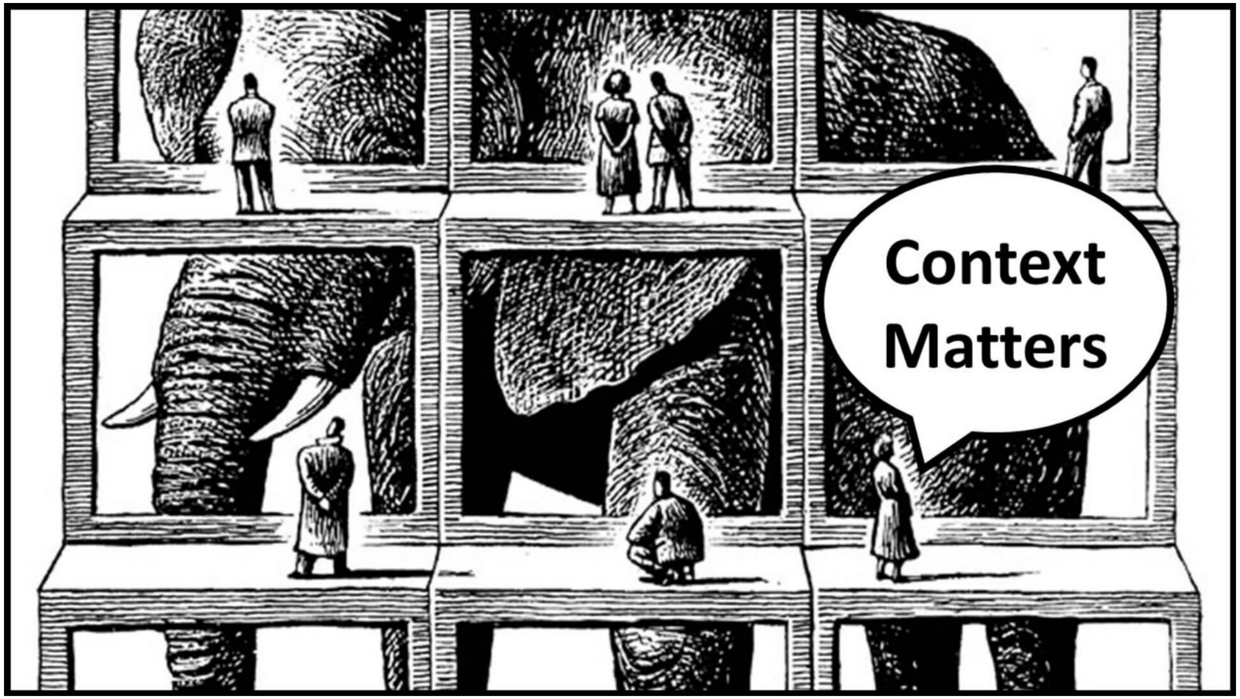


Nissenbaum: Privacy as contextual integrity

Privacy is not „either-or“

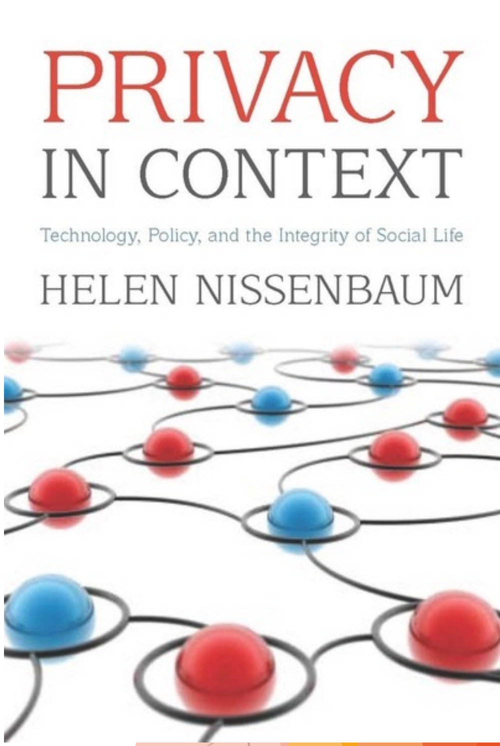
- Often assumption of dichotomy between privacy and publicity, reflected in legal norms regarding private vs public information
- but not doing justice to the specific features of informational norms in a given context
- particularly problematic in the field of digital data practices, e.g.:
    - Private information can be deduced from specific public characteristics
    - Publicly available information can become more sensitive when it becomes accessible beyond the local
- Importance of having an analytic framework that allows more ethically differentiated reflection on the impact of new and emerging data practices

4 core claims (Nissenbaum 2019)

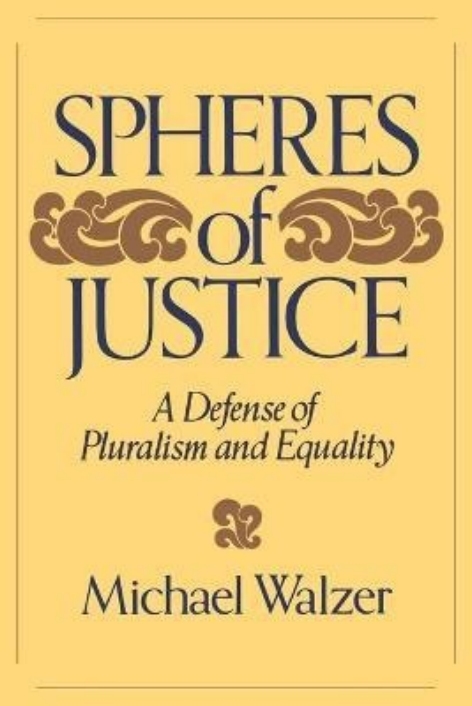
- 1. Privacy is the appropriate flow of personal information
- 2. Appropriate flows conform with contextual informational norms or “privacy norms”
- 3. Five Parameters Define Privacy (Contextual Informational) Norms:
  - Subject, Sender, Recipient, Information Type, and Transmission Principle
- 4. The Ethical Legitimacy of Privacy Norms is Evaluated in Terms of:
  - A) Interests of Affected Parties, B) Ethical and Political Values, and C) Contextual Functions, Purposes, and Values

Spheres/contexts of privacy

- Our activities take place in different social spheres, i.e. specific contexts that have specific norms about how people interact, what to expect, what others will do with information they receive in those contexts
- “[People] are at home with families, they go to work, they seek medical care, visit friends, consult with psychiatrists, talk with lawyers, go to the bank, attend religious services, vote, shop, and more. Each of these spheres, realms, or contexts involves, indeed may even be defined by, a distinct set of norms, which governs its various aspects such as roles, expectations, actions, and practices.” (Nissenbaum, 2004, p. 137)
- Importance of functions, purposes (goals, ends), and values around which contexts are oriented (Nissenbaum 2019, p.226)



Walzer’s theory as philosophical foundation for contextual norms



SPHERES of JUSTICE

A Defense of Pluralism and Equality

Michael Walzer

- Nissenbaum refers to Michael Walzer’s understanding of justice in his “Spheres of justice” as model for her understanding of privacy
- communitarian approach that focuses on the idea of specific social goods/values implicit in or embodied by specific spheres of activity
- Particularity of “history, culture and membership” as crucial for understanding communities
- Communities characterised by pluralistic values, valuing various social goods
- Each value comes with specific distributive norms, no overarching clear ordering system that is independent of the spheres

Norms of appropriateness and norms of distribution of information

- Each context defines what is appropriate to disclose and do with information and what values govern the information practices in this context
- Norms of appropriateness: “circumscribe the type or nature of information about various individuals that, within a given context, is allowable, expected, or even demanded to be revealed” (138)
- Norms of distribution: these norms identify what kinds of information flow can be expected in a given context,
  - e.g. differences in where information can flow from doctors, tax office, strangers, close friends…
- Proposal: identify established norms applying to past contexts of use and aim to apply and adapt to new technology

Contextual integrity and social media – continuity or novelty?

- Social media originally conceived as way of facilitating people to connect who may already be connected in real life or be likely to connect
- value: connection, intimacy, mutual understanding, shared action
- Contextual integrity: should normal norms of information flow in social contexts apply to social media? E.g. mirror information flow of human conversations (or “normal” gossip)?
- Differences:
    - Widening range of people and accelerated social dynamics
    - Highly curated self-presentation (including e.g. automated beauty filters on Snapchat)
    - Curated newsfeed, selected for “engagement” (i.e. contributions selected by emotional relevance, unlike timeline as e.g. Tumblr)
    - Massive backstage data collection e.g. with facebook button on webpages
    - Vehicle for advertising, including e.g. personalised “endorsement” of ads by friends on facebook

The end of “Privacy in Public”

- what was previously public but “ephemeral” becomes permanent and widely accessible in the digital realm
- Difference between:
- talking to somebody in public park (public, but mostly anonymous and soon forgotten)
- chatting to somebody on a public Twitter feed (public, archived, accessible/searchable to anybody who cares to look for conversations with keywords you used, and combinable with other sources of information to potentially re-identify you)

Innocuous components can combine to harmful product

- Claim: privacy risks arising from new ways of combining and processing personal data: simple “data primitives” can be easily converted to highly meaningful personal information with potentially risky uses
- Comparing this with individually innocuous components that can be brought together to create a dangerous bomb (Nissenbaum 2019, p.246)