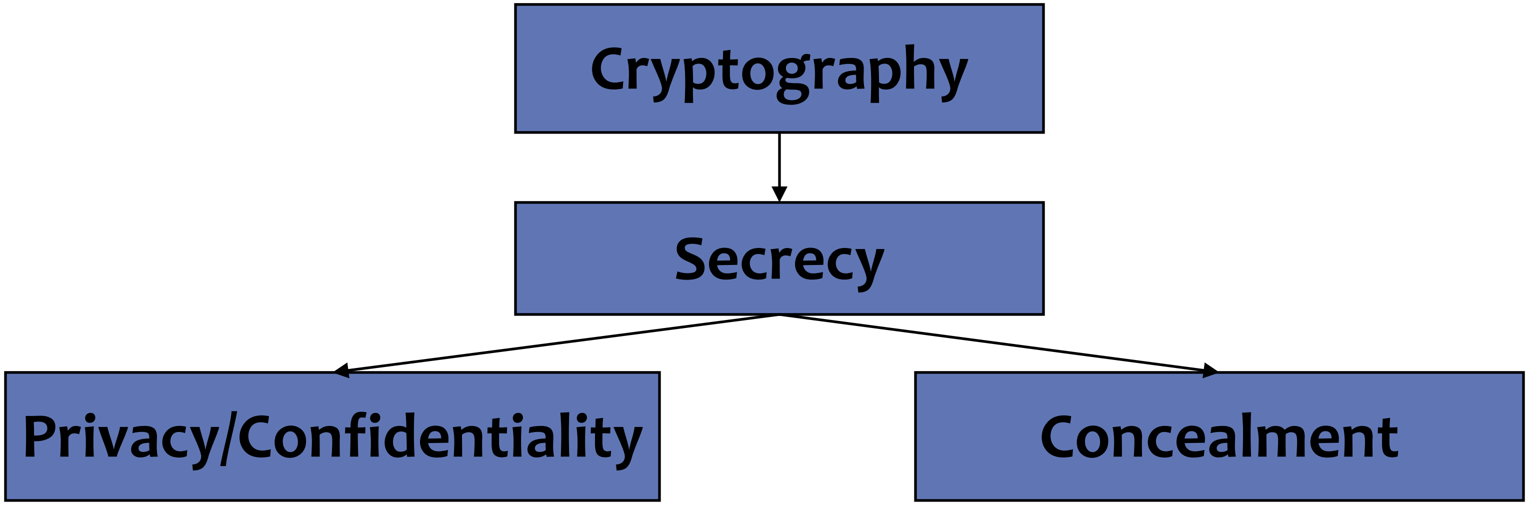
By Charlie Savage

May 4, 2018

WASHINGTON — The National Security Agency vacuumed up more than 534 million records of phone calls and text messages from American telecommunications providers like AT&T and Verizon last year — more than three times what it collected in 2016, a new report revealed on Friday.

What Are the Questions to Ask Here?

The Cryptography Dilemma



- Protection of medical records
- Banking/financial operations
- Free speech
- …

- Allows to defeat wiretaps
- Crime
- State terrorism
- …

Is there a right policy we can adopt?

Possible Solutions

- **No restrictions on crypto**
- **Prohibit civilian crypto**
- **Restrict crypto**
  - Allow weak crypto only
    - Breakable or at least thought to be breakable by government/law enforcement agencies
  - Allow licensed crypto only
    - Can enforce a full array of restrictions
    - Monitoring easier
  - Trapdoors/backdoors
    - By compromising code
    - By compromising standards
  - Key escrow

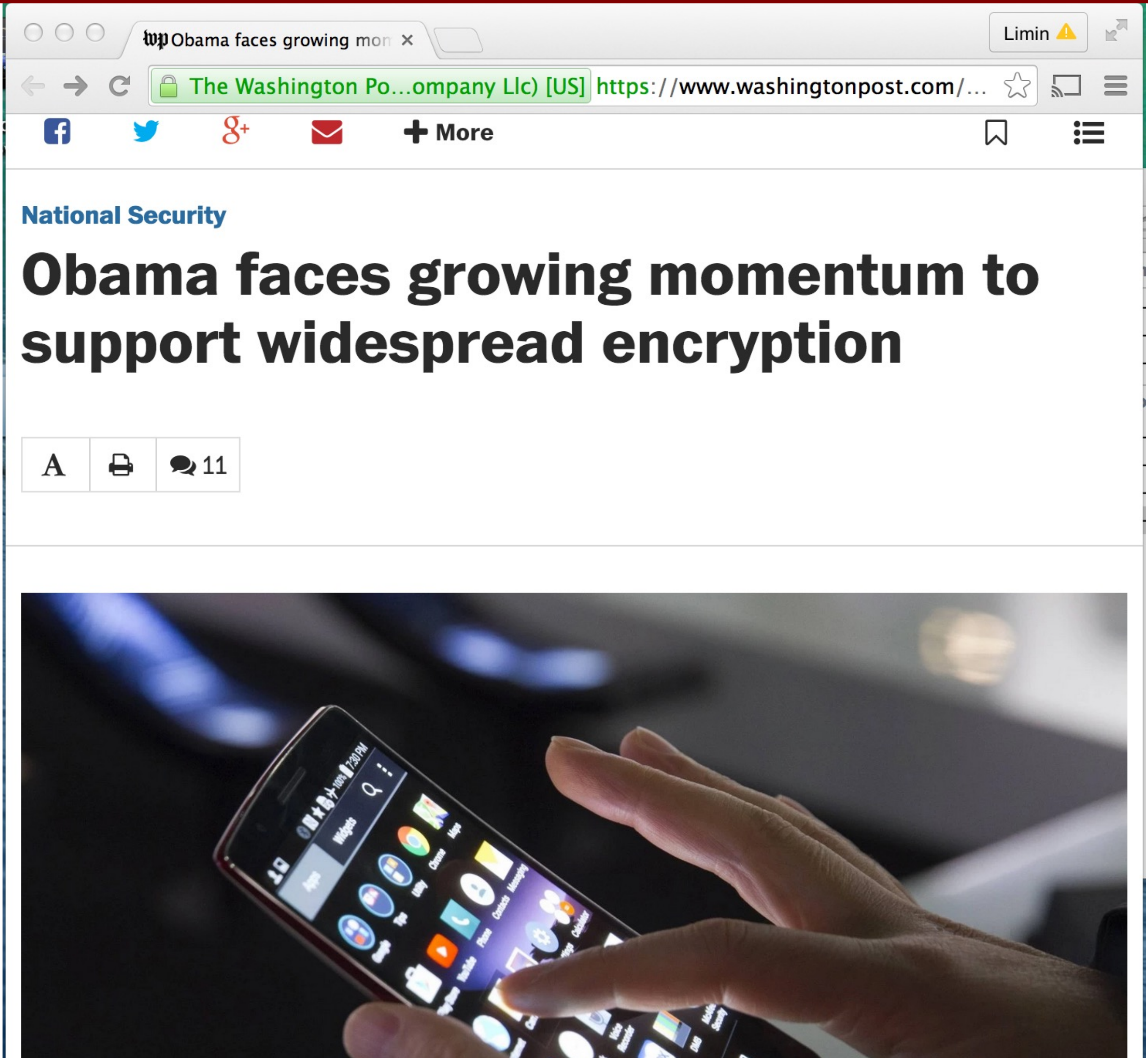
Domestic Control: Key Escrow

- A duplicate of the key should be given to the government/law enforcement agencies (also known as a “gold key” in recent debates)
- Why is this an excellent idea?
- Why is this a horrible idea?

Domestic Control: Trapdoors/Backdoors

- Mandate product to use algorithms that allow the government to decrypt using the backdoor
- Why is this an excellent idea?
- Why is this a horrible idea?

Who Won?



wp Obama faces growing mon ×
Limin
The Washington Po...ompany Llc) [US] https://www.washingtonpost.com/...
More
A
11

National Security

Obama faces growing momentum to support widespread encryption

Middle of the Road Position

- **Traditionally**
  - most crypto used for authentication rather than secrecy (with the exception of business transactions)
    - This helps law enforcement
  - Using encrypted communications can actually raise red flags that may lead the police to look for other traffic patterns!
    - Unless everybody starts using crypto…
- **Now encryption is more common**
  - Gmail uses https://
- **We don't need to be able to break the crypto to gather incriminatory evidence**

Traffic Analysis vs. Wiretapping

- **Most of the time law enforcement relies on traffic patterns rather than communication contents to seize evidence**
  - Hard to wiretap communication between Alice and Bob
    - Need order from a judge?
      - Although secret courts apparently make this a lot easier
    - Expensive?
      - But a lot less so than before for digital communications
  - Much easier to obtain phone records of Alice and Bob
    - Alice called Bob right after Charlie was murdered even though she claims she hasn’t talked to Bob in 10 years…

Traffic Analysis and Privacy

- **Even traffic analysis can raise serious privacy concerns when indicators of content is actually part of the query string**
  - http://www.google.com/search?q=ecstasy+production
  - Is this coming from a chemistry student, a political science student, …
  - … or from an aspiring drug-dealer?
- **What constitutes meta-data?**
- **If you are a chemistry student, you probably don't want to be on a watch-list just because you run that type of query…**
- **Law enforcement want URLs available**
- **Of course most citizens prefer IP address only**

Foreign Targets

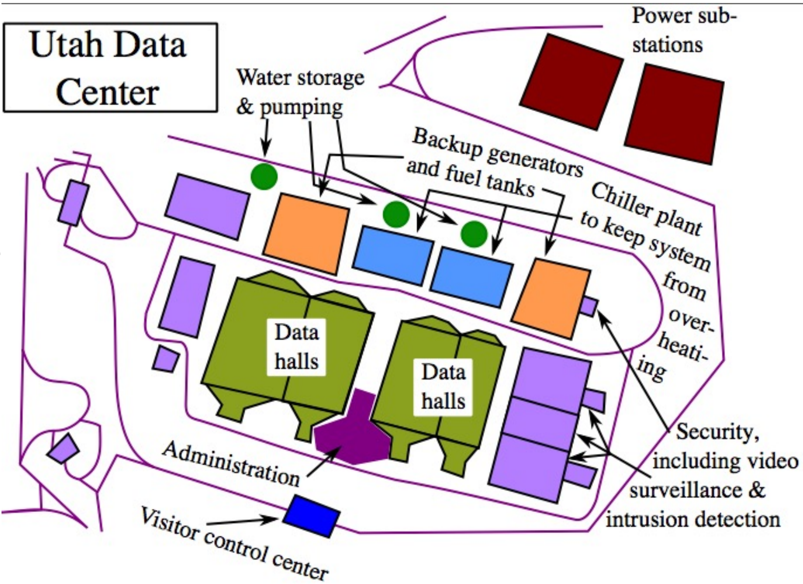
- **Traffic crosses borders**
- **Laws differ between countries**
- **Joint efforts between different countries**
  - Worldwide signal intelligence collection systems
  - “Five eyes”
  - E.g., Echelon
- **“Protect America Act”: NSA didn’t need a warrant for wiretap if one target is outside the USA or a non-US person (expired February 08)**
  - FISA amendments of 2008 renewed most provisions
- **It is near impossible to determine the citizenship of the producer on the data without eavesdropping!**
  - Location, IP address?
  - Language used?

Echelon

- Joint effort by U.S. and parts of the British Commonwealth (UK, Australia, NZ, Canada = Five Eyes)
- Created in 1960s, cold war era
- International communications (phone and data traffic) are collected
- Messages are searched for certain keywords, correlated with source/destination addresses

Difficulties

- **Too much data?**
- **Too much information?**
- **How long should it be stored?**
- **Need to sample/select traffic?**


Utah Data Center
Water storage & pumping
Power sub-stations
Backup generators and fuel tanks
Chiller plant to keep system from over-heati-ing
Data halls
Data halls
Administration
Security, including video surveillance & intrusion detection
Visitor control center

- Blurring the line between law enforcement and intelligence
  - DEA vs. NSA
  - “Parallel construction”
- Legality vs. ethics

Information Technology Policy

- Crypto policy
- Government surveillance policy
- Data privacy

Data Protection / Privacy Policy

- **Very different attitudes depending on which country you are considering!**

European Union

- Very strict privacy laws
- Can inspect, correct data
- Understand how data is processed
  - Can for instance see credit-scoring algorithms used
- Prevent data from being passed to other organizations
- Some exemptions for national security
- Now Enforcing GDPR

United States

- Very loose privacy laws
- Mostly left to self-regulation
- Major exceptions
  - Fair Credit Reporting Act allows consumers to see their credit scores
  - Video Privacy Protection Act
- Can become data haven
- Trade barriers?

Facebook/Cambridge Analytica

- **2010**
  Facebook launches Open Graph API which allows 3rd party app developers to access user data

- **2011**
  The US Federal Trade Commission and Facebook sign a consent decree: Facebook promises not to share users’ data without their permission

- **March 2018**
  News broke reports on Cambridge Analytica harvested private information from more than 50 million (turned out to be 87 million) Facebook users in developing techniques to support US President Donald Trump's 2016 election campaign, etc.

GDPR

- **European General Data Protection Regulation (GDPR) enforcement started May 25, 2018**
- **Replaces previous 1995 directive**
- **New rights for access, data collection, data processing**
- **Better data management for businesses**
  - Large companies need to document why personal data are being collected
  - Companies that do persistent surveillance need a data protection officer
- **New regime of fines**
  - Up to €20 million, or up to 4% of annual revenue
  - About 30 in year 1. Largest was €50 million for Google; behavioral ad data without proper consent structure

Information Technology Policy

- Crypto policy
- Government surveillance policy
- Data privacy
- DMCA (Digital Millennium Copyright Act)

DMCA (Digital Millennium Copyright Act)

- **Copyright law**
- **It criminalizes**
  - production and dissemination of technology, devices, or services intended to circumvent measures (commonly known as digital rights management or DRM) that control access to copyrighted works.
  - the act of circumventing an access control, whether or not there is actual infringement of copyright itself.
- **Bad idea or good idea?**

DMCA Then and Now

- **Late 1990s early 2000s**
  - Content providers like Sony believed that technology can provide absolutely secure DRM
  - Reality
    - Not hard to circumvent
    - Incentive to circumvent DRM is high
    - Sony DRM = rootkit, malware exploits and Windows crashes
- **Now**
  - Everyone agrees that technology alone **cannot** solve the problem
    - For all DRM, exists a circumvention strategy
  - DRM “works” because
    - Makes it difficult enough to avoid **easy** circumvention
    - Content is priced right, so there is not a lot of incentive to steal

Information Technology Policy

- Crypto policy
- Government surveillance policy
- Data privacy
- DMCA (Digital Millennium Copyright Act)
- CFAA (Computer Fraud and Abuse Act)

CFAA (Computer Fraud and Abuse Act)

- **Protects computers from unauthorized access**
  - trespassing
  - threats
  - damage
  - espionage,
  - being corruptly used as instruments of fraud
- **Notable cases:**
  - US vs Morris (1991)
  - US vs Bradley Manning (2010-)
  - US vs Aaron Swartz (2011)
  - MBTA vs Anderson (2008)
    - MIT students found flaws in transit card system
- **Responsible disclosure**

Evidential Issues

- **Burden of proof**
  - Who should prove their guilt or innocence?
  - Recall Anderson's paper
- **Computer forensics**
  - Generally, extremely complicated task
  - Can be done technically
    - Some of you will even become experts in the field
  - Can it be understood by laymen (i.e., judges, lawyers)?

Electronic Signatures

- **Fairly low-tech in US and UK: just putting your name at the end of a message is considered signing it**
- **Various forms of signatures: pushing button, etc**
- **EU distinguishes between electronic signatures and advanced electronic signatures**
  - The latter require digital signature (e.g., PGP signature), or biometrics…
  - Should unambiguously provide authentication and prevent forgery

Take Away Slide (1)

- **Risk perception**
  - Humans do not react “rationally” to catastrophic events
  - Impacts public policy
- **Cryptography policy**
  - Dilemma between privacy and concealment
  - Governments generally wary of crypto
    - Assimilated to weapons
  - Surveillance issues
  - Risk of blurring law enforcement and intelligence
    - Spies are not cops, and cops are not spies
  - Export control laws greatly vary depending on country
- **Privacy policy**
  - Significant differences between countries – can it be a trade barrier?

Take Away Slide (2)

- **DMCA**
  - Still restricting research, allows content provider to charge “too much”
  - “Works” in general but perhaps not because of the law itself
- **CFAA**
  - A lot of criticism for being too strict
  - Hinders research and hard to disclose flaws
- **Evidential issues**
  - Courts are still very much behind technology-wise
  - As an expert, need to have a foolproof case and ability to introduce evidence in lay terms