What is privacy?

Mainack Mondal

CS 60081
Autumn 2020

Roadmap

- What is privacy?
  - Privacy theories
- How to protect privacy?

Recall CIA model

- Is confidentiality == privacy?

Recall CIA model

- Is confidentiality == privacy? NO

Recall CIA model

- Is confidentiality == privacy? NO
- Secrecy, confidentiality, privacy, anonymity are different
  - Secrecy: Keep data hidden (e.g., incriminating evidence)
  - Confidentiality: Keep data hidden from unauthorized entities
  - Privacy: Both disclose and hide a person's data depending on correct context
  - Anonymity: Keep identify of a person secret

Recall CIA model

- Is confidentiality == privacy? NO
- Secrecy, confidentiality, privacy, anonymity are different
  - Secrecy: Keep data hidden (e.g., incriminating evidence)
  - Confidentiality: Keep data hidden from unauthorized entities
  - Privacy: Both disclose and hide a person's data depending on correct context
  - Anonymity: Keep identify of a person secret

Privacy: definitions

- Have a very extensive history
  - 1890: Warren and Brandeis (Law)
  - 1967: Alan Westin (Law)
  - 1975: Irwin Altman (Anthropology)
    - 1992: Sandra Petronio (CPM theory)
    - 2003: Palen and Dourish's interpretation
  - 2008: Daniel Solove (Solove's taxonomy
  - 2011: Helen Nissenbaum (Contextual integrity theory)

  - Privacy laws around the world

Privacy: definitions

- Have a very extensive history
  - 1890: Warren and Brandeis (Law)
  - 1967: Alan Westin (Law)
  - ~~1975: Irwin Altman (Anthropology)~~
    - ~~1992: Sandra Petronio (CPM theory)~~
    - ~~2003: Palen and Dourish's interpretation~~
  - 2008: Daniel Solove (Solove's taxonomy
  - 2011: Helen Nissenbaum (Contextual integrity theory)

  - Privacy laws around the world

Warren and Brandeis's theory

- "the protection afforded to thoughts, sentiments, and emotions, … enforcement of the more general *right of the individual to be let alone*"
  - Libel and slander are insufficient in considering only damage to reputation
  - The right to prevent, rather than profit from, publication of personal information
  - What about information of public figures / incidents?

Warren and Brandeis's theory (1890)

- "the protection afforded to thoughts, sentiments, and emotions, … enforcement of the more general *right of the individual to be let alone*"
  - Libel and slander are insufficient in considering only damage to reputation
  - The right to prevent, rather than profit from, publication of personal information
  - What about information of public figures / incidents? (Does not consider them)

Westin: Privacy as control (1967)

- "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."

--- Alan Westin

- Four states of privacy
  - Solitude: not observed by others
  - Intimacy: communicate with a small group
  - Anonymity: free from identification/surveilance
  - Reserve: limit information disclosure to others and others respecting the desire

Westin: Privacy as control (1967)

- Question:
  - X and Y are sitting in a restaurant and X was talking about his personal life.
  - Z, an eavesdropper sitting in the next table, are listening to them, although X did not realize it.
  - Can you explain, using Alan Westin's privacy definition and privacy states, if X's privacy is being violated in this scenario?

Solove's pluralistic notion of privacy

- Uses Wittgenstein's concept of 'family resemblances'
  - capture the notion of privacy people have in their mind
  - Privacy has many meanings
  - Like family resemblances, they are all related

- Focuses on data lifecycle
  - Different disruptions in each phase (data collection, processing, dissemination and invasion)
  - https://wiki.openrightsgroup.org/wiki/A_Taxonomy_of_Privacy

Solove's pluralistic notion of privacy

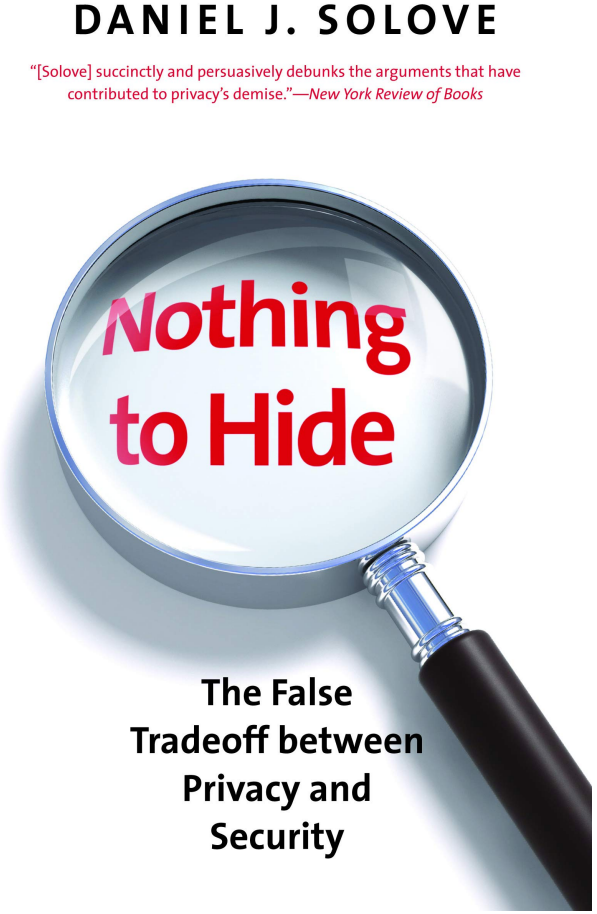
Information collection	surveillance (watching, listening to, or recording an individual's activities)
	interrogation (pressuring of individuals to divulge information)
Information processing	aggregation (gathering together information about a person)
	identification (connecting information to an individual)
	insecurity (problems caused by the way information is handled and protected)
	secondary use (use of data for purposes unrelated to the purposes for which the data was initially collected without the data subject's consent)
	exclusion (failure to provide individuals with notice and input about their records)

Solove's pluralistic notion of privacy

Information Dissemination	breach of confidentiality (breaking a promise to keep a person's information confidential)
	disclosure (revealing true information about a person to others)
	exposure (revealing another's nudity, grief, or bodily functions)
	increased accessibility (amplifying the accessibility of information)
	blackmail (threat to disclose personal information)
	appropriation (use of the data subject's identity to serve the aims and interests of another)
	distortion (the dissemination of false information about a person)
Invasion	intrusion (invasive acts that disturb one's tranquility or solitude)
	decisional interference (the government's incursion into the data subject's decisions regarding her private affairs)

An interesting application

a person should not worry about government or surveillance if they have "nothing to hide."



Nothing to hide

"When engaged directly, the nothing-to-hide argument can ensnare, for it forces the debate to focus on its narrow understanding of privacy. But when confronted with the plurality of privacy problems implicated by government data collection and use beyond surveillance and disclosure, the nothing-to-hide argument, in the end, has nothing to say."

Nothing to hide

"When engaged directly, the nothing-to-hide argument can ensnare, for it forces the debate to focus on its narrow understanding of privacy. But when confronted with the plurality of privacy problems implicated by government data collection and use beyond surveillance and disclosure, the nothing-to-hide argument, in the end, has nothing to say." (aggregation, secondary use)

Privacy as contextual Integrity (CI)

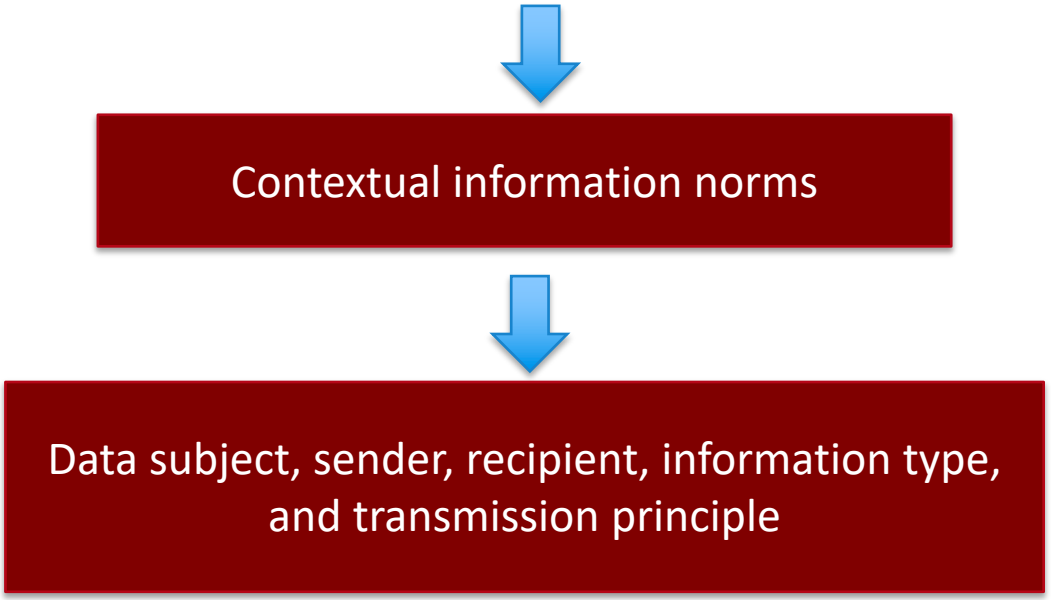
- A “normative” model of privacy
  - How privacy should be

- Considers “appropriate flow” of information
  - Appropriate flows conform to contextual informational norms
  - Each norm is : <Data subject, sender, recipient, information type, and transmission principle>
  - There are socially appropriate *norms*
  - Useful to systematically understand social norms: Evaluating the Contextual Integrity of Privacy Regulation: Parents' IoT Toy Privacy Norms Versus COPPA, N. Apthorpe, S. Varghese, N. Feamster, USENIX Security Symposium, 2019

Basic approach of CI

A framework to argue about privacy violation

Privacy is preserved by **appropriate flows of information**



Conceptions of privacy are based on **dynamic ethical concerns**

Roadmap

- What is privacy?
  - Privacy theories

- How to protect privacy?

Privacy laws around the world

- US has sector-specific laws, minimal protections
  - FTC investigates fraud & deceptive practices
  - FCC regulates telecommunications
- EU GDPR (general data protection regulation)
  - More later in the course

Fair Information practice principles (FIPP)

- Notice/Awareness: Consumers should be given notice of an entity's information practices before any personal information is collected from them

Fair Information practice principles (FIPP)

- Notice/Awareness: Consumers should be given notice of an entity's information practices before any personal information is collected from them
- Choice/Consent: Choice and consent in an on-line information-gathering sense means giving consumers options to control how their data is used

Fair Information practice principles (FIPP)

- Notice/Awareness: Consumers should be given notice of an entity's information practices before any personal information is collected from them
- Choice/Consent: Choice and consent in an on-line information-gathering sense means giving consumers options to control how their data is used
- Access/Participation: Not only a consumer's ability to view the data collected, but also to verify and contest its accuracy in inexpensive and timely manner

Fair Information practice principles (FIPP)

- Notice/Awareness: Consumers should be given notice of an entity's information practices before any personal information is collected from them
- Choice/Consent: Choice and consent in an on-line information-gathering sense means giving consumers options to control how their data is used
- Access/Participation: Not only a consumer's ability to view the data collected, but also to verify and contest its accuracy in inexpensive and timely manner
- Integrity/Security: Information collectors should ensure that the data they collect is accurate and secure

Fair Information practice principles (FIPP)

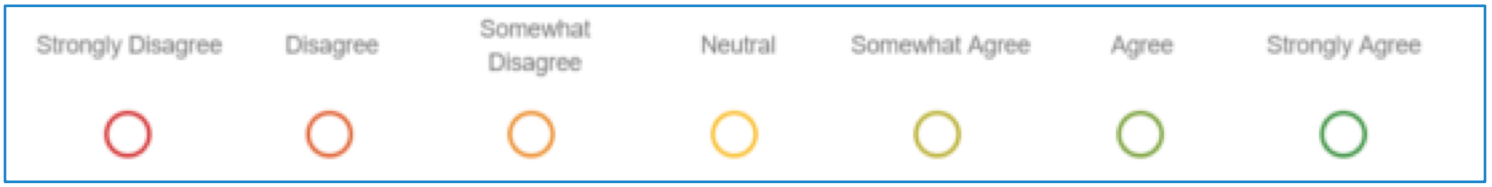
- Notice/Awareness: Consumers should be given notice of an entity's information practices before any personal information is collected from them
- Choice/Consent: Choice and consent in an on-line information-gathering sense means giving consumers options to control how their data is used
- Access/Participation: Not only a consumer's ability to view the data collected, but also to verify and contest its accuracy in inexpensive and timely manner
- Integrity/Security: Information collectors should ensure that the data they collect is accurate and secure
- Enforcement/Redress: In order to ensure that companies follow the Fair Information Practice Principles, there must be enforcement measures (self-regulation, sue by users, Government regulation)

Privacy enhancing tools

- Encryption (bitlocker)
- Anonymity (Tor, VPN)
- Tracker Blockers (ublock, adblocker)
- Opt-out tools (consent form, cookie banners)
- Social network privacy controls / Access control

How to measure privacy?

- Internet Users' Information Privacy Concerns (IUIPC)
  - 10 multiple choice questions divided into 3 sections: control, awareness, collection
  - Options are 7-point scale for each questions
    - From strongly disagree to strongly agree



- Malhotra, N.K., Kim, S.S., Agarwal,J., 2004. Internet users' information privacy concerns (IUIPC): the construct, the scale, and a causal model. Information Systems Research15(4), 336–355.

IUIPC control scale questions

1. Consumer online privacy is really a matter of consumers' right to exercise control and autonomy over decisions about how their information is collected, used, and shared.

2. Consumer control of personal information lies at the heart of consumer privacy.

3. I believe that online privacy is invaded when control is lost or unwillingly reduced as a result of a marketing transaction.

IUIPC awareness scale questions

1. Companies seeking information online should disclose the way the data are collected, processed, and used.

2. A good consumer online privacy policy should have a clear and conspicuous disclosure.

3. It is very important to me that I am aware and knowledgeable about how my personal information will be used.

IUIPC collection scale questions

1. It usually bothers me when online companies ask me for personal information.
2. When online companies ask me for personal information, I sometimes think twice before providing it.
3. It bothers me to give personal information to so many online companies.
4. I'm concerned that online companies are collecting too much personal information about me.