Information Privacy Primer

What is Privacy?

- We have personal privacy, workplace privacy, and information privacy – among others.
- Privacy is largely an idea – it can be different for each person
- Privacy is not security – we can have security without privacy but not vice versa
- Organizationally speaking, information privacy today is where information security was 5 years ago

U.S. Privacy Law Origins

- 1791 – Bill of Rights
  - 4th Amendment right against unreasonable search and seizure
    - Affects computer and electronic device searches
    - Third party doctrine
  - Katz v. United States (1967) established concept of "reasonable expectation of privacy"
    - Supreme Court has not addressed "reasonable" privacy expectations for email, text messages, tweets, etc.
- 1890 – Samuel Warren and Louis Brandeis publish influential article "The Right to Privacy"
  - Introduce concept of "the right to be left alone"
  - Justice Brandeis reiterates this right in Olmstead vs. U.S. (1928)
  - Several Federal laws regulating marketing communications based on this

Select U.S. Federal Laws

- Fair Credit Reporting Act (1970, 1996, 2003 FACTA)
  - Consumer right to access credit info – request corrections
  - Enforced by Federal Trade Commission, State Attorneys General
- Privacy Act of 1974
  - Regulates collection, use, dissemination of personal info by government
- Graham-Leach-Bliley Act (GLBA)
  - Privacy Rule, Safeguards Rule (privacy notices and opt-out)
  - Enforced by FTC, Financial Regulators, State Attorneys General
- Health Insurance Portability &Accountability Act (HIPAA)
  - Security Rule and Privacy Rule – limit info disclosure and maintain records
  - Enforced by Dept. Health & Human Services, State Attorneys General
- Children's On-line Privacy Protection Act (COPPA)
  - Verifiable parental consent prior to collecting data about children
  - Enforced by FTC and State Attorneys General
- Family Education Rights and Privacy Act (FERPA)
  - Protect student records, right to correct info. Enforced by US DOE.
- U.S. Laws Regulating Marketing Communications
  - Telemarketing Sales Rule, CAN SPAM Act, Junk Fax Prevention Act
  - Enforced by Federal Communication Commission (and/or FTC)

Select U.S. Federal Laws

- Electronic Communications Privacy Act (1986)
  - Interception and disclosure of wire, oral, or electronic communications prohibited
  - Title I covers communications in transit
  - Title II – Stored Communications Act – protects stored communications
  - Law enforcement generally does not need warrant for messages 180 days old
  - Inconsistent interpretation of how ECPA applies to tweets , text messages and other transitory or stored communications

Select U.S. State Laws

- Breach Notification Laws
  - Forty-six states, the District of Columbia, Puerto Rico and the Virgin Islands
  - Specify instances where breaches require notification of affected parties, and possibly regulators
- State Security Laws
  - Most states have laws regulating use/disclosure of SSN and/or other personal information
  - Typically require "reasonable" security

Information Privacy Views

United States

- Laws largely based on privacy as a consumer protection
- Use of information about persons largely acceptable unless harmful or prohibited

European Union

- Laws based on privacy as a basic human right
- Use of information about persons largely prohibited unless requirements met

Source: IAPP

Information Privacy Definitions

- **Personal Information** – any information related to an identified or identifiable person

- **Personal Data (EU)** - any information related to identified or identifiable natural person (data subject); identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural, or social identity

Source: IAPP

Sensitive Personal Info

United States

- Social Security Numbers
- Financial Information
- Driver's License
- Medical Records

European Union

- Certificates/Licenses
- Financial Information
- Health Records
- Racial/Ethnic Origin
- Political Opinions
- Religious Beliefs
- Trade Union Membership
- Sexual Orientation
- Offenses and Criminal Convictions

Source: IAPP

OECD Guidelines

- Collection Limitation
  - Limits on collection of personal data
  - Data obtained lawfully, fairly, with knowledge/consent of data subject
- Data Quality
  - Personal data relevant to purposes for which collected
  - Should be accurate, complete, and up to date
- Purpose Specification
  - Purposes for collection specified at or prior to collection time
  - Subsequent use of data only as specified or per change notification
- Use Limitation
  - Personal data should not be disclosed, made available or otherwise used for purposes other than those specified

Source: IAPP

OECD Guidelines

- Security Safeguards Principle
  - Personal data should be protected by reasonable safeguards
- Openness Principle
  - Should be a general policy of openness regarding developments, practices and policies with respect to personal data
- Individual Participation Principle
  - Individual should have the right to get timely confirmation on data held about him/her and redress to information corrected or possibly deleted
- Accountability Principle
  - Data controller is held accountable for complying with these principles

Source: IAPP

EU Data Protection Directive

- Enacted to allow more freedom of movement of personal data within EU
- Personal data movement outside of EU is severely restricted
- Data Protection Authorities in member countries enforce laws and investigate complaints
- OECD Guidelines formed Data Protection Principles used in EU DPD

Source: IAPP

EU DPD Definitions

- **Data Subject** – individual who is subject of personal information
- **Data Elements** – types of personal information processed
- **Data Controller** – natural or legal org which determines – alone or with others – purpose and means of processing personal information
- **Data Processor** – natural or legal person that processes personal data on behalf of data controller

Source: IAPP

Privacy Definitions

- **Privacy Policy** - An organization's standard pertaining to the user information it collects and what is done with the information after it is collected

- **Privacy Statement** - An organization's communication regarding its privacy policies, such as what personal information is collected, how it will be used, with whom it will be shared, and whether one has the option to exercise control over how one's information is used. Privacy statements are frequently posted on Websites.

Source: IAPP

Choice and Consent

- **Choice** - An individual's ability to determine whether or how personal information collected from him or her may be used or disclosed by the entity that collected the information.
- *Also:* The ability of an individual to limit certain uses of his or her personal information. For example, an individual may have choice about whether to permit a company to contact the individual or share the individual's data with third parties

Source: IAPP

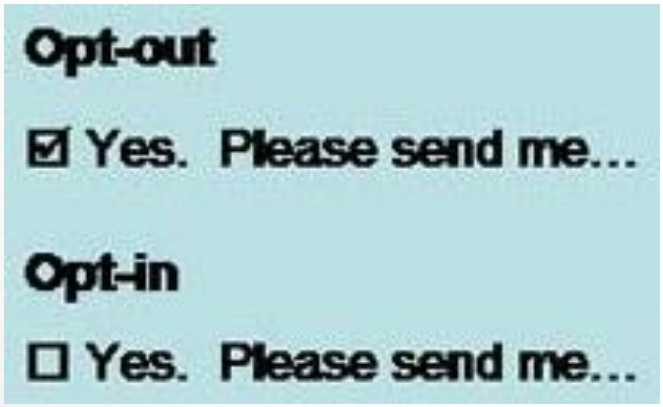
Choice and Consent

- **Consent** - This privacy requirement is one of the fair information practices. Individuals must be able to prevent the collection of their personal data, unless legally required. If an individual has a choice about the use or disclosure of his or her information, consent is the individuals' way of giving permission for the use or disclosure. Consent may be affirmative (*e.g.*, opt in) or implied (*e.g.*, the individual didn't opt out.)

Source: IAPP

Opt in vs Opt out

- **Opt in:** A consumer's expression of affirmative consent based upon a specific act of the consumer
- **Opt out:** A consumer's exercise of choice through an affirmative request that a particular use of disclosure of data not occur



Source: IAPP

Data Lifecycle

- The time period defined from the originating point at which an organization acquires personal information to the time when the information is removed from the organization. Components of the life cycle include: collection, storage, use, sharing and destruction.

Source: IAPP

Ongoing Privacy Issues

- Harvesting of personal data without knowledge or explicit consent (Google, Facebook, et al.)
- Use of personal data beyond original consent agreement
- Huge volume of publicly available data about individuals makes anonymizing largely ineffective
  - Sweeney examined 1990 census data and found 87.1% of people in the United States were uniquely identified by their combined five-digit ZIP code, birth date (including year), and sex
  - Narayanan and Shmatikov examined Netflix data released in 2006 and could identify "anonymized" users 85% of the time

Recent Privacy Issues

- CBS News examined copiers
  - Almost every digital copier since 2002 has a hard drive
  - By default, most keep copy of every item scanned until need for disk space requires overwrite
  - Copiers are typically leased rather than purchased, often the disk is full of images from the previous user
  - 60% of users were unaware that images were stored

Recent Privacy Issues

- Wall Street Journal investigates smartphones and apps
  - Apple iPhone and Google Android have unique device identifiers (UDID) that cannot be changed or turned off
- Examination of 101 popular apps revealed
  - 56 transmitted UDID to companies w/o user knowledge or consent
  - 47 transmitted user's phone location
  - 5 transmitted age, gender, and other personal details
  - 45 provided NO privacy policy on the website or in the app itself
  - NEITHER GOOGLE NOR APPLE REQUIRE APPS TO PROVIDE PRIVACY POLICY