03. Conceptualizing & Measuring Privacy

Blase Ur and Mainack Mondal

April 2nd, 2018

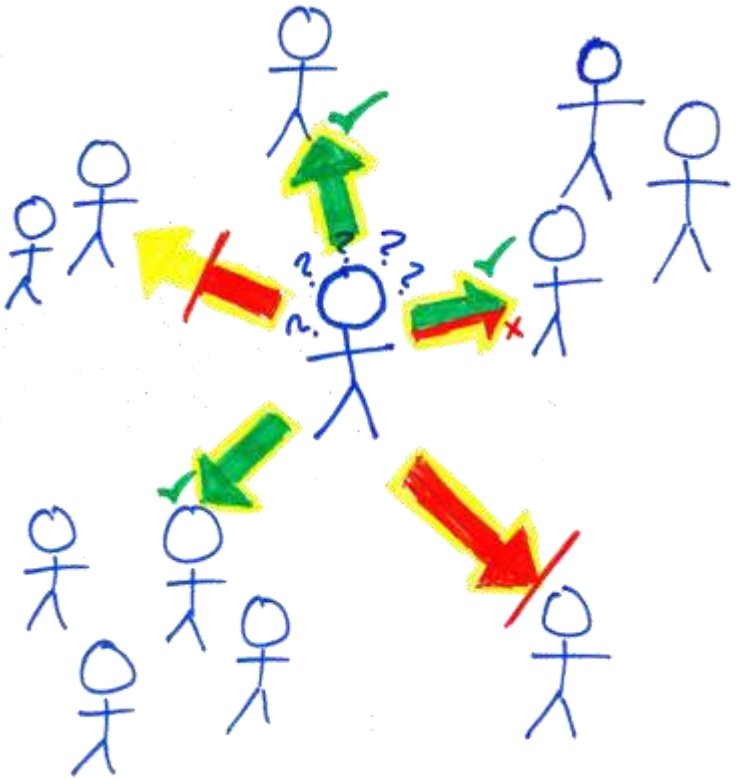
CMSC 23210 / 33210

THE UNIVERSITY OF CHICAGO

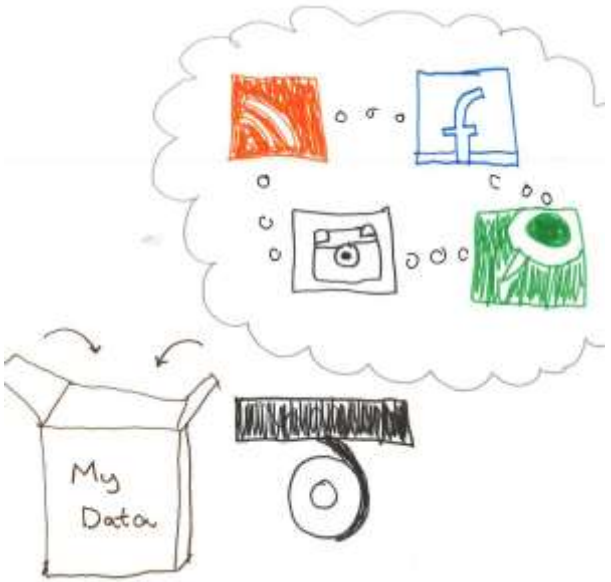
Security, Usability, & Privacy Education & Research

Today’s class

- Conceptualizing and measuring privacy



Conceptualizing & Measuring Privacy



Privacy is Hard to Define

"Privacy is a value so complex, so entangled in competing and contradictory dimensions, so engorged with various and distinct meanings, that I sometimes despair whether it can be usefully addressed at all."

Robert C. Post, Three Concepts of Privacy, 89 Geo. L.J. 2087 (2001).

Michael Wolf- The Transparent City

Michael Wolf- The Transparent City

"Chicago has recently undergone a surge of new construction…In early 2007, the Museum of Contemporary Photography…invited Michael Wolf as an artist-in-residence….Wolf chose to photograph the central downtown area, focusing on issues of voyeurism and the contemporary urban landscape….his details are fragments of life—digitally distorted and hyper-enlarged—snatched surreptitiously via telephoto lenses

http://aperture.org/shop/the-transparent-city/

Michael Wolf- The Transparent City

Michael Wolf- The Transparent City

Michael Wolf- The Transparent City

Michael Wolf- The Transparent City

Warren and Brandeis (1890)

HARVARD

LAW REVIEW.

VOL. IV. DECEMBER 15, 1890. NO. 5.

THE RIGHT TO PRIVACY.

"It could be done only on principles of private justice, moral fitness, and public convenience, which, when applied to a new subject, make common law without a precedent; much more when received and approved by usage."

WILLES, J., in Millar *v.* Taylor, 4 Burr. 2303, 2312.

THAT the individual shall have full protection in person and in property is a principle as old as the common law; but it has been found necessary from time to time to define anew the exact nature and extent of such protection. Political, social, and economic changes entail the recognition of new rights, and the common law, in its eternal youth, grows to meet the demands of society. Thus, in very early times, the law gave a remedy only

Warren and Brandeis's Inspiration

Warren and Brandeis's Argument

- "The individual shall have full protection in person and in property"
- The legal basis for fear
  - Battery → assault
  - Tangible property → intangible property
- Gossip pages about high society

Warren and Brandeis's Argument

- Libel and slander are insufficient in considering only damage to reputation
- Considers property rights
- The right to prevent, rather than profit from, publication
- **"The right to be let alone"**
- Excludes topics of general interest

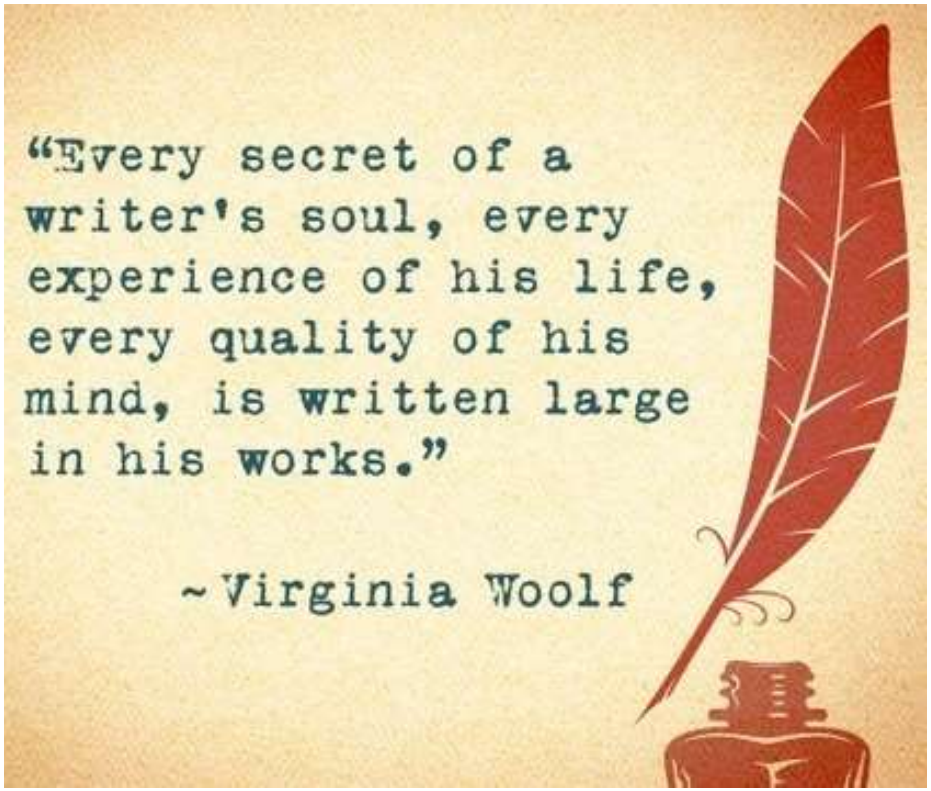
Photography Laws

Consent required for action related to a picture of a person in a public place (by country)

Country	Take a picture	Publish a picture	Commercially[1] use a published picture
Afghanistan	No	Yes (with exceptions)	Yes (with exceptions)
Argentina	No	Yes (with exceptions)	Yes (with exceptions)
Australia	No (with exceptions)	No (with exceptions)	Yes
Austria	No	No (with exceptions)	Yes
Belgium	No	Yes (with exceptions)	Yes
Brazil	Yes	Yes	Yes
Bulgaria	No	No	Yes
Canada	Depends on province	Yes (with exceptions)	Yes
China	No	No	Yes
Czech Republic	Yes (with exceptions)	Yes (with exceptions)	Yes (with exceptions)
Denmark	No	Yes (with exceptions)	Yes (with exceptions)
Ethiopia	No	Yes (with exceptions)	Yes
Finland	No	Yes (with exceptions)	Yes (with exceptions)
France	Yes (with exceptions)	Yes (with exceptions)[3]	Yes
Germany	No (with exceptions)	Yes (with exceptions)	Yes (with exceptions)
Greece	No	No	Yes (with exceptions)
Hong Kong	Depends on circumstances	Depends on circumstances	Depends on circumstances
Hungary	Yes (with exceptions)	Yes (with exceptions)	Yes (with exceptions)
United Kingdom	Depends on circumstances	Depends on circumstances	Depends on circumstances
United States	No	No	Usually (although laws differ by state)

https://commons.wikimedia.org/wiki/Commons:Photographs_of_identifiable_people#The_right_of_publicity

Is Being “Let Alone” Sufficient?



Privacy as Control / Secrecy (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."

"…each individual is continually engaged in a personal adjustment process in which he balances the desire for privacy with the desire for disclosure and communication…."

Alan Westin, Privacy and Freedom, 1967

Is Limiting Access Sufficient?

- Individuals sometimes prefer to be let alone, yet sometimes want to be social
  - Privacy was traditionally “social withdrawal”

Privacy Regulation Theory (1975)

- Irwin Altman (social psychology)
  - Preceded by Altman and Taylor's Social Penetration Theory (1973) about intimacy in relationships
- Dialectic and dynamic process of boundary regulation
  - Continuous movement on a continuum
- Goal: optimum balance of privacy and social interaction

CPM Theory (1991)

- Sandra Petronio (communications)
  - Communication Privacy Management Theory
- Regulate boundaries based on perceived costs and benefits
  - Movement on a continuum
- Expect rule-based management
- Boundary turbulence related to clashing expectations

Is Regulating Disclosure Enough?

Purpose Matters

The Washington Post

Local

Patients trusted Johns Hopkins gynecologist who allegedly videotaped them

By Brigid Schulte and Peter Hermann February 19, 2013 Email the author

For more than two decades, women came to see Johns Hopkins gynecologist Nikita Levy and trusted him with not only the most private parts of their bodies but also with their innermost secrets. Listening to problems with husbands and boyfriends, the joys and frustrations of motherhood, Levy was a caring confidant, said patients and co-workers.

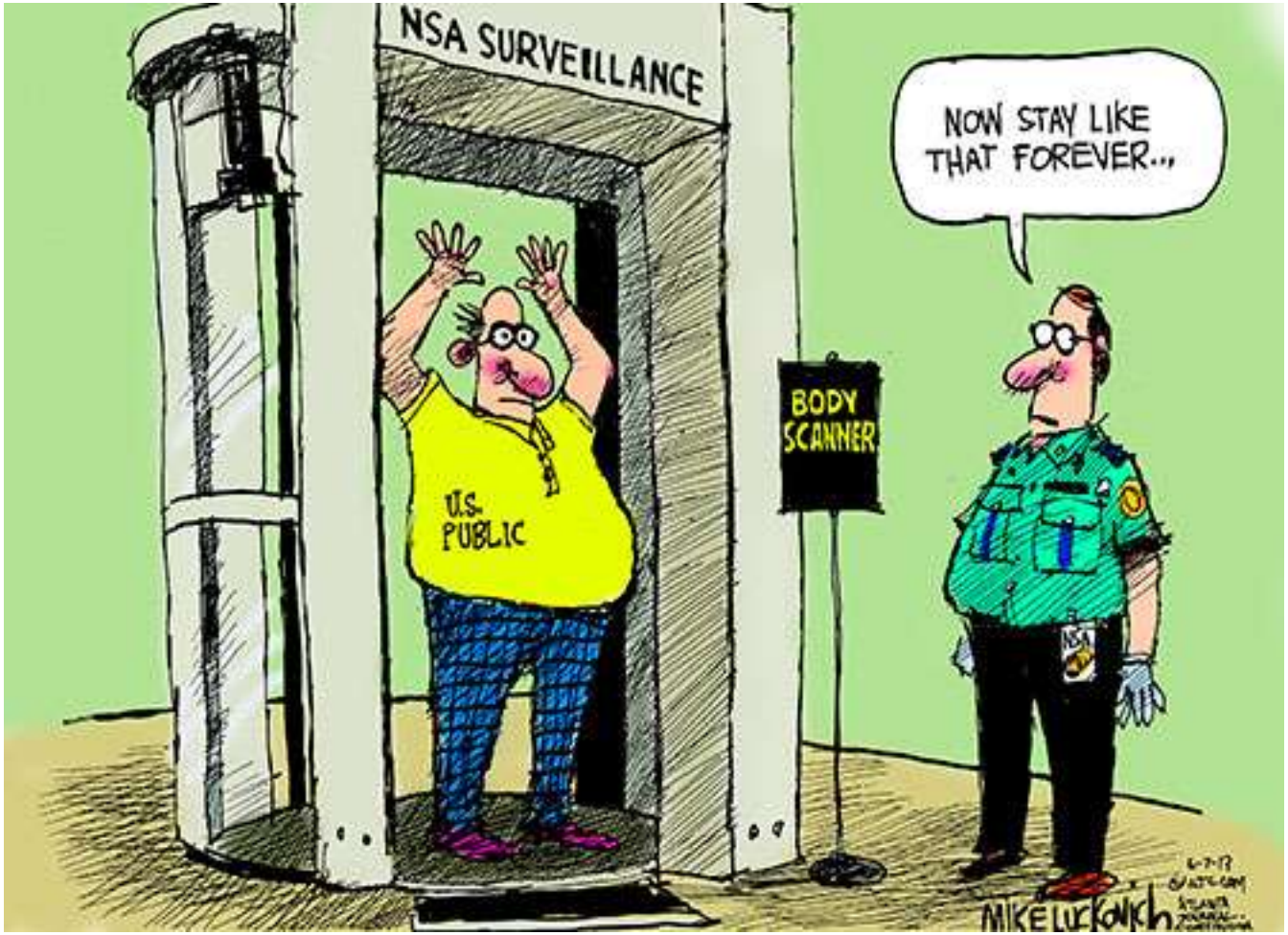
On Tuesday, they were reeling from the news that their doctor had committed suicide after being accused of surreptitiously videotaping and photographing many of his patients. Police said they have removed nearly 10 image-filled computer hard drives from Levy's home in Towson, Md.

(Details)

- “For 25 years, Dr. Nikita Levy ran an obstetrics and gynecology practice out of the East Baltimore Medical Center, a community clinic run by the Johns Hopkins Hospital and Health System. Last February, Johns Hopkins authorities discovered that Levy had been secretly filming his patients in the examination room, using cameras embedded into pens that he wore around his neck and key fobs he carried in his pockets. At his home, police found hard drives and servers stocked with thousands of videos and photographs of his patient’s naked bodies, snapped under the auspices of performing routine pelvic examinations.”

http://www.slate.com/blogs/xx_factor/2014/07/22/johns_hopkins_190_million_ob_gyn_settlement_it_won_t_buy_closure_for_nikita.html

Purpose Matters (?)



Privacy as Contextual Integrity (2004)

- Helen Nissenbaum (philosophy)
- “Contextual integrity ties adequate protection for privacy to norms of specific contexts, demanding that information gathering and dissemination be appropriate to that context.”

Privacy as Contextual Integrity

- Appropriate flows of information
- Appropriate flows conform to contextual information norms
- Norms refer to the data subject, sender, recipient, information type, and transmission principle
- Conceptions of privacy evolve over time and are grounded in ethics

Dan Solove's Pluralistic Conceptions

- Some data isn't "sensitive," but its collection and use impact privacy
  - Impact power relationships
  - Kafka-esque
- Solove's privacy taxonomy
  - Information collection
  - Information processing
  - Information dissemination
  - Invasion

Important terms

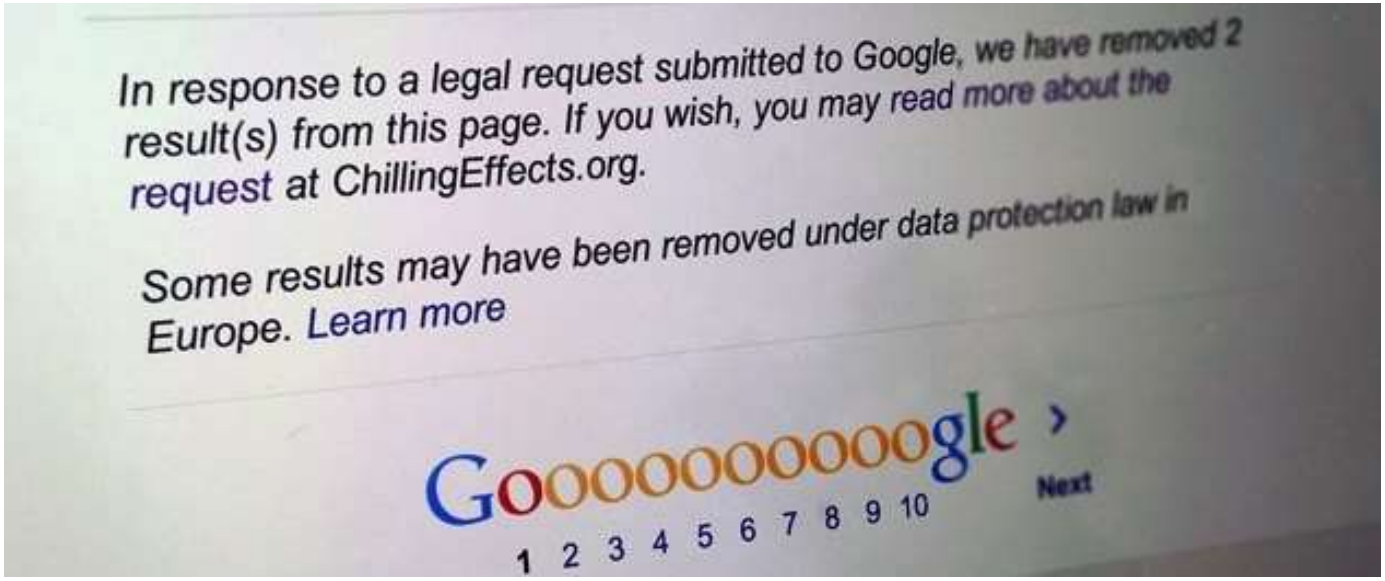
- **Chilling effect**: discouragement of exercising a legitimate right
- **Privacy paradox**: behaviors are inconsistent with concerns
- **Privacy by design**: consider privacy throughout the lifecycle of a product
- **Secondary use**: those other than the intended purpose

Issues of privacy

- Can conflict with free speech / security
- How do we quantify privacy harms?
- Can we measure chilling effects?
- How do we provide transparency?
- Distortion: false of misleading information
- Data mining → future activities?
- Oversight and accountability

Right to be forgotten

- Should a person have the agency to cause items from the past to be removed?
- Who owns information?
- EU



How does each goal relate to privacy?

I want to have…

- Solitude, uninterrupted
- Unseen, unheard, unread
- Not talked about
- Not judged
- Not profiled, not targeted, not treated differently than others
- Not misjudged
- Free to try, practice, make mistakes, self-reflect
- Not surprised (contextual integrity)
- Not accountable

I want to be….

- Not required to reveal
- Unknown
- Forgotten
- Intimacy
- Control
- Boundaries
- Identity
- Security
- Safety
- Others?

Measuring privacy

- Why is privacy hard to measure?
- Why are attitudes about privacy hard to measure?
- Why is the cost of privacy invasion hard to measure?

How privacy is protected

- Laws, self regulation, technology
  - Notice and access
  - Control over collection, use, deletion, sharing
  - Collection limitation
  - Use limitation
  - Security and accountability

Privacy laws around the world

- US has mostly sector-specific laws, minimal protections, often referred to as “patchwork quilt”
  - No explicit constitutional right to privacy or general privacy law
  - Some privacy rights inferred from constitution
  - Narrow regulations for health, credit, education, videos, children
  - FTC investigates fraud & deceptive practices
  - FCC regulates telecommunications
  - Some state and local laws
- Data Protection Directive - EU countries must adopt similar comprehensive laws, recognize privacy as fundamental human right
  - Privacy commissions in each country

OECD Fair Information Principles

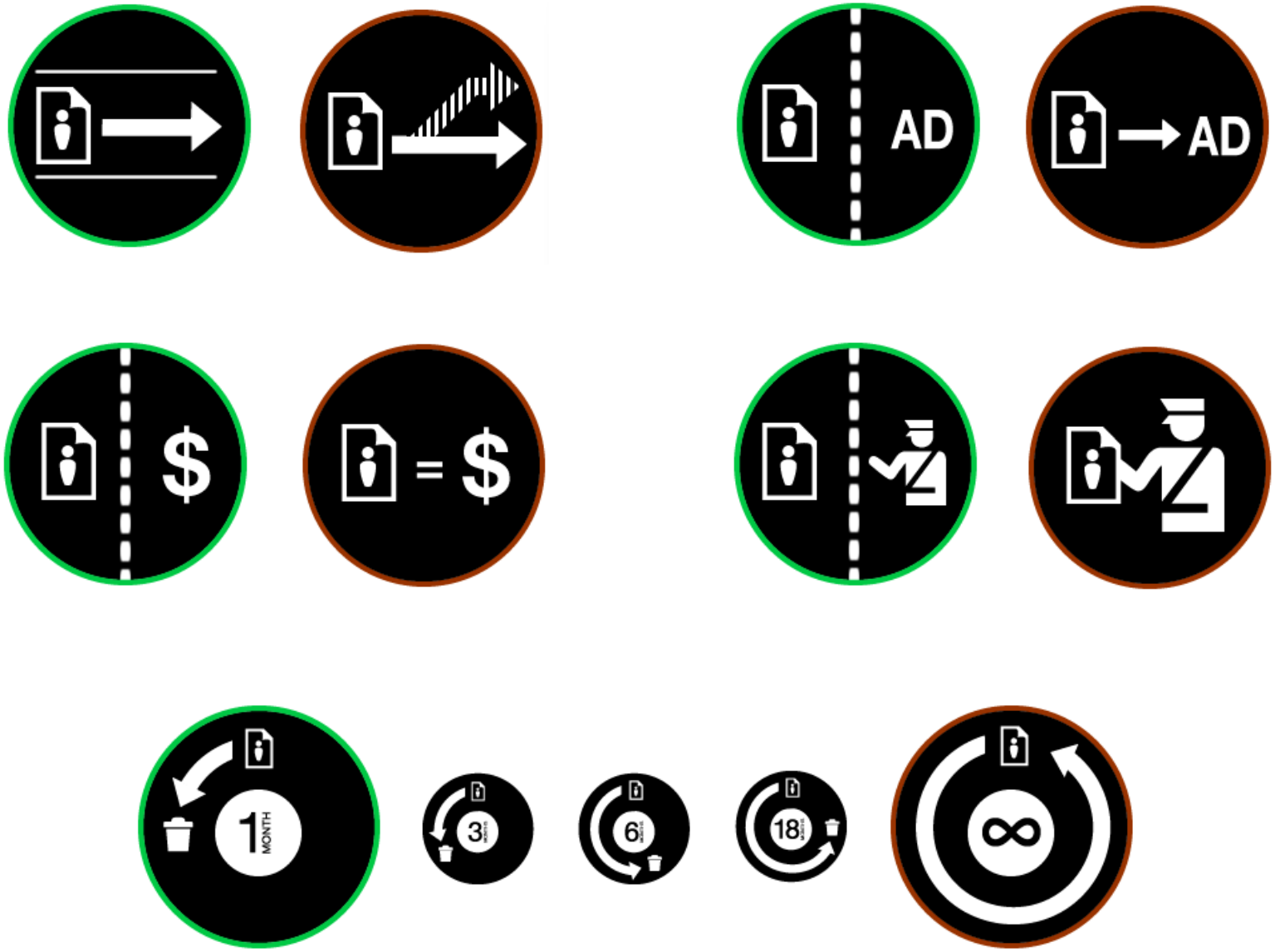
- Collection limitation
- Data quality
- Purpose specification
- Use limitation
- Security safeguards
- Openness
- Individual participation
- Accountability
- http://www.privacyrights.org/ar/fairinfo.htm

US FTC's Fair Information Practice Principles (FIPPs)

- Notice / Awareness
- Choice / Consent
- Access / Participation
- Integrity / Security
- Enforcement / Redress
- https://en.wikipedia.org/wiki/FTC_Fair_Information_Practice

Privacy Icons

http://www.azarask.in/blog/post/privacy-icons/ *2010*



k-Anonymity (1998)

- Latanya Sweeney / Pierangela Samarati
- Each person cannot be distinguished from k-1 other individuals in the database

Name	Age	Gender	State of domicile	Religion	Disease
*	20 < Age ≤ 30	Female	Tamil Nadu	*	Cancer
*	20 < Age ≤ 30	Female	Kerala	*	Viral infection
*	20 < Age ≤ 30	Female	Tamil Nadu	*	TB
*	20 < Age ≤ 30	Male	Karnataka	*	No illness
*	20 < Age ≤ 30	Female	Kerala	*	Heart-related
*	20 < Age ≤ 30	Male	Karnataka	*	TB
*	Age ≤ 20	Male	Kerala	*	Cancer
*	20 < Age ≤ 30	Male	Karnataka	*	Heart-related
*	Age ≤ 20	Male	Kerala	*	Heart-related
*	Age ≤ 20	Male	Kerala	*	Viral infection

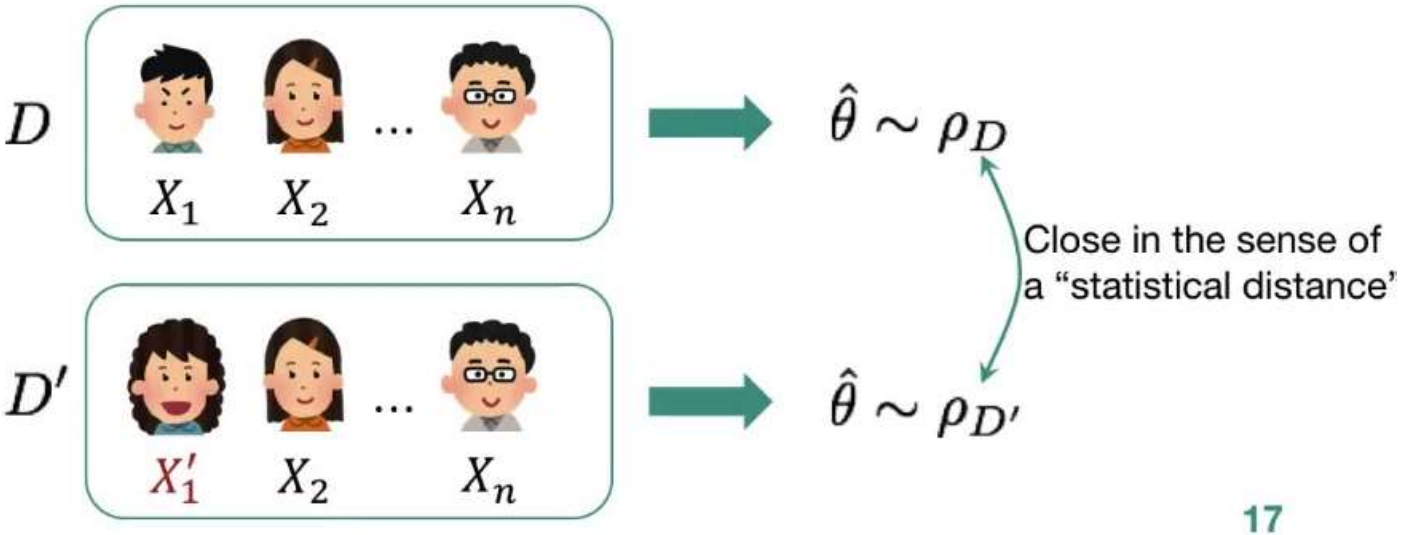
https://en.wikipedia.org/wiki/K-anonymity

Differential Privacy

- Cynthia Dwork, Frank McSherry, Kobbi Nissim, Adam D. Smith

Idea:

2. Two "adjacent" datasets differing in a single individual should be statistically indistinguishable



Differential Privacy

- 2020 US Census data will be protected by differential privacy
  - https://privacytools.seas.harvard.edu/why-census-bureau-adopted-differential-privacy-2020-census-population