Data Privacy

How *<u>can</u>* we, or how *<u>should</u>* we, use data?

- **Legal Standards**
  - Established by law, order, or rule to compel treatment of certain classes of data
- **Ethical Standards**
  - Standards established by industry or professional organizations which seek to establish level of non-legally binding treatment of information
- **Policy Standards**
  - Established by a company or agency's own published Data Privacy policy
- **Good Judgment Standards**
  - Even if technically ok by more formal standards, one should always stop to ask *"Is this a good idea?"* and *"What might be the consequences?"*

Personally Identifiable Information (PII)

- **Definition**: Ainformation about an individual maintained by an agency, including

  1) any information that can be used to distinguish or trace an individual‘s identity, such as name, social security number, date and place of birth, mother‘s maiden name, or biometric records; and

  2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information

Personally Identifiable Information (PII) - Examples

- Name, such as full name, maiden name, mother‘s maiden name, or alias
- Personal identification number, such as social security number (SSN), passport number, driver‘s license number, taxpayer identification number, or financial account or credit card number
- Address information, such as street address or email address
- Personal characteristics, including photographic image (especially of face or other identifying characteristic), fingerprints, handwriting, or other biometric data (e.g., retina scan, voice signature, facial geometry)
- Information about an individual that is linked or linkable to one of the above (e.g., date of birth, place of birth, race, religion, weight, activities, geographical indicators, employment information, medical information, education information, financial information).

Personally Identifiable Information (PII)

“ A common misconception is that PII only includes data that can be used to directly identify or contact an individual (e.g., name, e-mail address), or personal data that is especially sensitive (e.g., Social Security number, bank account number). The OMB and NIST definition of PII is broader . The definition is also dynamic, and can depend on context. Data elements that may not identify an individual directly (e.g., age, height, birth date) may nonetheless constitute PII if those data elements can be combined, with or without additional data, to identify an individual. In other words, if the data are linked or can be linked ("linkable") to the specific individual, it is potentially PII.

Moreover, what can be personally linked to an individual may depend upon what technology is available to do so. As technology advances, computer programs may scan the Internet with wider scope to create a mosaic of information that may be used to link information to an individual in ways that were not previously possible (this is often referred to as the "mosaic effect").”

https://cio.gov/wp-content/uploads/downloads/2012/12/Standardized_Digital_Privacy_Controls.pdf

Personally Identifiable Information (PII)

N characteristics with two possible values each (e.g., M or F)

Number of different type of people = 2^N

29 attributes = 536,870,912 kinds of people

- *More than the US population of ~320M*

33 attributes = 8,589,934,592 kinds of people

- *More than the worldwide population of ~7.4B*

37 attributes = 137,438,953,472 kinds of people

- *More than all people who have every lived! ~108B*

PII-Related Regulations

U.S. Federal

- Title 18 of the United States Code, section 1028d(7)
- The Privacy Act of 1974, codified at 5 U.S.C. § 552a et seq.
- US "Safe Harbor" Rules (EU Harmonisation)

U.S State

- California: The California state constitution declares privacy an inalienable right in Article 1, Section 1; California Online Privacy Protection Act(OPPA) of 2003; SB 1386 requires organizations to notify individuals when PII is known or believed to be acquired by an unauthorized person. In 2011, the California State Supreme Court ruled that a person's ZIP code is PII.
- Nevada: Revised Statutes 603A-Security of Personal Information
- Massachusetts: 201 CMR 17.00: Standards for The Protection of Personal Information of Residents of the Commonwealth; In 2013, the Massachusetts Supreme Court ruled that ZIP codes are PII.

European Union

- Article 8 of the European Convention on Human Rights
- Directive 95/46/EC (Data Protection Directive); he General Data Protection Regulation adopted in April 2016 will supersede the Data Protection Directive.
- Directive 2002/58/EC (the E-Privacy Directive)
- Directive 2006/24/EC Article 5 (The Data Retention Directive)

United Kingdom

- The UK Data Protection Act 1998
- General Data Protection Regulation (Europe, 2016)
- Article 8 of the European Convention on Human Rights
- The UK Regulation of Investigatory Powers Act 2000
- Employers' Data Protection Code of Practice Model Contracts for Data Exports
- The Privacy and Electronic Communications (EC Directive) Regulations 2003
- The UK Interception of Communications (Lawful Business Practice) Regulations 2000
- The UK Anti-Terrorism, Crime and Security Act 2001

Consumer Financial Information (CFI)

Definition: Any information that is not publicly available, and that:

a) A consumer provides to a financial institution to obtain a financial product or service from the institution

b) Results from a transaction between the consumer and the institution involving a financial product or service

c) A financial institution otherwise obtains about a consumer in connection with providing a financial product or service

Governing Law:

- Gramm-Leach-Bliley Act driven into FTC, SEC rules
- Fair Credit Reporting Act

Consumer Financial Information (CFI)

Key Provisions:

- Applies to financial institutions and those who collect "nonpublic personal information" from "customers" , "consumers" or financial institutions.
- Specific provision on account numbers and other information
- Mostly around disclosure vs. prescription of what’s allowed or not allowed
- Defines notice and opt-out duties to customers

Customer Proprietary Network Information (CPNI)

Definition: Data collected by telecommunications companies about a consumer's telephone calls.

- It includes the time, date, duration and destination number of each call, the type of network a consumer subscribes to, and any other information that appears on the consumer's telephone bill.
- Does NOT explicitly include non-telephone activity (e.g., web browsing)

Governing Law:

- U.S. Telecommunications Act of 1996
- 2007 FCC CPNI Order
- Electronic Privacy act of 1996
- Communications Assistance for Law Enforcement Act of 1994 (CALEA)

Customer Proprietary Network Information (CPNI)

Key Provisions:

- Limits the information which carriers may provide to third-party marketing firms without first securing the affirmative consent of their customers
- Defines when and how customer service representatives may share call details
- Creates new notification and reporting obligations for carriers (including identity verification procedures)
- Verification process must MATCH what is shown with the company placing the call.

The Fine Print:

- CAN freely share information with an other ‘communications’ company
- Opt-out based (i.e., customer has to explicitly request information NOT be shared)

Protected Health Information (PHI)

Governing Law:

- Health Insurance Portability and Accountability Act of 1996 (HIPAA)

Definition:

1. Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and
2. Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and
    i. That identifies the individual; or
    ii. With respect to which there is a reasonable basis to believe the information can be used to identify the individual
3. Transmitted by electronic media; Maintained in electronic media; or Transmitted or maintained in any other form or medium.

Protected Health Information (PHI)

Key Provisions:

- Has a ‘Privacy Rule’ (applies to ALL PHI) and a ‘Security Rule’ (applies to electronic PHI)
- Applies to Health Care Providers, Health Plans, Health Care Clearinghouses
- Lots of specific data treatment provisions, including stripping out of identifiable info, etc.

Exclusions:

- Education records covered by Family Educational Rights and Privacy Act
- Employment records held by a covered entity in its role as employer

Recap

Personally Identifiable Information (PII)

Consumer Financial Information (CFI)

Customer Proprietary Network Information (CPNI)

Protected Health Information (PHI)

Ethical Standards

Ethical Standards:

- Most Academic / Science / Medical / Legal fields have broad ethical standards-making bodies, some of which address use of data
  - Consequences include sanctions, revoking membership, etc.
- Marketing/Advertising as business practices are particularly rich:
  - Direct Marketing Association (DMA) – broad guidelines
  - Digital Advertising Alliance (DAA) – first party data collection
  - Network Advertising Initiative (NAI) – third party & network exchanges
  - Enforcement weaker, but compliance still a good idea!

Corporate Policy

Corporate Policy:

- Most companies have formal privacy policies that are actively disclosed to consumers
- Generally, these policies outline what is captured & shared, and outline opt-out or opt-in procedures

Know what legal, ethical and corporate standards apply in your situation!

Good Judgment

Even if it's legal, ethical, and within corporate policy, it still might not be a good idea:

- *The "Creepiness" Factor*
- *Backlash from bad PR – "stay out of the news"*
- *Unintended behaviors by customers*
- *Often, a purely economic risk assessment, if properly inclusive, will align with a good 'gut feeling' on whether it's the right thing to do!*