Going Dark

Implications of an Encrypted World

Abraham Wagner and Sophia d'Antoine

July 23, 2019

Overview

- Solving the cybersecurity problem
- A new paradigm for user demand
- Encryption technology – old and new
- Privacy and a changing legal regime
- Technical solutions
- Policy implications

Solving the Cybersecurity Problem

- **The problem will be solved**
- **Users are demanding it**
- **Low-cost technical solutions can be implemented**
  - *Marginal cost to users will be zero*
- **Deal with known and evolving vulnerabilities**
- **Most solutions involve encryption**
  - *Ongoing debate over impact*

New Paradigm – Users No Longer Control their Data

- **Old analog world – data in physical form**
  - *Traditional security and privacy worked*
  - *Paper and plastic could be locked up*
- **Digital world – data no longer in physical form**
  - *Much "personal data" in digital form on many systems*
  - *Users not in control of servers and systems*
  - *Simply don't have any choice*

Transition to the Digital World

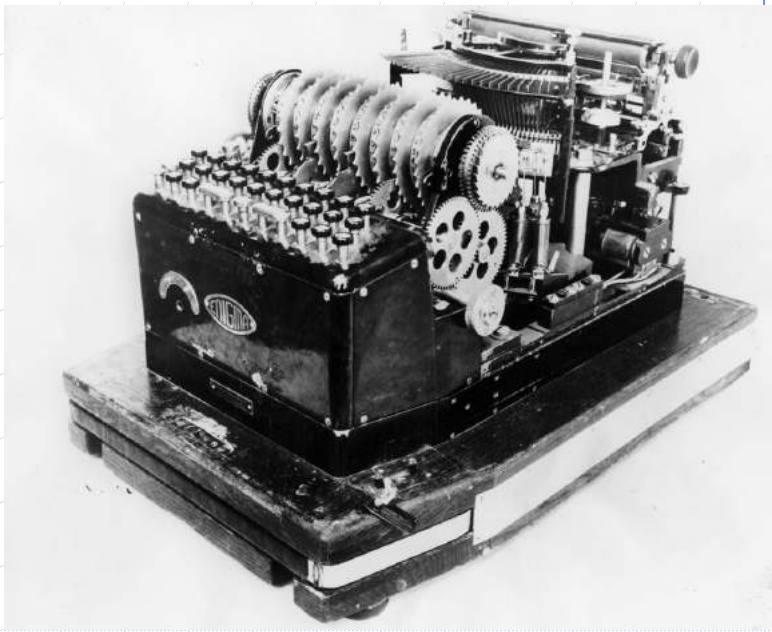
- **Users have lost control of their data**
- **Communications and data storage are highly vulnerable**
- **Users now include criminals and terrorists**
- **Publicity surrounding hacks and government surveillance**
  - *Increasing demand for privacy and encryption*

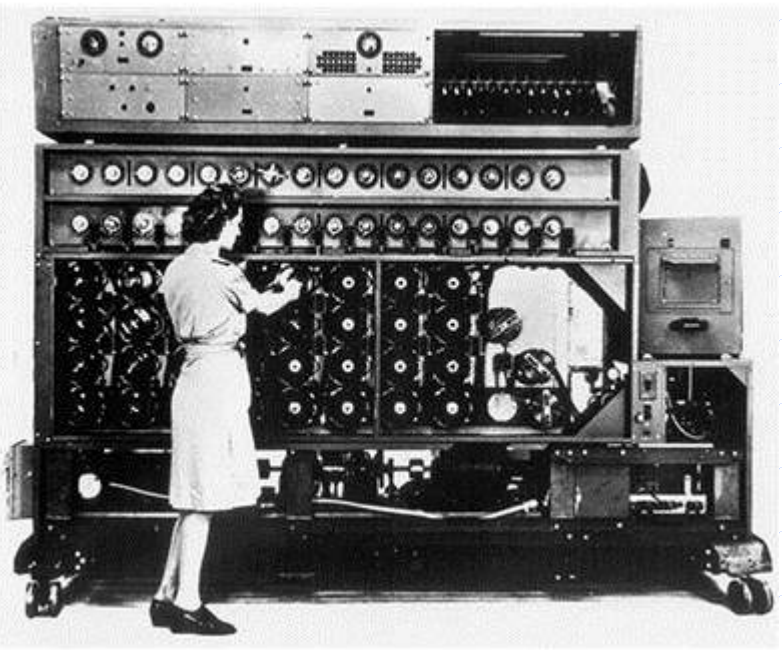
Encryption is Now all in Software

- **No costly electromechanical devices or chips**
- **All devices contain powerful processors**
- **High grade algorithms readily available**
  - *Cannot be controlled by government any more*
- **Marginal cost to users is zero**
  - *Will be essential feature in all new applications*

The Old World –

Devices like the Enigma were costly electromechanical ones which nobody wanted to buy





German ENIGMA

Current Debate – Is the World Really "Going Dark"?

- **Encryption is a two-edged sword**
- **Needed levels of privacy and security**
- **Challenge for intelligence and law enforcement**
  - *Legal controls are no longer viable*
  - *Technical "solutions" over the long term?*
- **Ongoing debate on key issues**

Going Dark Time Horizon

	Current	18 months	5 years	10 years
Devices and Processors	Smartphones to servers with powerful processors	Smartphones to servers with more powerful processors	Next generation PDs, servers with more powerful processors	Next generation PDs, servers with more powerful processors
Encryption Algorithms	3X-DES, RSA-1024, Blowfish, Twofish, AES	QKD, ID Quantique	Honey encryption; quantum key	Honey encryption; quantum key; others
Keys and Distribution	DES; RSA	QKD, ID Quantique	Quantum key	Quantum key; others
Application Software				
User Demands				
Legal Regime	No controls on algorithms and keys Titles 10, 50, and 18	No controls on algorithms and keys Titles 10, 50, and 18	New USC, useless O/CONUS	New USC, useless O/CONUS
Technical Access	TAO ? FBI - limited/poor	TAO ? FBI - limited/poor	TAO ? FBI - poor to none	TAO - none FBI - none

Background – The ARPAnet and Security

ARPAnet – The Early Days

- **Experiment in switched-packed communications**
  - *Technology for network optimization*
  - *Alternative to traditional line switching*
- **Limited to ARPA (now DARPA), contractors and others connected to DoD and NSF**
  - *ARPA contractors and universities working with ARPA*
  - *DoD and military services*
  - *COINS system at NSA*
- **No e-mail, web, browsers or content**
  - *Ray Tomlinson (BBN) did e-mail protocol (SMTP) on his own*
  - *HTTP not developed until 1991; Browser in 1992*
- **Connecting to the net was difficult and costly**
  - *Initially required 56kb leased-line hard wired into net*
  - *Dial-up modems were very slow (300 baud) and few ports*

Why the Paradigm Shift?

- **Moore's Law – Cheap computers for everybody**
  - *Named after Gordon Moore – inventor of the integrated circuit*
  - *Increasingly cheap and powerful integrated circuits (chips)*
    - Era of "free" hardware
- **Packet switching – Demonstrated by the ARPAnet**
  - *Largest media revolution since moveable type*
- **Digital everything**
  - *Data, voice, video, etc. – whatever "it" is, it is digital*
- **Infinite/cheap bandwidth**
  - *Landline and RF available cheaply worldwide*

Early ARPAnet

- **Only nodes were mainframe computers**
  - *University, contractor and government research centers*
  - *Users largely scientists at mainframe consoles*
- **Connectivity was only by leased lines**
  - *56 Kb, later upgraded to T1 (1.54 Mb)*
  - *No LANS, WANS or modems in the early years*
- **Assumptions about computing were wrong**
  - *"Future" would be a few supercomputers with users connected by "dumb" terminals*
  - *Applications software and data would be connected via the net*
- **ARPAnet not designed to survive nuclear war**
  - *Survivability is an attribute of the net – not a reason for it*

Cybersecurity Not an Issue

- **No way to access or hack the net**
  - *Mainframe computers on leased lines*
- **Nothing to steal on the net**
  - *Virtually no content*
  - *No e-commerce, banks, etc. in the early years*
- **Nothing connected to the net**
  - *No SCADA or other systems*
- **Net was not a mass communications medium**
  - *Limited e-mail; no web; little content*
- **Denial of service attack largely impossible**
  - *Need to cut leased line or destroy IMPs*
- **ARPA tried "breaking" the net to test software**
  - *Software engineers then fixed the buggy code*

The Digital Revolution

- **For most of history the world was analog**
  - *Media were paper, parchment, plastic, wood, etc.*
  - *Magnetic media (tape) was also analog*
  - *Communications were largely analog*
  - *Analog-digital conversion was complex/costly*
- **The world goes digital**
  - *Documents created on computers as digital files*
  - *Entertainment – CDs, DVDs, images, video etc. all digital*
  - *Conversion of analog media to digital*
- **Media are also free or nearly free**
  - *Most Internet media are free or cheap*
  - *First time in recorded history*
  - *Physical media are rapidly vanishing – find a "record store"*

Content Comes to Cyberspace

- **Hosts and servers connected to the net**
  - *Business, government, legal system, military, medical, etc.*
  - *Paper files transition to digital files*
- **E-commerce emerges**
  - *On-line marketing of traditional products*
  - *New goods and services*
- **Vast array of other media come on-line**
  - *Web sites of every type imaginable*
  - *Adjuncts to broadcast and print media (e.g., CNN.com)*
  - *Audio and video now as digital files to download*
- **Communications and social interaction**
  - *Social networking (SAS) – (Facebook, Twitter, etc.)*
  - *Dating sites now lead all other methods*
  - *Games and other new types of media*

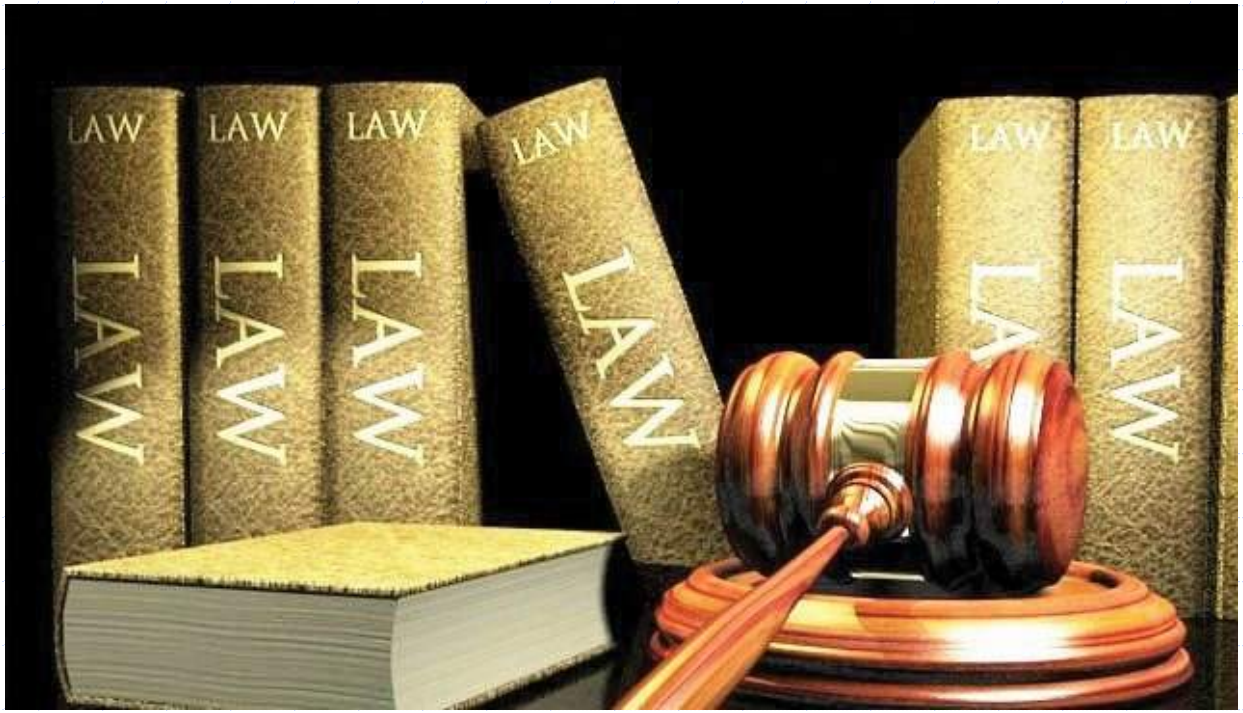
Cybersecurity Becomes an Issue

- **Expansion of the net – now stuff to steal**
  - *Users to annoy and potential for real damage*
  - *Now possible for hackers and others to access net*
- **Uninformed policy and missed opportunities**
  - *1990s were largely a lost decade*
    - Network exploded and never adequately secured
  - *USG programs were minimal, underfunded or killed*
- **Cyberspace not treated as a national resource**
  - *Everybody through it was somebody else's job to fix it*
  - *Policies failed to promote security effective development*
  - *Commercial firms not integrated with government agencies*
- **U.S. Government – "the pig at the trough"**
  - *Military, IC and others became massive net users*
  - *Funding, R&D for security was trivial, at best*

Demands for Privacy and Security

- **Privacy and security – overlapping concepts**
  - *Fourth Amendment to U.S. Constitution; Federalist Papers*
  - *Protected rights for individuals; commercial entities*
  - *Legal domain is rapidly evolving in this area*
- **Expectations changed as net evolved**
  - *User base greatly expanded*
  - *Far more "computer literate" and savvy*
  - *More on-line to protect*
- **Demands for actual security**
  - *Banks and other commercial enterprises*
  - *Government needs for "secure" systems*
  - *Media disclosures post-Snowden*
  - *New era for FISA and other legal issues*

The Legal Regime



Elements of The Legal Regime

- **Constitution and statutes**
  - *Constitution – Articles 1, 2, 3, 4 and 5*
  - *National Security Act (1947); HSA (2002); IRTPA (2004)*
  - *ECPA (1986), FISA (1979, FAA (2008), and others*
- **Executive Orders and Presidential Directives**
  - *E.O. 12333 and others*
- **Agency directives (DoD, NSA, DCI, DNI)**
  - *USSID 18 and others*
- **Case law**
  - *Electronic surveillance*
  - *Other privacy cases – almost all related to drugs*
  - *Encryption technology cases*

Constitutional Powers for National Security and Surveillance

- **Congress**

"provide for the common Defense
Art I § 8 Cl. 1

"declare War, grant letter of Marque and Reprisal, and make rules concerning Capture on Land and Water
Art I § 8 Cl. 11

"To raise and support Armies

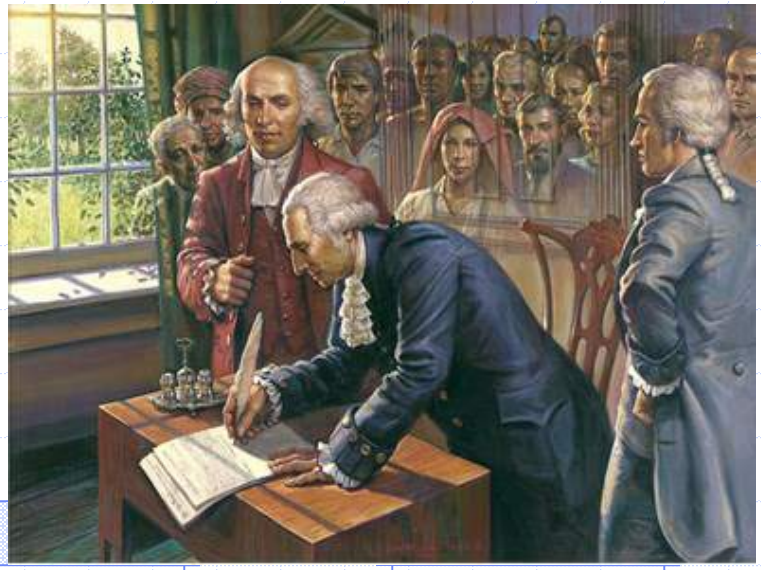
"To provide and maintain a Navy
Art I § 8 Cl. 12-13

"To declare War
Art I § 8 Cl. 1

- **President**

"tak[ing] Care that the Laws [are] faithfully executed
Art II § 3

"Serve as the Commander-in-Chief of the Army and Navy
Art II § 3 Cl. 1



We the People

of the United States

The Fourth Amendment

"The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."

What were the Founders thinking?

The Constitution, Intelligence and Electronic Surveillance

- **Articles I and II of the Constitution**
  - *Intelligence is not an enumerated power of Congress (Art. I)*
  - *Not mentioned as a Presidential responsibility (Art. II)*
  - *Clear framers didn't intend to leave it to the states*
- **Domain of both foreign affairs and war powers**
  - *Both areas inhabited by the President and Congress*
- **Steel Seizure Case,**
  Youngtown Sheet & Tube v. Sawyer, (1952)
  - *Courts can decide extent of Presidential authority in national security matters*
  - *Supreme Court declared Truman action unconstitutional*

Security, Surveillance and Privacy

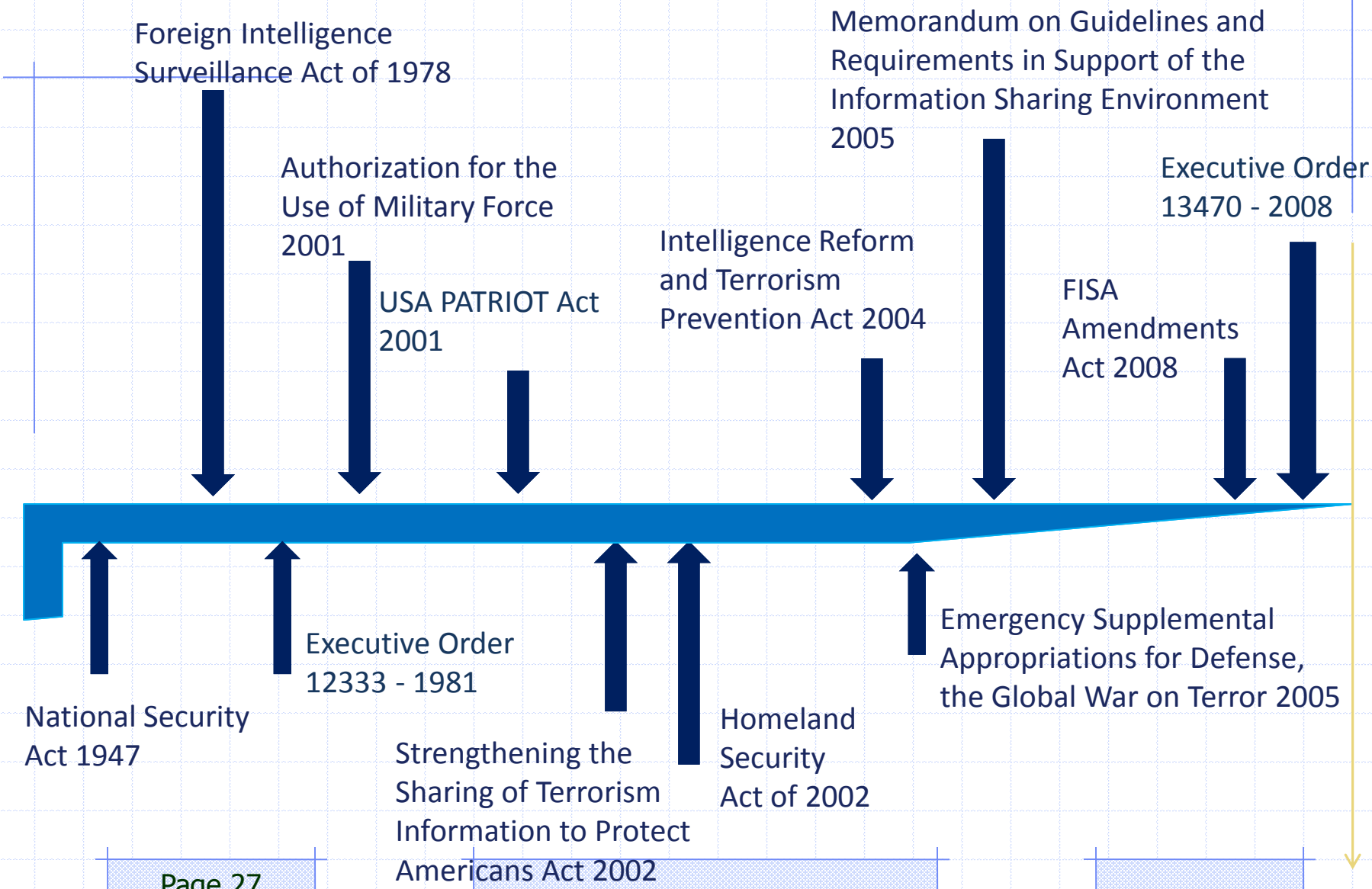
- **Constitution says little about national security and nothing about intelligence**
- **First Amendment**
  - *Freedom of speech – possible "chilling effect" of surveillance*
    - "Big Brother" is listening. . .
- **Fourth Amendment**
  - *Constitutional "Right to Privacy"*

    "The right of the people to be secure in their persons, houses, papers and effects, against unreasonable searches and seizures shall not be violated . . ."
  - *Nothing about communications or technology*
  - *Telegraph was still 50 years away; phone was 100 years off*

Federal Statutes

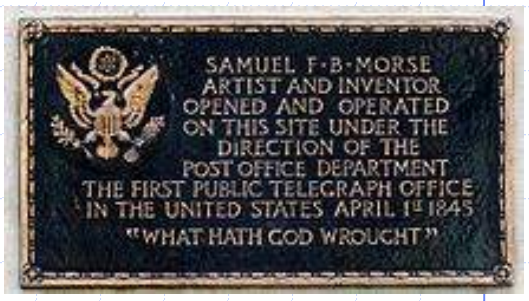
- **Electronic Communications Privacy Act of 1986 (ECPA)**
- **Foreign Intelligence Surveillance Act (1978)(FISA)**
  - *Freedom of speech – possible "chilling effect" of surveillance*
- **Homeland Security Act (2002)**
  - *Established Department of Homeland Security*
- **Intelligence Reform and Terrorism Protection Act (IRTPA) (2004)**
  - *Reorganization of the Intelligence Community*
  - *Added some domestic authority*
- **FISA Amendments Act (2008)**
  - *Constitutional "Right to Privacy"*

Evolution of Intelligence Law

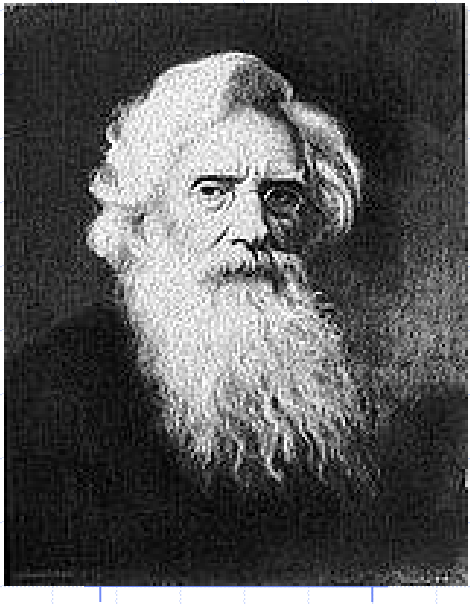


Surveillance and The Law

In the beginning. . .



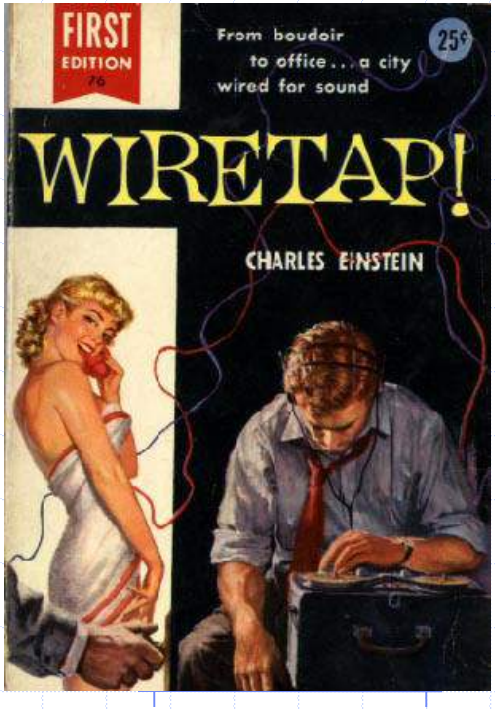
- **Morse invents the telegraph – 1835**
  - *USG funds demonstration (Washington – Baltimore) - $30K*
    - Message "What hath God Wrought" (24 May 1844)
  - *Successful, but USG decides telegraph is of no use*
- **Telegraph grew with the railroads**
  - *Dispatching of trains – 1851*
  - *Transcontinental service – Western Union 1861*
    - Used railroad right-of way
    - Railway offices were "dual use"
- **Intercept invented by criminals**
  - *Tapped telegraph lines*
    - Looking for data on trains with valuables
    - Don't waste time robbing the wrong trains



Samuel F.B. Morse

Early Days – Pre Katz

- **Electronic intercept not covered by the Fourth Amendment**
  - *Olmstead v. United States, (1928)*
    - Chief Justice Taft decision; Brandeis dissent
  - *No reasonable expectation of privacy when using a phone*
  - *No real case law prior to Olmstead*



Olmstead v. United States (1928)

- **Electronic intercept not covered by Fourth Amendment right to privacy**
  - *No reasonable expectation of privacy when using a phone*
  - *No real case law prior to Olmstead*
- **Chief Justice Taft decision; Brandeis dissent**

Chief Justice William Howard Taft

Associate Justice Lewis Brandeis

Katz v. United States (1967)

- **Olmstead reversed - Fourth Amendment right to privacy protects electronic communications**
  - *Majority opinion by J . Stewart ; Dissent by J. Black*
    - Eavesdropping goes back to ancient times and Framers were certainly aware of it; Could have prohibited this activity but didn't want to
  - *Concurring opinion by J. Harlan – 2 prong test*
    - Is there a reasonable expectation of privacy?
    - Does society recognize this as a reasonable expectation?
- **Concept of person vs. place**
  - *Fourth Amendment follows the person, not the place*
  - *Warrant required for intercept of communication*
- **Katz remains prevailing law in privacy area**

Other Major Privacy Cases

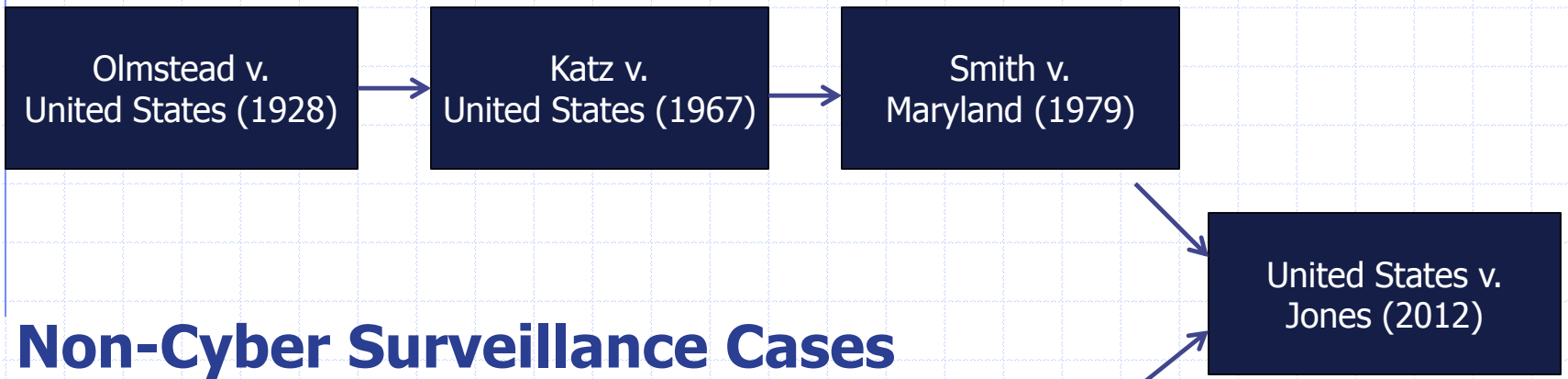
- **Smith v. Maryland (1979)**
  - *"Pen register" data not covered by Fourth Amendment*
    - Pen registers [now metadata] do not acquire the contents of a conversation or even tell if a conversation took place
  - *Critical concept of subjective expectation of privacy*
    - Show that the person wants it private, and
    - Society recognizes this expectation as reasonable
- **United States v. Jones (2012)**
  - *J. Scalia opinion extends Katz to GPS device on car*
    - Violated "reasonable expectation of privacy"
  - *J. Alito statement during oral argument:*
    - "[p]eople's use of technology is changing what the expectation of privacy is for the courts.. .I don't know what society expects and I think it's changing. Technology is changing people's expectations of privacy. Suppose we look forward 10 years, and maybe 10 years from now 90 percent of the population will be using social networking sites . . .through the use of their cell phones. Then — what would the expectation of privacy be then?"[

Recent Battle on Metadata

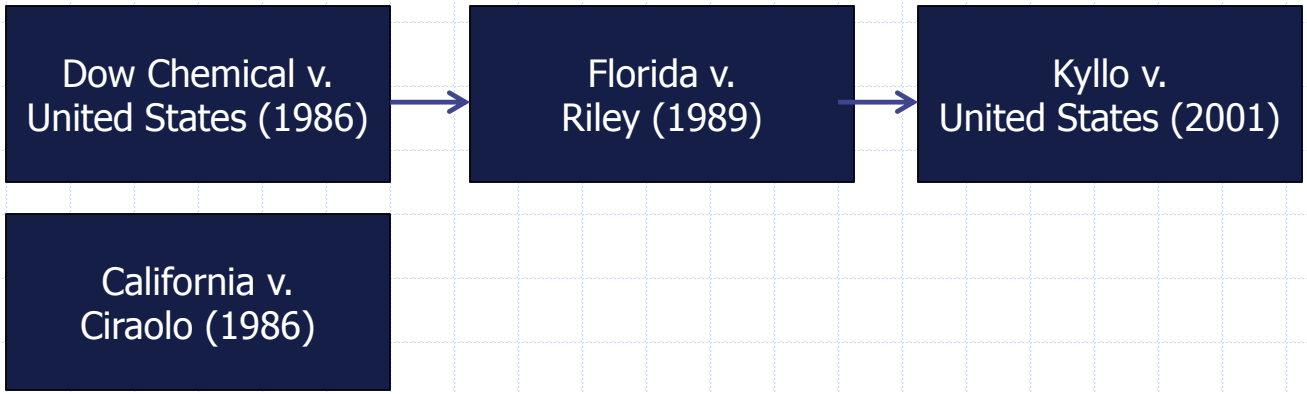
- **Clapper v. Amnesty (2013)**
  - *Challenge to FISA Amendments Act of 2008*
  - *Surveillance without showing of "probable cause" if subject is agent of foreign power*
    - ACLU claims Act enables NSA "to engage in dragnet surveillance of Americans' international communications"
  - *Supreme Court dismissed case on standing*
- **Klayman v. United States (2015)**
  - *Challenge to NSA collection of bulk phone and Internet metadata under FISA Amendments Act of 2008*
    - Claim violation of 1st, 4th and 5th Amendments and exceeds authority under Section 215 of FISA Amendments Act
  - *District court (J. Leon) held unconstitutional*
  - *DC Court of Appeals reversed decision on standing (8/15)*

Parallel Lines of Privacy Cases

Electronic Surveillance Cases



Non-Cyber Surveillance Cases



Federal Statutes Post-*Katz*

- **Law Enforcement – Title III (1968)**
  - *Omnibus Crime Control and Safe Streets Act of 1968, 18 U.S.C. §2510 - Requirement for judicial warrant*
  - *Exception for President to protect the nation against actual or potential attack*
- **Electronic Communication Privacy Act (1986)**
  - *Title I – Protects wire, oral or electronic communications while in transit*
    - More stringent requirements for search warrants
  - *Title II – Protects electronic storage*
    - Also known as the Stored Communications Act (SCA)
    - 180 day limit – e-mail considered "abandoned"
  - *Title III – Prohibits use of pen register and trap/trace devices without a court order*
    - Major change from prior legal principle (Smith v. Maryland)

Limits on The Legal Regime

- **Limits on intelligence – "stealing secrets"**
  - *U.S. persons as targets – intended or not*
    - FISA issues (AUMF, 2008 FISA Amendments Act, etc.)
  - *Collection precedes target identification in many cases*
    - Orthogonal to FISA concept
  - *Location of the collector; agreements with 2nd and 3rd parties*
  - *Risks to operatives*
    - Espionage not covered by international law
- **Limits on law enforcement**
  - *Increasing application of Fourth Amendment protections*
    - Case law since Katz v. United States (1967)
  - *Title III requirement for warrant*
    - Difficult in many cases due to new systems, economics, culture

Legal Regime Antiquated and Behind Current Technologies

- **Title III (1968), FISA (1978), ECPA (1986) are all old law**
  - *Predate modern technologies and threats*
  - *Some may be unconstitutional*
  - *Encryption may make enforcement impossible*
- **Bi-partisan agreement that new law is needed, but none have been enacted**
  - *Four current bills on cybersecurity*
  - *Amendments to ECPA and others*
- **Can't fix with Executive Orders and Presidential Directives**
  - *Band-Aids didn't work before, and won't work now*

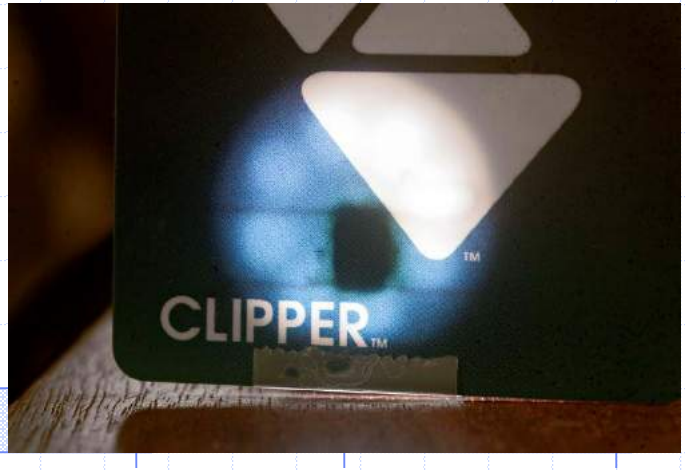
Encryption and The Law

Encryption – A Brief Overview

- **For most of history, encryption was analog, costly and a commercial disaster**
  - *Required expensive machines*
  - *Only users were military and intelligence services*
    - Forced to use it or needed the security
    - Had the money to pay for it
- **Wagner's law – Users will avoid encryption if:**
  - *1. It costs money*
  - *2. Involves any inconvenience*
  - *3. Degrades quality (phone sounds like Donald Duck)*
- **New world avoids Wagner's law**
  - *All in software – avoids marginal cost to users*
  - *Program around any inconvenience to users*
  - *Everything is digital – no quality issues*

USG Approach to Encryption

- **Control encryption technology**
  - *National security concerns*
    - Enable adversaries to avoid intercept
    - Enhance adversary ability to decrypt U.S. communications
  - *Long time battle over university research in cryptology*
- **Legal limits and failed programs**
  - *Impossible to ban completely, so limit to quality of algorithms and key lengths – PGP, RSA etc.*
  - *FBI "Clipper Chip," key escrow and other stupid ideas*



Control on Encryption Today

- **Major tool remains export control**
  - Arms Export Control Act (AECA)
  - International Traffic in Arms Regulations (ITAR) scheme
  - Executive Order 13563 (2011)
  - Wassenaar Arrangement under debate
    - What are intrusion and surveillance items?
    - Prohibited classes of software?
- **Largely beyond U.S. control**
  - *Proliferation of high-grade algorithms worldwide*
  - *Commercial firms started by former KGB*
  - *Ongoing efforts such as Wassenaar Arrangement likely to fail*

Bernstein v. Department of Justice (1999)

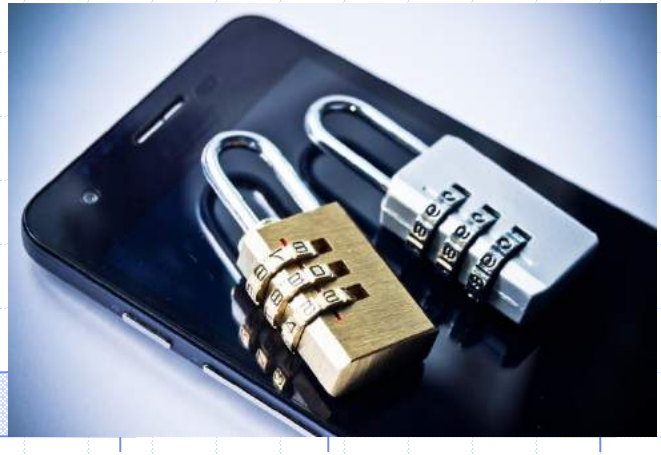
- **Berkley grad student develops "snuffle" encryption algorithm**
  - *Tries to publish paper containing: (a) the algorithm (b) a paper describing and explaining the algorithm; and (c) source code that incorporates the algorithm*
  - *Wants to give conference papers on his work*
  - *Arms Export Control Act and ITAR scheme required him to submit his ideas about cryptography to the government for review; to register as an arms dealer; and obtain a license from the Government to publish his ideas*
- **Ninth Circuit ruled software source code was speech protected by the First Amendment**
  - *Regulations preventing publication were unconstitutional*
  - *Supreme Court has not addressed the issue*

Forced Decryption and the Fifth Amendment – Mixed Results

- **United States v. Fricosu (2012)**
  - *Laptop encrypted with RSA algorithm; mortgage fraud case*
  - *Fricosu ordered to provide decryption key*
  - *District court holds this was not a violation of 5th Amendment protection against self incrimination*
- **United States v. Doe (2012)**
  - *Encrypted computers; child pornography case*
  - *Grand jury orders Doe to provide decryption keys*
  - *Eleventh Circuit holds this is a violation of 5th Amendment protection against self incrimination*
    - Distinction is whether the act is "testimonial" in Doe's mind
- **FBI v. Apple – still very much unsettled**
  - *Cases involving cell phones; PDAs; etc.*
  - *End-to-end encryption is becoming a major deal*

"Going Dark" – Ultimate Nightmare

- **End-to-end encryption is a commercial reality**
  - *Apple and others; USG lost the battle to stop it*
  - *Unlikely to crawl back to earlier regime*
- **Suppliers can't comply with court orders**
  - *Don't have keys and access to unencrypted data*
  - *Forcing user to provide keys is unsettled issue*
- **Impact on NSA and law enforcement**
  - *Open question is how fast encryption proliferates*
  - *No major technical, legal or economic barriers*
  - *Golden age of SIGINT ending?*



Challenges

Geography No Longer Relevant

- **Servers and people all over the globe**
  - *Intelligence targets not always "foreign"*
  - *Microsoft v. USA (2015) – U.S. court order to turn over data on server in Ireland*
- **Antiquated laws hard to apply to current and evolving technologies**
  - *Operations beyond the reach of U.S. law*
  - *Foreign assistance of limited use*
- **Need effective organization for cybersecurity**
  - *Putting DHS "in charge" is recipe for disaster*
  - *Only critical mass of skills is at NSA and CYBERCOM*
  - *Recent Executive Order and PDD-21 are no real help*
  - *Title 10 and Title 50 issues still exist*

Issues Related to "U.S. Persons"

- **Use FISA definition?**
  - *Doesn't include visitors, illegal aliens, etc.*
  - *Terrorism and other exceptions may be unconstitutional*
  - *Collection systems don't enable a priori targeting*
- **New technologies enable anonymity**
  - *Cell phones with no identified owners – burners*
  - *E-mail with aliases and new accounts*
  - *Can't meet requirements*
- **Often impossible to identify a priori**
  - *Can't meet legal requirement for FISA warrant*

Media Issues

- **Deep packet inspection**
  - *Privacy requirements and how "deep" can we go?*
- **Are all media covered by Fourth Amendment?**
  - *Data mining issues*
  - *Commercial firms and economic intelligence – not a major issue in 1986 when ECPA enacted*
- **Transient and stored media**
  - *Does 180 day limit in ECPA make sense?*

Study Team

David Aitel
Immunity, Inc.

Sophia d'Antoine
Center for Advanced Studies on Terrorism

Edward Doyle
Center for Advanced Studies on Terrorism

Daniel Gallington
Center for Advanced Studies on Terrorism

Thomas Garwin
Center for Advanced Studies on Terrorism

Daniel Guido
Trail of Bits, Inc.

Nicholas Rostow
Yale Law School

Ryan Stortz
Trail of Bits, Inc.

Abraham Wagner
Columbia Law School

Kevin Yorke
New York Attorney's Office

RESEARCH ASSISTANTS

Baruch Bacharach
Columbia Law School

Christine Chen
Columbia Law School

Theodore Rostow
Yale Law School

Kathryn Witchger
Columbia Law School