Data Privacy and Protection in the US – An Overview

Michael D. Orosz, Ph.D.
Research Director, Decisions Systems
Research Associate Professor
mdorosz@isi.edu
310-448-8266
310-486-2150 (mobile)

Information Sciences Institute
Viterbi School of Engineering
University of Southern California
Marina del Rey, CA

Image Credits:
Image Zoo Illustrations

Intel Course – Spring

USC Price
Sol Price School of Public Policy

Course: PPDE 672 An Exploration of the Intelligence Community – From Policy to Cyber Espionage
Units: 4 Units
When: Spring Semester, Wednesdays, 6-9:20pm
Instructor: Professor Michael Orosz

- Exploration of the US and Foreign intelligence communities
- Detailed discussions on collection and analytic methods
- Policy and geopolitical considerations (domestic and globally)
- Cyber methods/approaches
- Deep dive into OSINT methods – including major focus on social media and Dark Web
- Ethical concerns
- Course: Mid-term exam, course project, final project

Agenda

- “Genie out of the bottle…”
- Policies that govern the private sector
  - General consumer protections
  - Health/medical protections
  - Research protections
- Policies that govern the public sector (emphasis on law enforcement and intelligence community)

Genie out of the Bottle

- Theft of physical property: With time, can usually be returned or replaced
- Theft of electronic information : More difficult to correct, but for many situations there is a legal framework that can be leveraged to help mitigate (e.g., compensation for loss)
  - The exception: personal identity information...once out there, very difficult to remove or “take back”

Types of Data

- Intellectual property (IP) – business, state, country....and academic/research
- Sensitive – usually associated with state secrets, but can include business (e.g., marketing plans)
- Personal Identity Information (PII) – the focus of today's discussion

Ethical Responsibilities

- Due to the “genie out of the bottle” problem, we have an ethical responsibility to protect PII
- It is very easy to overlook this responsibility
  - Sharing data with others (i.e., lost chain of custody)
  - Accidental exposure through data breaches (e.g., third-party clouds)
  - Not slowing down (e.g., sending an email message without thinking about consequences)

Private Sector

Personal Information Protection in the US

- There is no federal-level ***general data*** privacy protection policy in the US (unlike the EU's General Data Protection Regulation – GDPR (2016))
- However, there are nation-wide policies that govern how health/medical information is handled/protected:
  - Health Insurance Portability and Accountability Act (HIPAA)
  - Health Information Technology for Economic and Clinical
- There are also acts that protect the privacy of underaged children:
  - Children's Online Privacy Projection Act (COPPA)

Some Reasons for Lack of a Federal Policy

- Cost to business to implement is high
- Access to PII is part of the business model
- Low priority – although this is changing
- Recognition that US can't govern the rest of the world

Personal Information Protection in the US (Cont.)

- There are, however, many state level acts and regulations:
  - California Consumer Privacy Act (CCPA)
  - California Privacy Rights Act (CPRA – 2023)
  - Colorado Privacy Act (similar to the CCPA - 2021)
  - Maine Act to Protect the Privacy of Online Consumer Information (2020)
  - Mass Data Protection Act (2010)
  - ...and many others...similar, but each has nuances

Personal Information Protection in the US (Cont.)

- Almost all research undertaken in the US (especially US Government funded research) is governed by data protection/privacy rules.
- Example: DARPA, IARPA, NSF, NIH and most other US Government funding agencies require a data handling/protection plan be submitted as part of the proposal and implemented during project execution
- Universities also have internal data handling requirements to project human subject identity/privacy (Institutional Review Board (IRB))

USC Office for the Protection of Research Subjects (OPRS)

- Data use agreement: https://oprs.usc.edu/wp-content/uploads/sites/3/2021/09/Data-Use-Agreement.doc

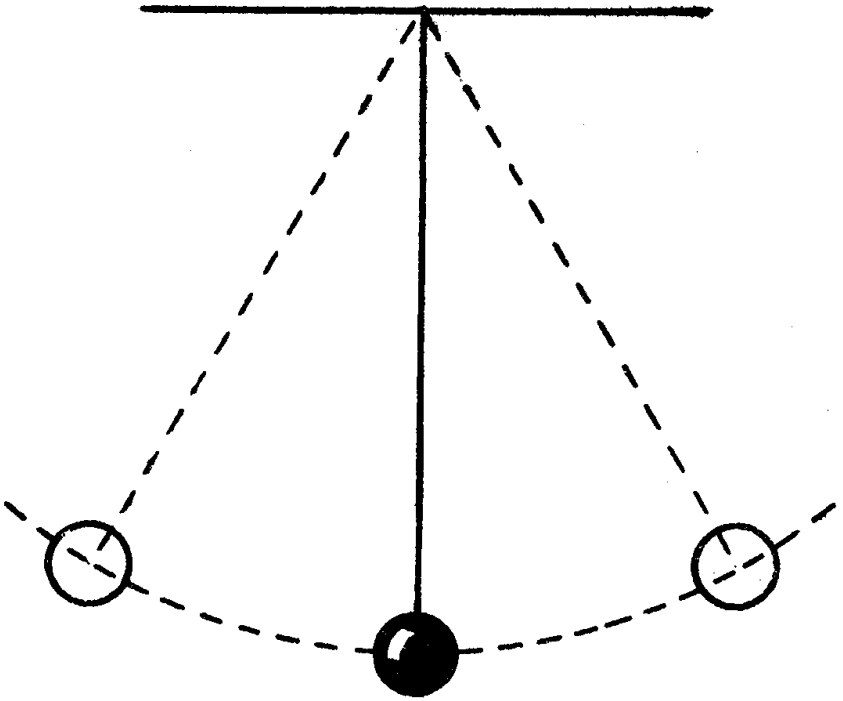
Typical PII Protection Protocol

- All names and other identifying information from people's data is removed prior to distribution or publishing
- Follow all federal, state, and local laws and regulations for keeping information safe.
- Maintain internal policies and procedures to prevent misuse of data (e.g., only people with a need to see the data are allowed access – "need to know")
- Store information on protected computers. Limit and keep track of who can see it.
- Notify research subjects if there is a risk to their privacy because of a data breach.

Public (Government) Sector (focus on the IC and Federal Law Enforcement)

The Pendulum

- In the US law enforcement & intelligence communities, there is constant tension between security and privacy
- A pendulum swings from security to privacy and back – driven mainly by US National Security events



This back and forth looking for the right balance is what makes the US unique

US Citizen vs. US Person

- US Persons include:
  - US Citizens (birth or naturalized)
  - Green card holders
  - H1-B and other special permit holders

- A visitor (documented or undocumented) is not a US Person

Speech vs. Privacy

- Unlike the Freedom of Speech (1st Amendment), the right to privacy is not specifically guaranteed in the US Constitution
- However, the right of privacy is inferred by the 4th Amendment – the freedom from unreasonable search and seizure
- However, the US Supreme Court has ruled that the 4th Amendment does not give US Persons a legally recognized expectation of privacy in information that **he or she gives to a third party**

More on this shortly

“Reasonableness”

- Further, the Supreme Court has said that the “reasonableness” of a warrantless search depends on balancing the “intrusion on the individual’s Fourth Amendment interests against” the search’s “promotion of legitimate Governmental interests.”

Third-Party Doctrine

- Makes legal that information loses Fourth Amendment protection when it is knowingly revealed to a third party.
- A lack of privacy protection allows the United States government to obtain information from third parties without a legal warrant
- Katz v. United States (1967), United States v. Graham (2012) and other cases argued successfully in front of US Supreme Court the legality of the Third-Party Doctrine
- But, Carpenter v. United States (2019) SCOTUS ruled that a warrant is required for phone tracking information

This ruling makes sense. Tracking phone movements is similar to putting a tracking device on a car…which requires a warrant

Significant Acts/Events

- Examples of acts that govern US intelligence collection and analysis:
  - National Security Act of 1947
  - Privacy Act of 1974 (and amendments)
  - Electronic Communications Privacy Act of 1986 (and amendments)
  - FISA Act of 1978 (and revisions in 2001 and 2008)
  - Executive Order 12333

Key Acts (Part 1)

- **National Security Act of 1947**: Restricts CIA to collecting only foreign intelligence (the CIA is not a law enforcement agency)
- **Privacy Act of 1974**: Restricts who can access intelligence on US Persons maintained in US Federal Government databases. Was later amended to allow DHS access (for international air travel) and by President Trump to exclude legal foreign nationals
- **Electronic Communication Privacy Act of 1986**: Amended wiretap laws to include electronic communications (& storage)
- **FISA Act of 1978**: Established framework for legally accessing foreign intelligence
- **Executive Order 12333 (1981)**: Addresses areas of foreign intelligence not covered by the FISA Act of 1978

FISA Act of 1978

- FISA Act of 1978:
  - Prior to 1978: Existing rules were “fuzzy” on preventing the IC from collecting on US Persons
  - Law prevents collecting on US Persons if they have **no foreign intelligence value** or are not involved in a crime
  - If of foreign intelligence value, that information can only be disseminated to individuals/organizations that have **a need to know**

FISA – Key Takeaways

- Original FISA Act of 1978:
  - The US Government does not need a warrant (***up to one year***) to collect foreign communications within and outside of the US ***as long as all effort is taken to ensure the privacy of US Persons accidently caught up in the collection***.
  - A ***warrant is required*** if the US Government collects communications of US Persons suspected of having links with foreign entities of interest
  - Established the FISA Court (FISC) to review and grant warrants (if appropriate) to collect on US Persons suspected of working with foreign entities of interest

Executive Order 12333

- Originally signed into law by Reagan in 1981, it has been amended three times over the years (to address technical, privacy and security issues)
- FISA of 1978 addresses when a warrant is required and that the privacy of US Persons must be protected (as best as possible)
- EO 12333 discusses what can be collected…the details such as records, email messages, cell traffic, etc.
- EO 12333 recognizes that some intelligences on US Persons may be collected, but specifies how to protect that data (FISA doesn't get into those details)

FISA establishes a framework for foreign intelligence collection/analysis, but EO 12333 addresses implementation

Section 215 of the US Patriot Act

- Amended Section 501 of the Foreign Intelligence Surveillance Act (FISA)
- Allows collection of intelligence on US Persons if relevant to preventing terrorism or espionage
- Allows bulk collection of "telephony metadata," – numbers, dates, times and length of call. BUT NOT names or physical addresses

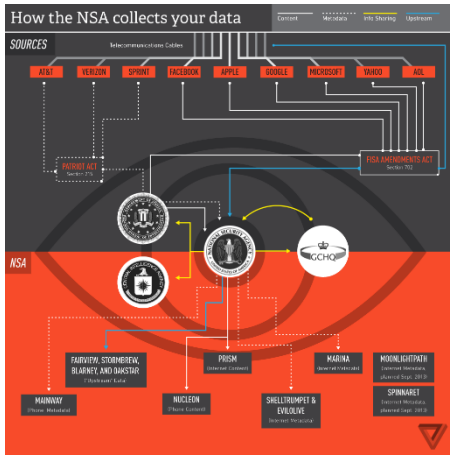
Section 702

- Added to FISA via the *FISA Amendments Act of 2008* (FAA)
- Extends the FISA to focus on collection of intelligence on foreigners *"overseas."* This includes metadata and content
- But recognizes that intelligence on US Persons is also collected (just like the original FISA Act of 1978)
- Specifies that such information (on US Persons) must be protected from illegal use
- **Most importantly**: Data is stored in a database that can be accessed by domestic law enforcement interested if a US Person of interest. A warrant must already exist on the US Person of Interest….but this can be abused

Section 702 is all about countering terrorism

NSA PRISM

- NSA requested “bulk” data dumps of telecon metadata (phone number of caller, phone number of receiver, date, time and duration…no GPS or location data, no names).
- This is information already collected and stored by **3rd parties** (telecon companies)
- “Bulk” collection is what alarmed everyone. It’s possible for data mining techniques to be used to extract “networks” of contacts. It’s a simple procedure to link a name to a phone number
- On the other hand, “bulk” records can aid the US in discovering terrorist networks



28 CFR Part 23 (Domestic Intelligence Processing)

28 CFR Part 23

- The purpose of this regulation is to assure that all criminal intelligence systems operating through support under the Omnibus Crime Control and Safe Streets Act of 1968 (and as amended) are utilized in conformance with the privacy and constitutional rights of individuals
- The regulation helps protect an individual's privacy and constitutional rights during the collection, storage, and dissemination of criminal intelligence information as part of a criminal investigation

28 CFR Part 23 - Guidelines

- Can only collect, analyze and store information if there is ***reasonable suspicion*** that the individual and/or organization is involved in **criminal conduct or activity** and the information is relevant to that criminal conduct or activity.
- Can **not collect** or maintain criminal intelligence information about the **political, religious or social views, associations, or activities** of any individual or any group, association, corporation, business, partnership, or other organization **unless** such information **directly relates to criminal conduct or activity** and there **is reasonable suspicion** that the subject of the information is or may be involved in criminal conduct or activity.

28 CFR Part 23 - Guidelines

- Can not collect, analyze and store any criminal information which has been obtained in violation of any applicable Federal, State, or local law or ordinance
- An authorized authority shall disseminate criminal intelligence information only where there is a need to know and a right to know the information in the performance of a law enforcement activity
- However, such criminal information can be disseminated, when necessary, to avoid imminent danger to life or property

28 CFR Part 23 - Guidelines

- An auditing system must be maintained to ensure protection of criminal intelligence.
- Such a system must control who can access a record, when that record was accessed, if the record was modified (e.g., added to) and under what authority
- In addition, such information must be labeled to indicate levels of sensitivity, confidence and the identity of the submitting agencies

28 CFR Part 23 - Guidelines

- Procedures need to exist to allow destruction of records that are no longer relevant
- Periodic reviews of the stored data are required to ensure relevancy of stored information
- No information can be stored beyond 5 years

28 CFR Part 23

- 28 CFR Part 23 is also a guideline for law enforcement agencies that operate federally funded multijurisdictional criminal intelligence systems such as fusion centers.
- The Joint Regional Intelligence Center (JRIC) in LA County is responsible for the processing of SARs – Suspicious Activity Reports
- Regional law enforcement agencies submit to the JRIC SARs that they feel may indicate a potential terrorist act
- The JRIC is staffed by personnel from various LA agencies. It is run by the FBI (specifically, by the Joint Terrorism Task Force (JTTF)

28 CFR Part 23 and Fusion Centers

- When a SAR is submitted to the JRIC for processing, local law enforcement and the FBI examine it to determine if the SAR points to a potential criminal or terrorist activity
- If possible criminal activity, the SAR is returned to the submitting agency and handled per 28 CFR Part 23
- If possible terrorism activity, the SAR falls under the FBI and DHS umbrellas and the US IC regulations apply

Image Credits:
Image Zoo Illustrations

Discussion