Privacy

COMP620

"Cloud computing, smartphones, social media platforms, and Internet of Things devices have already transformed how we communicate, work, shop, and socialize. These technologies gather unprecedented data streams leading to formidable challenges around privacy, profiling, manipulation, and personal safety."

Oren Etzioni

CIA

- Privacy is a part of **C**onfidentiality
- Most people do not want everything from their life to be available on the web
- We often relinquish aspects of our privacy for convenience

Cultural Value

- Privacy is the ability of an individual or group to seclude themselves or information about themselves and thereby reveal themselves selectively *(Wikipedia)*
- An individual's expectation of privacy differs based on their cultural environment

Location Privacy Concern

- A few years ago I gave a survey on location privacy to about 50 people
- There was a strong correlation between concern about releasing your location and age
- Younger people are less concerned about others knowing their location

Your opinion

How concerned are you that your friends (and only selected friends) can always learn your geographical location?

A. Very concerned
B. Somewhat concerned
C. Somewhat unconcerned
D. Not concerned at all

Your opinion

How concerned are you that your friends and service providers, such as Google, can always learn your geographical location?

A. Very concerned
B. Somewhat concerned
C. Somewhat unconcerned
D. Not concerned at all

Your opinion

How concerned are you that the government can always learn your geographical location?

A. Very concerned
B. Somewhat concerned
C. Somewhat unconcerned
D. Not concerned at all

Information Privacy

- Privacy concerns exist wherever uniquely identifiable data relating to a person or persons are collected and stored, in digital form or otherwise. *(Wikipedia)*
- People may be willing to trade privacy for other advantages such as security or lower prices

Universal Declaration of Human Rights

Article 12 of the United Nation's Universal Declaration of Human Rights states

- *No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks.*

Technology and Privacy

This ad for telephone service in 1912 promoted dial phones instead of operator assisted connections as a privacy advantage

Constitutional Right

- The United States constitution does not explicitly define a right to privacy
- The Supreme Court has ruled that the constitution implicitly grants a right to privacy against government intrusion

Types of Private Information

- There is a wide variety of information that a person may wish to keep private
  - Financial
  - Medical
  - Political
  - Internet
- People may feel the need to keep this private to avoid discrimination or embarrassment

Identity Theft

- Through various methods, thieves can obtain personal information that allows them to masquerade as someone else.
- Identity thieves usually use this information to obtain credit under someone else’s name

Privacy Laws

- Health Insurance Portability and Accountability Act of 1996 (HIPAA)
- Children's Online Privacy Protection Act of 1998 (COPPA)
- Fair and Accurate Credit Transactions Act of 2003 (FACTA),

HIPPA

- Modernizes the flow of healthcare information
- Stipulate how Personally Identifiable Information maintained by the healthcare and healthcare insurance industries should be protected from fraud and theft
- Address limitations on healthcare insurance coverage
- Establishes national standards for electronic health care transactions

Protected Health Information

- Individuals have the right to access all health-related information, including health condition, treatment plan, notes, images, lab results, and billing information
- Data may be provided on paper or in many electronic formats
- Individuals have the right to request an organization to correct any inaccurate Protected Health Information (PHI)

HIPPA Security Safeguards

- Administrative - policies and procedures designed to clearly show compliance
- Physical – controlling physical access to protected data
- Technical – controlling access to computer systems and transmitted data
- Transmitted PHI must be encrypted
- Message authentication and digital signatures must be used
- Organizations must authenticate entities with which they communicate

Children's Online Privacy Protection Act

- Website operators that collect information must seek parental consent for children under 13 years old
- Obtaining verifiable parental consent can be time consuming
- Some organizations simply prohibit children from participating

Fair and Accurate Credit Transactions

- Allows consumers to request a free credit report once every year from each of the three nationwide consumer credit reporting companies
- Provides provisions to help reduce identity theft, such as the ability for individuals to place alerts on their credit histories
- Companies can not print more than 5 digits of a credit card number

Wiretapping

- U.S. Electronic Communications ACT of 1986 protects against wiretapping
  - Requires ISP and phone companies to provide data with a court order
- USA Patriot Act of 2001 relaxes requirements for wiretaps
  - Sets penalties for damaging computer systems

Organizational Privacy

- Companies and other organizations may need to keep private information about their operation
- Employees may have little privacy from their employer while they work

Trade Secrets

- A trade secret is something a company knows that gives them a competitive advantage
- Can often be protected with patents and trademarks These require the company to reveal their secrets
- The Uniform Trade Secrets Act is a model for state laws
- Provides for civil penalties

Home Assistants

- Voice activated devices such as the Amazon Echo, Google Home and Apple HomePod are always connected to the Internet
- These systems are always listening
- So the services can learn to respond better to future commands, they keep a history of past commands
- Systems store the audio and translated text

Now with video

- During the first quarter of 2018, Google shipped 3.2 million of its Google Home and Home Mini devices, while Amazon shipped 2.5 million Echoes
- The latest Amazon Spot and Echo look also have a camera for video communications
- The Drop-In feature allows you to video call a trusted friend without them confirming the call

“How To Secure The Amazon Echo”, forbes.com

General Data Protection Regulation

- A European Union law that went into effect in May 2018
- Regulates data protection and privacy for all individuals within the EU and EEA
- Addresses the export of personal data outside the EU and EEA
- Data cannot be made publicly available without explicit, informed consent
- California passed a similar bill called The California Consumer Privacy Act of 2018

Wikipedia

GDPR

A processor of personal data must

- Clearly disclose any data collection
- Declare the lawful basis and purpose for data processing
- State how long data is being retained
- Indicate if data is being shared with any third parties or outside of the EU

Wikipedia

Data Rights

- People have the right to request a portable copy of the data collected by a processor in a common format, and the right to have their data erased under certain circumstances
- Pseudonymisation is recommended to reduce the risks to the concerned people
- Pseudonymisation differs from anonymization in that it can be reversed with additional information

Wikipedia

Data protection by design and by default

- Systems must use the highest-possible privacy settings by default
- Businesses whose core activity centers around personal data must have a data protection officer
- Encryption must be carried out locally, not by remote service, because both keys and data must remain in the power of the data owner if any privacy is to be achieved

Wikipedia

Getting Consent

- *“This call is being recorded for training purposes.”*
- A typical disclaimer is not considered sufficient to gain assumed consent to record calls
- If a person refuses consent, then anything previously recorded must be erased
- You may have noticed an increase in pop-up boxes on websites telling you they use cookies
- Santa Claus's “naughty or nice” list violates the GDPR