

# The Landscape of Privacy

Anupam Datta  
Carnegie Mellon University

---

# What is Privacy?

---



# Philosophical studies on privacy

---

## ▶ Reading

- ▶ Overview article in Stanford Encyclopedia of Philosophy

<http://plato.stanford.edu/entries/privacy/>

- ▶ Alan Westin, *Privacy and Freedom*, 1967
- ▶ Ruth Gavison, *Privacy and the Limits of Law*, 1980
- ▶ Helen Nissenbaum, *Privacy as Contextual Integrity*, 2004



# Westin 1967

---

- ▶ Privacy and control over information

“Privacy is the claim of individuals, groups or institutions to determine for themselves when, how, and to what extent information about them is communicated to others”

- ▶ Relevant when you give personal information to a web site; agree to privacy policy posted on web site
- ▶ May not apply to your personal health information



# Gavison 1980

---

- ▶ Privacy as limited access to self

“A loss of privacy occurs as others obtain information about an individual, pay attention to him, or gain access to him. These three elements of *secrecy*, *anonymity*, and *solitude* are distinct and independent, but interrelated, and the complex concept of privacy is richer than any definition centered around only one of them.”

- ▶ De-anonymization attacks used to “obtain information about an individual”, online tracking related to “pay(ing) attention”
- 



# Gavison 1980

---

- ▶ On utility

“We start from the obvious fact that both perfect privacy and total loss of privacy are undesirable. Individuals must be in some intermediate state – a balance between privacy and interaction ... Privacy thus cannot be said to be a value in the sense that the more people have of it, the better.”

- ▶ This balance between privacy and utility will show up in database privacy as well as in privacy policy languages, e.g. health data could be shared with medical researchers



# Contextual Integrity

---

[Nissenbaum 2004]

- ▶ Privacy as a right to appropriate flows of personal information



# Contextual Integrity

---

- ▶ **Central concept: *Context***

- ▶ Examples: Healthcare, banking, education

- ▶ **What is a context?**

- ▶ *Set of interacting agents in roles*

- ▶ Roles in healthcare: doctor, patient, ...

- ▶ *Informational norms*

- ▶ Doctors should share patient health information as per the HIPAA rules

- ▶ Norms have a specific structure (descriptive theory)

- ▶ *Purpose*

- ▶ Improve health

- ▶ Some interactions should happen - patients should share personal health information with doctors



# Informational Norms

---

“In a **context**, the flow of information of a certain **type** about a **subject** (acting in a particular capacity/role) from **one actor** (could be the subject) to **another actor** (in a particular capacity/role) is governed by a particular **transmission principle**.”

Examples of transmission principles: secrecy, reciprocity, control, dessert, consent, notice,....

Contextual Integrity [Nissenbaum2004]

---



# Privacy Regulation Example (GLB Act)

---

Sender role

Subject role

Financial institutions must notify consumers if they share their non-public personal information with non-affiliated companies, *but the notification may occur either before or after the information sharing occurs*

Attribute

Recipient role

Transmission principle



# Privacy Laws in the US

---

- ▶ **HIPAA (Health Insurance Portability and Accountability Act, 1996)**
  - ▶ Protecting personal health information
- ▶ **GLBA (Gramm-Leach-Bliley-Act, 1999)**
  - ▶ Protecting personal information held by financial service institutions
- ▶ **COPPA (Children's Online Privacy Protection Act, 1998)**
  - ▶ Protecting information posted online by children under 13



# Question

---

What can we as computer scientists do to provide better privacy protection?

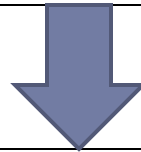


# Dimensions of Privacy

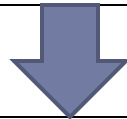
---

## **What is Privacy?**

Philosophy, Law, Public Policy

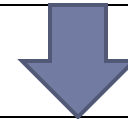


## **Formalize and Enforce Privacy Policies**



## **Individual Information**

Logics, Learning, Game Theory, Planning



## **Aggregate Statistics**

Cryptography, Statistics



# Applications

---

- ▶ **Healthcare**

- ▶ Electronic health records, health information exchanges, personal health records (Google Health), genomic databases

- ▶ **Government Databases**

- ▶ Census, property records, court records

- ▶ **Web and Online Social Media**

- ▶ Facebook, Google, Yahoo, Amazon



---

Thanks!  
Questions?

