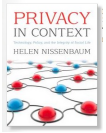
1

Privacy → data governance?

There's a lot going on in the world of privacy regulatory efforts + industry ("PETs") + pressure from academia and advocacy



Contextual Integrity is a different way of thinking about privacy

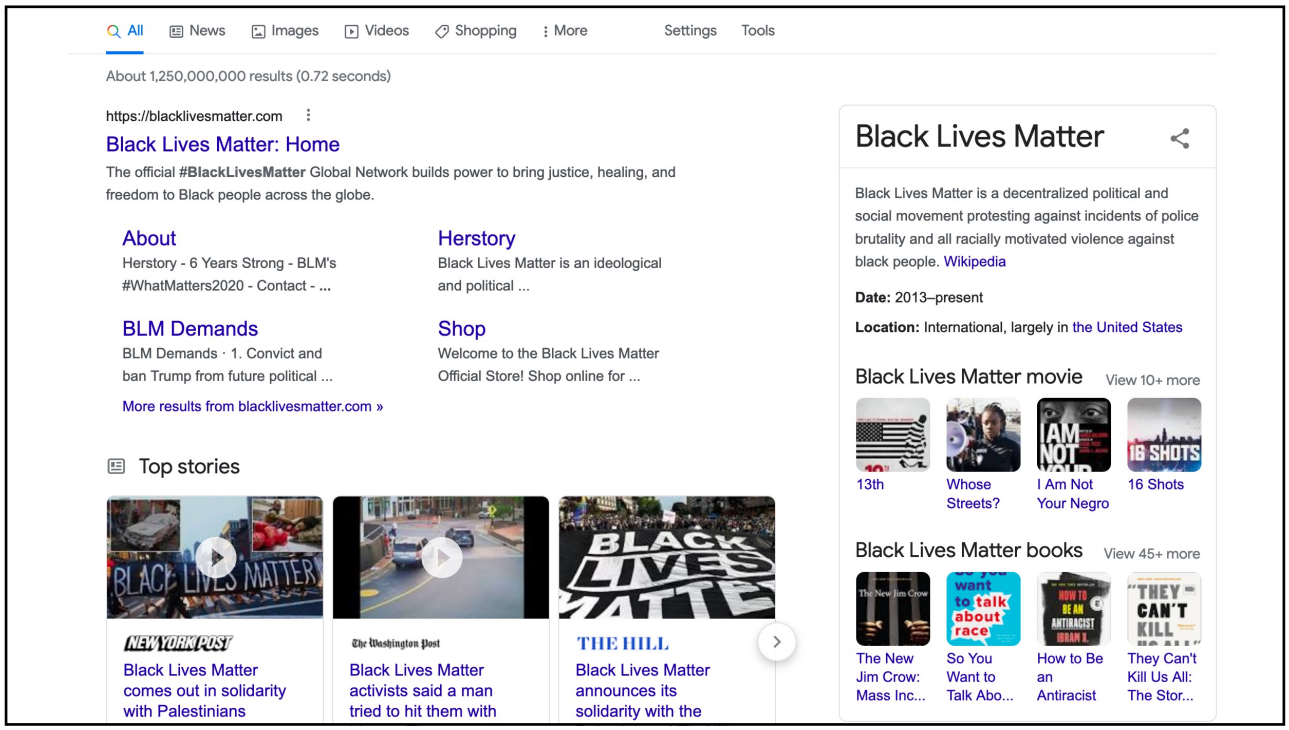
2


iOS
amazon
Meta
OpenAI
ChatGPT
Alphabet

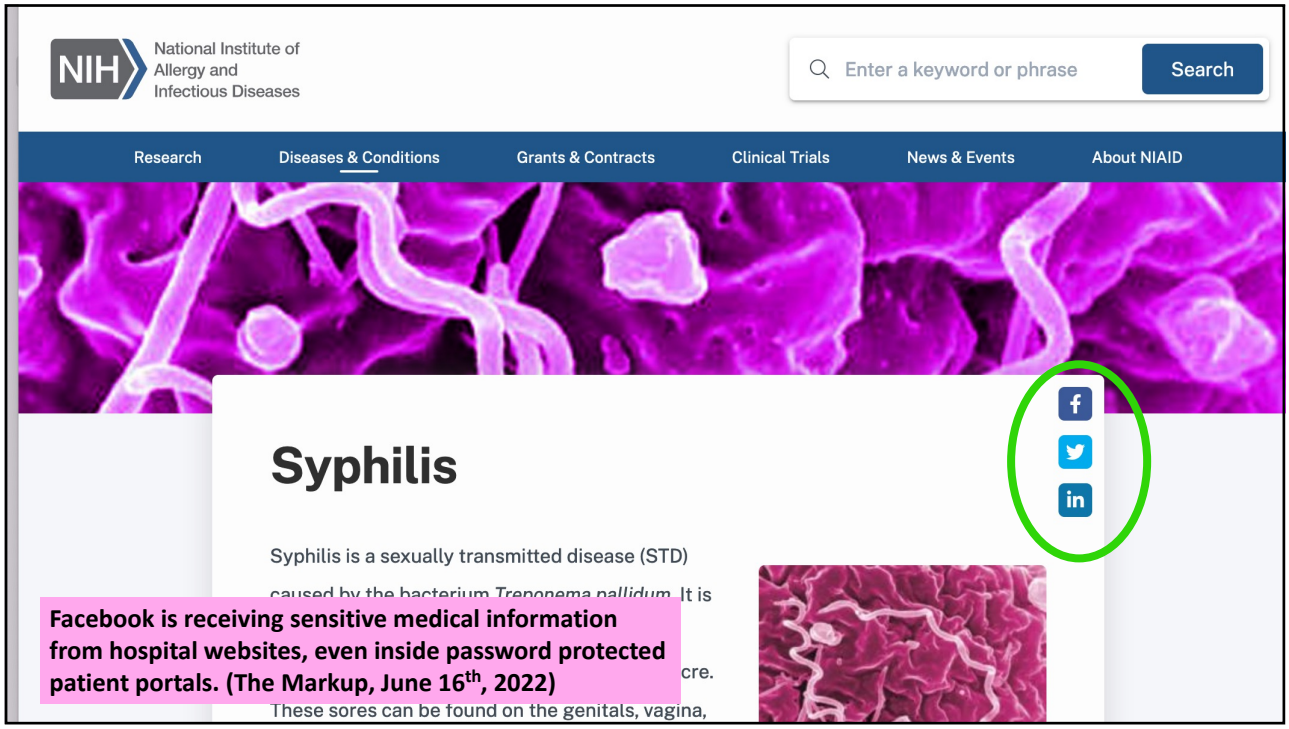
3


Health tracking tech
Mobile & Web
Sun exposure
Fitness
GLOW
For fertility and beyond
Fertility Calendar & Period Tracker
Daily Health Log
Health Insights
Partner Connected
Fertility+Period
Mood Panda
Mental health

4


All
News
Images
Videos
Shopping
More
Settings
Tools
About 1,250,000,000 results (0.72 seconds)
https://blacklivesmatter.com
Black Lives Matter: Home
The official #BlackLivesMatter Global Network builds power to bring justice, healing, and freedom to Black people across the globe.
About
Herstory - 6 Years Strong - BLM's #WhatMatters2020 - Contact - ...
Herstory
Black Lives Matter is an ideological and political ...
BLM Demands
BLM Demands · 1. Convict and ban Trump from future political ...
Shop
Welcome to the Black Lives Matter Official Store! Shop online for ...
More results from blacklivesmatter.com »
Top stories
NEW YORK POST
Black Lives Matter comes out in solidarity with Palestinians
The Washington Post
Black Lives Matter activists said a man tried to hit them with
THE HILL
Black Lives Matter announces its solidarity with the
Black Lives Matter
Black Lives Matter is a decentralized political and social movement protesting against incidents of police brutality and all racially motivated violence against black people. Wikipedia
Date: 2013–present
Location: International, largely in the United States
Black Lives Matter movie
View 10+ more
13th
Whose Streets?
I Am Not Your Negro
16 Shots
Black Lives Matter books
View 45+ more
The New Jim Crow: Mass Inc...
So You Want to Talk Abo...
How to Be an Antiracist
They Can't Kill Us All: The Stor...

5


NIH
National Institute of Allergy and Infectious Diseases
Enter a keyword or phrase
Search
Research
Diseases & Conditions
Grants & Contracts
Clinical Trials
News & Events
About NIAID
Syphilis
Syphilis is a sexually transmitted disease (STD)
caused by the bacterium Treponema pallidum. It is
These sores can be found on the genitals, vagina,
Facebook is receiving sensitive medical information from hospital websites, even inside password protected patient portals. (The Markup, June 16th, 2022)

6

Digital Technologies Threaten Privacy!

GPS, mobile, implantable devices, RFID, CCTV, Sensors, networked sensors, image, video and audio, Web cookies, flash cookies, web bugs, cross device, browser tracking

Collect, Track, Surveil, Monitor,

"Big Data," Databases, data aggregation, mining, predictive modeling, machine learning, data science, data analytics, **AI**, biometrics, facial recognition, recommendation

Profile, predict, target, manipulate

Internet, Web, IoT, social computing, social networks, Email, mobile tech, "gig" work

Distribute, communicate, network, platforms

7

8

Need a conception that holds up, explains, guides, justifies

9

Privacy as Contextual Integrity

Key ideas

https://nissenbaum.tech.cornell.edu/

10

Benchmarks

[A meaningful conception of privacy]

faithful to common use

Clear and rigorous

reveals privacy's ethical significance

explains the technology challenges

informs technology & policy

11

Contextual Integrity

Is Not

12

Contextual Integrity (CI): The one-liner

(The right to) privacy is (a right to)

appropriate information flow

13

Contextual Integrity (CI): The one-liner

(The right to) privacy is (a right to)

appropriate information flow

Why flow?

14

KEY IDEAS

1. Appropriate flow
2. Contextual informational norms [policy+technology]
3. Legitimacy (rules & practices) [moral standing]

We'll return to this later

15

CI Building blocks

16

Social Contexts

- Differentiated social spheres
  - E.g. health, education, family, politics, commerce
- May differ across nations, historical times, cultures
- Interact with one another in complicated ways
  - overlap, be nested, include specific institutions
- Constituted by functions, practices; distinctive ontologies of roles and information types;
- Governed by contextual norms & rules
  - Include information flow norms, rules, expectations
- Defined by contextual purposes, goals, values

17

Contexts

- Differentiated social spheres
  - E.g. health, education, family, politics, commerce
- May differ across nations, historical times, cultures
- Interact with one another in complicated ways
  - overlap, be nested, include specific institutions
- Defined by purposes, goals, values
- Constituted by functions; practices; distinctive ontologies of roles and information types [has semantics]
- Governed by contextual norms & rules
  - Include information flow norms, rules, expectations

18

Contextual Informational Norms

<actors*: subject, sender, recipient>, <attributes*>, <transmission principle>

Actors: Physician, bank, merchant, police, Verizon, shopper, reader, advertiser, voter, insurance company, mother, spouse, teacher, friend, student, FBI, CIA, neighbor

Information type: Age, gender, books you've read, movies you've seen, purchases, whether you voted in previous election, salary, address, medical diagnosis, SSN, facial image, what you paid for your house, GPA, spoons of sugar in your coffee, sexual orientation

Transmission Principle: Consent, coerce, compel, steal, buy, sell, in confidence, surreptitiously, with notice, with a warrant, with authorization, reciprocity

---

*acting in capacities

*contextual ontologies

19

<subject><sender><recipient><information type> <transmission principle>

See cultural differences?

Schools must provide parents with information about their children's academic progress.

Universities must provide parents with information about their children's academic progress (with children's permission?)

Universities must provide companies with information about students' academic progress (with students' permission?)

Friends do not ask each other how much they paid for their apartments.

An interviewer is forbidden from asking a job candidate his/her religion

Travelers are obliged to show contents of their luggage to the TSA agents upon request.

20

ALL THE PARAMETERS MATTER!

A Rule must specify values for all parameters!

<subject> • <sender> • <recipient> • <attributes> • <TPs>

21

From Privacy Rule: US Health Insurance Portability & Accountability Act

A covered entity may disclose protected health information about an individual who has died to a law enforcement official for the purpose of alerting law enforcement of the death of the individual if the covered entity has a suspicion that such death may have resulted from criminal conduct." (1996)

22

From HIPAA privacy rules

Sender role — Subject role

A covered entity can disclose a patient's

Attribute — psychotherapy notes to the patient — Recipient role

only with prior approval from the patient's psychiatrist

Transmission principle

Exactly as **Contextual Integrity** says!

In our formal policy language,

$$\Box\forall p_1, p_2, q : P.\forall m : M.\forall t : T.$$
$$\text{incontext}(p_1, c) \wedge \text{send}(p_1, p_2, m) \wedge \text{contains}(m, q, t) \rightarrow$$
$$\text{inrole}(p_1, \textit{covered-entity}) \wedge \text{inrole}(p_2, \textit{individual}) \wedge (q = p_2) \wedge (t \in \textit{psychotherapy-notes}) \rightarrow$$
$$\diamondsuit\exists p : P.\, \text{inrole}(p, \textit{psychiatrist}) \wedge \text{send}(p, p_1, \textit{approve-disclose-psychotherapy-notes})$$

H. DeYoung, D.Garg, L. Jia, D. Kaynar, A. Datta, Experiences in the Logical Specification of the HIPAA and GLBA Privacy Laws, in *Proceedings of 9th ACM Workshop on Privacy in the Electronic Society*, October 2010.

23

Privacy DEFINITION: 1ST APPROXIMATION

Privacy as CI is satisfied iff:
information flows conform with
entrenched informational norms
(meet privacy expectations)

24

HEURISTIC (1st approximation)

Assessing an existing practice or evaluating a design alternative:

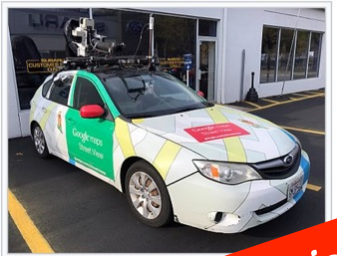
- Trace out data flows in terms of CI parameters
- Locate and map onto relevant privacy norms
- Check conformance

>Yes ✓
>No ✗
>other ?

25

Google Maps Street View, launched 2007

Privacy concerns



A Street View car park
Subaru Servi
New Jerse

Main article: Google Street View privacy concerns

Google Street View will blur houses for any user who m
to the automatic blurring of faces and licenc
objected to the Google Street Vie
strip clubs, protesters a ers in bil
engaging in property in which th
cern is the height of the came
and Switzerland,[45] Google has had to
so as to not peer over fences and hedges. The se
themselves to flag inappropriate or sensitive imagery for Go
remove.[46] Police Scotland received an apology for wastin
from a local business owner in Edinburgh who in 2012 had
for the Google camera car by lying in the road "while his colleague stood over him with a pickaxe ha
it was revealed that Google had collected and stored payload data from unencrypted Wi-Fi connecti
View.[48][49]

Google missed changes in recipients & TPs

Google Street View

26

27

Contextual Integrity – NOT

No flow, no collection, secrecy [access]

……..of sensitive information

Control over personal information [control]

…….that is sensitive

Balance and trade off

28

Contextual Integrity – NOT

No flow, no collection, secrecy
…….of sensitive information
Control over personal information
…….that is sensitive
Balance and trade off

29

? faithful to common use
? moral standing

30

Demonstrating that secrecy, even moderated by the private/public dichotomy **does not map onto privacy expectations**

Three empirical studies (with K. Martin):

I. CI Reveals Confounding Variables in "sensitive" data flows
II. CI Exposes Privacy Expectations in Public Records
III. CI Reveals Privacy Expectations in Location Data collected in public

Others empirical studies

I. CI and privacy expectations for IoT devices
II. "Contextual expectations of privacy" [Selbst, 2013]
III. CI reveals surprising practices of disaster apps
IV. CI exposes impossibility of privacy through Notice & Choice

31

Factorial Vignette Survey Method

Recipient:
- *Car Dealership D….all potential car buyers*
- *Bank B…all potential loan applicants*
- *A curious guest….the hosts of an upcoming neighborhood party*
- *Company C….all job applicants*

Recipient gathers information about Subject including **Information Type** which recipient learns by **Source**.

Source:
- *by consulting a data broker (i.e., a company that sells data)*
- *by asking them*
- *by checking online government records*

Information Type:
- *their marital status*
- *whether they had a criminal record*
- *whether they voted in the last election*
- *how much they paid for their home*

Is it OK? -100 to +100

Factor	Operationalized in Vignette		
Information	Marriage Records	their marital status	
	Court Records	whether they had a criminal record	
	Voter Records	whether they voted in the last election	
	Property Records	how much they paid for their home	
Source	Data Broker	by consulting a data broker (i.e., a company that sells data)	
	Subject	by asking them	
	Online Records	by checking online government records	
		Subject	**Recipient**
Context	Retail	all potential car buyers	Car Dealership D
	Bank	all potential loan applicants	Bank B
	Social	the hosts of an upcoming neighborhood party	a curious guest
	Employment	all job applicants	Company C

32

THE COLUMBIA
SCIENCE & TECHNOLOGY
LAW REVIEW

I. It's OK for "private" information to flow

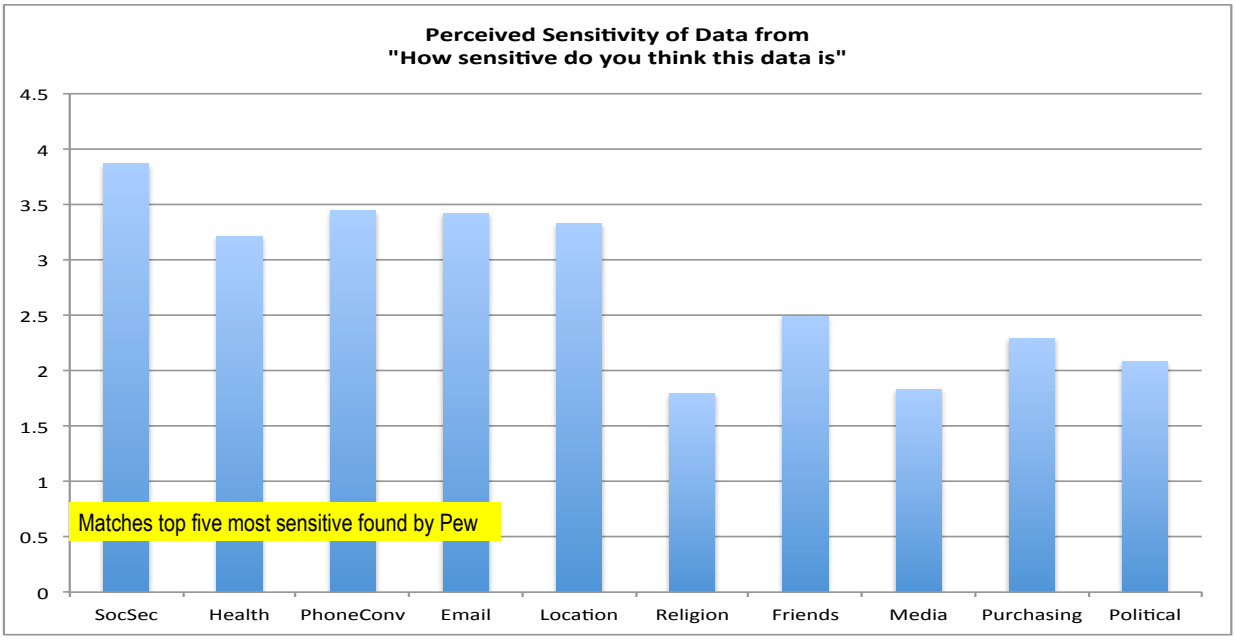
ARTICLE

MEASURING PRIVACY: AN EMPIRICAL TEST USING CONTEXT TO EXPOSE CONFOUNDING VARIABLES †

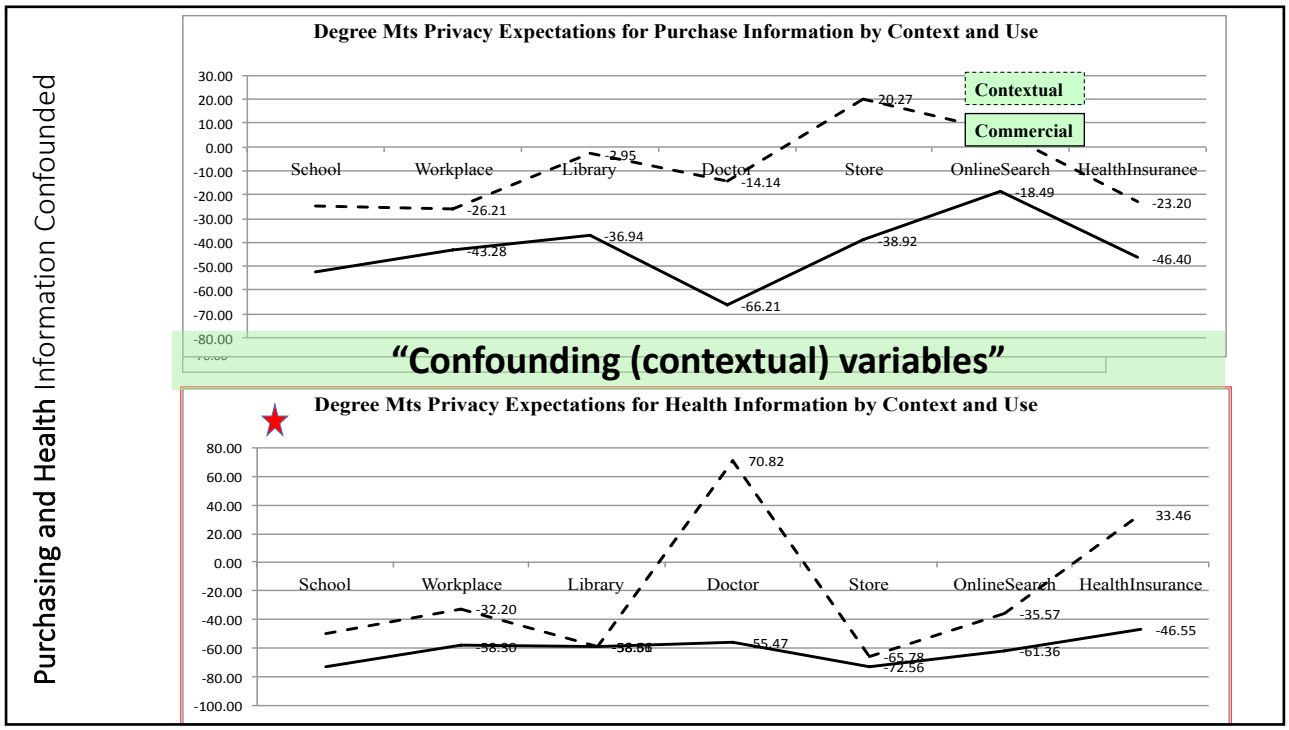
Kirsten Martin and Helen Nissenbaum*

33

Results for Sensitive Information questions



34



35

HARVARD JOURNAL OF LAW & TECHNOLOGY

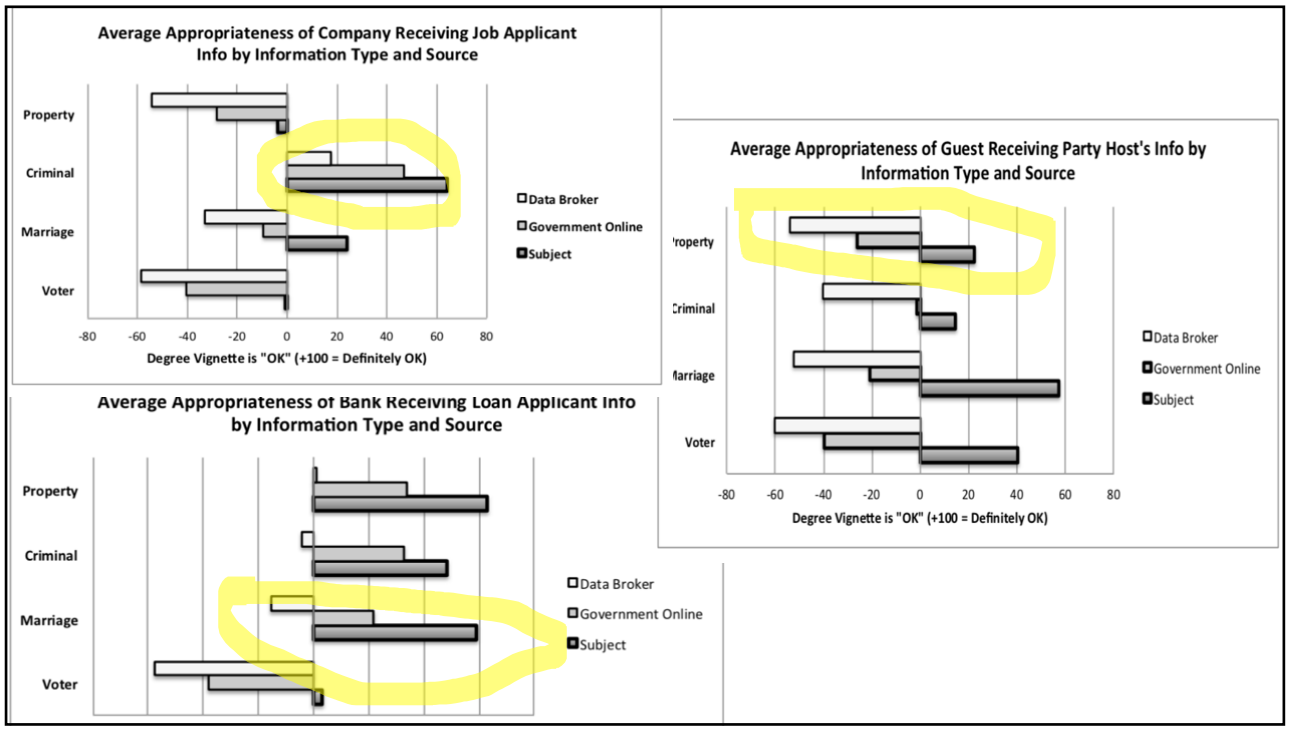
II. Privacy Interests in "public" information

ARTICLE

PRIVACY INTERESTS IN PUBLIC RECORDS: AN EMPIRICAL INVESTIGATION
Kirsten Martin & Helen Nissenbaum

NOT "Anything goes!"

36



37

Takeaways

1) Even if data is judged to be sensitive, people still are positive when the flow is appropriate

2) Even if data is available in public records, responses were sensitive to all the parameters are.

38

Caution

Much regulation and technology design presumes the dichotomy is a good proxy.

EG: GDPR

39

Clearview AI

Scraped over **30 billion** photos from social media & other public websites.

Used over 1 million times by 2,400 U.S. law enforcement agencies

"Publicly available photos and information derived from them: As part of Clearview's normal business operations, it collects photos that are publicly available on the internet. The photos may contain metadata which may be collected by Clearview due to it being contained in the photos, and information derived from the facial appearance of individuals in the photos." From Privacy Policy

Large Language Models

2.7 Privacy

GPT-4 has learned from a variety of licensed, created, and publicly available data sources, which may include publicly available personal information. [58, 59] As a result, our models may have knowledge about people who have a significant presence on the public internet, such as celebrities and public figures. GPT-4 can also synthesize multiple, distinct information types and perform multiple steps of reasoning within a given completion.

40

Caution

Much regulation and technology design presumes the dichotomy is a good proxy.

Per CI: This approach is reductive
& Does not align with common expectations

41

Contextual Integrity – NOT

No flow, no collection, secrecy
……..of sensitive information
Control over personal information
……that is sensitive
Balance and trade off

42

Reduces privacy to one parameter –TP- and accepts only one value for it!

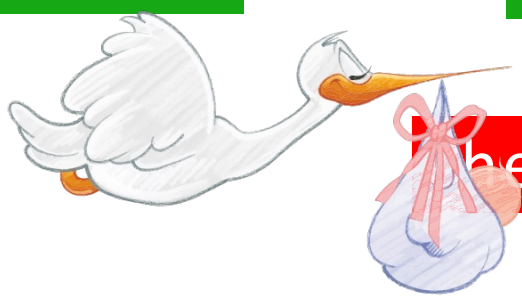
"notice + choice"
"informed consent"
present-day
privacy nightmare

43

Guided by Fair Information Principles

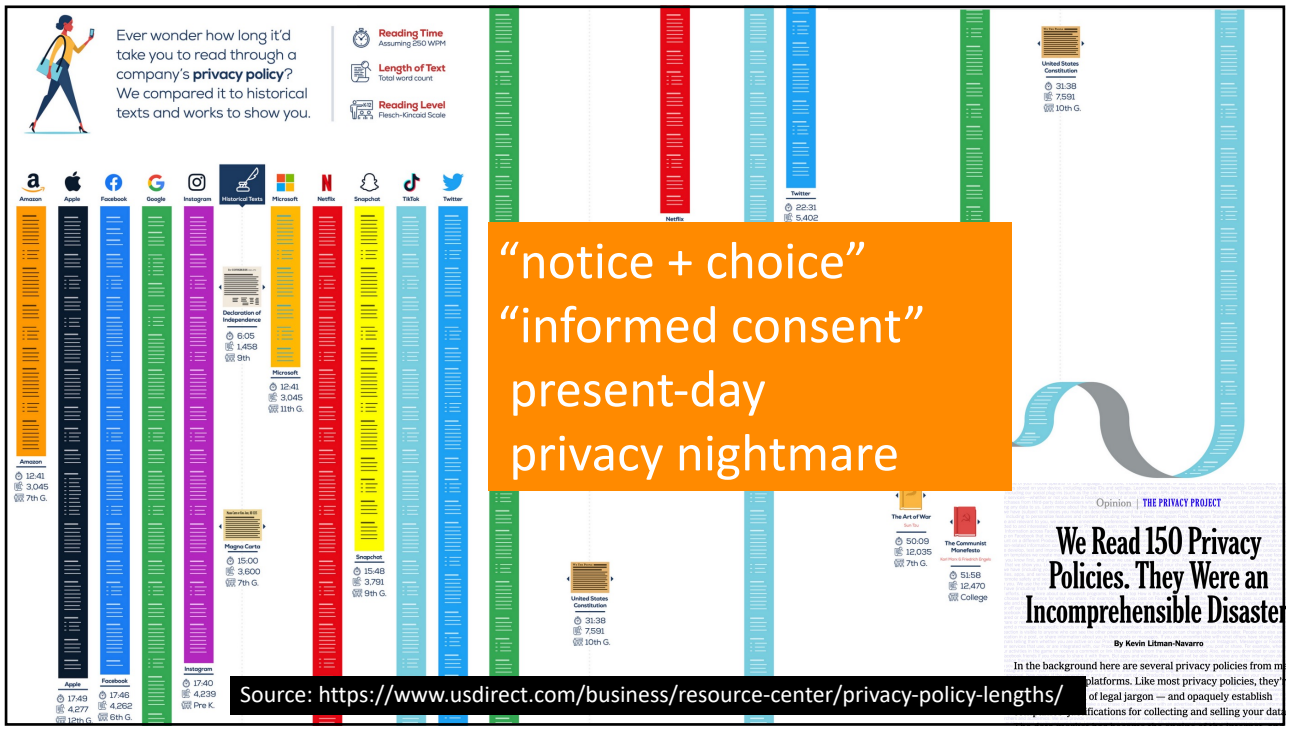
No secret databases
Know content/use
Purpose/use limit
Correction
Security/reliability

Control = **Notice & Choice**



The privacy policy…

44



45

Ongoing research to make consent work in practice

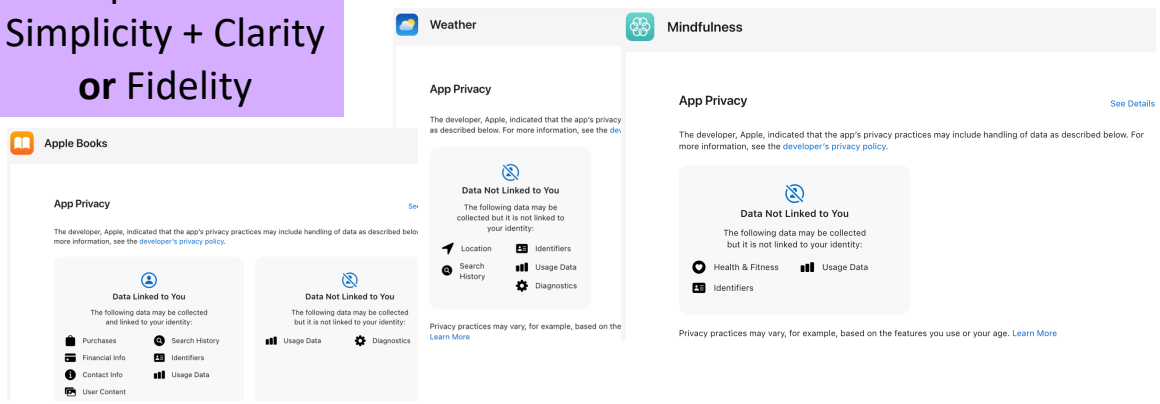
- Usable choice architectures; opt-in/opt-out; "just-in-time", tiered, etc.
- More comprehensible, supple privacy policies; plain language, "visceral notice," etc.
- Privacy nutrition labels

46

Transparency Dilemma

Comprehensible **or** Comprehensive
Simplicity + Clarity **or** Fidelity

Transparency is the best policy.
Our Privacy Nutrition Labels are designed to help you understand how apps handle your data, including apps we develop at Apple. This page brings privacy labels for our iOS, iPadOS, macOS, watchOS, and tvOS apps together in one place.



47

Consent regime punts decisions to data subjects

Least able to assess implications, let alone our own best interests

48

ENVIRONMENTAL CHANGE

SCIENTIFIC DISCOVERIES

TYRANNY OF CONVENTION

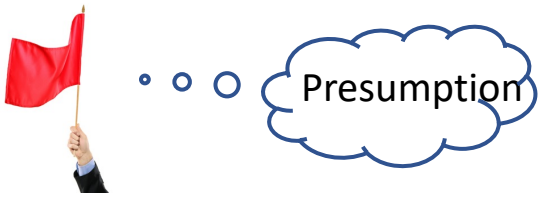
NO NORMS?

CULTURAL SHIFT

49

Heuristic

- Confront a disturbing case:
  - WebMD or NIH with Facebook button; 3rd party scripts "sell" user data
- Describe data flows in terms of 5 parameters
  - Note: in practice, parameters are often overlooked
- Relevant norm? [rule expressed in terms of 5 parameters]
  - Existence of norms can be discovered a variety of ways
- Notice a discrepancy?



50

what if

When tech practices are unprecedented

New practices don't meet expectations, or entrenched norm(al)

or

No relevant entrenched norm(al) guide or shape expectations

51

Stick-with-old or go-with-the-flow?

52

[achieving a meaningful concept of privacy]
clear and rigorous
faithful to common use
carries moral weight
& ideally defensible with technology & policy

53

"reveals privacy's moral significance"

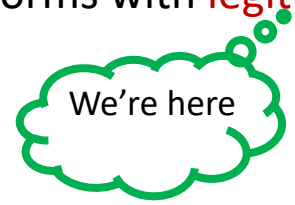
54

Contextual Integrity – KEY IDEAS

1) Appropriate flow of information/data

2) Flow conforms with contextual info norms

3) Flow conforms with legitimate contextual info norms



55

Data Governance = Regulation of data practices, entitlements, flow in accordance with societal values

CI evaluation of legitimacy

1. Interests & preferences of affected parties (stakeholders)
2. Ethical and political principles and values (societal)
3. Contextual functions, purposes, and values (societal)

56

Data Governance = Regulation of data practices, entitlements, flow in accordance with societal values

CI evaluation of legitimacy

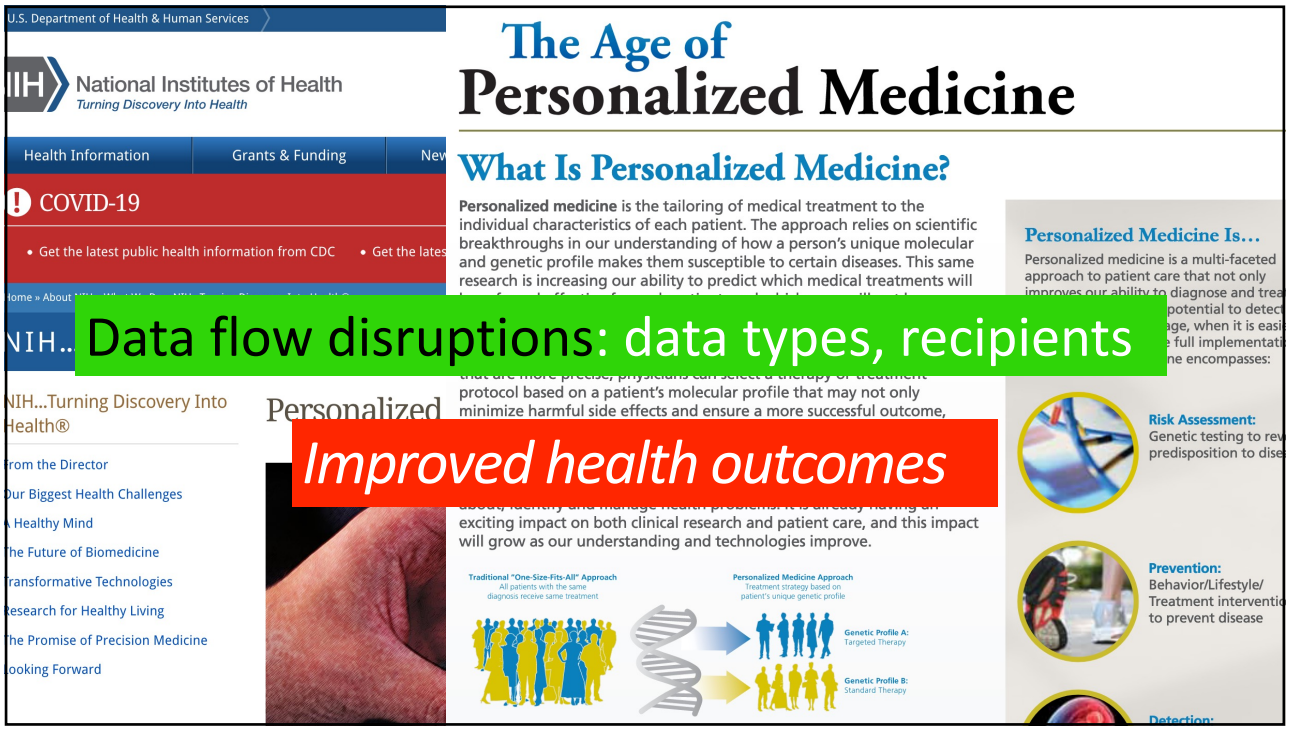
1. Interests & preferences of affected parties (stakeholders)
2. Ethical and political principles and values (societal)
3. Contextual functions, purposes, and values (societal)

57

Contextual functions, purposes and values

healthcare: cure disease, alleviate pain and suffering, equity …
E.g. how does confidentiality function in healthcare contexts
politics: democracy, autonomy, accountability, justice
home and social: trust, autonomy, stability
education: knowledge, intellect, creativity, fair distribution
commercial marketplace: sell, buy, compete, profit, trust, honesty
(and more)

58



59

Harvard Data Science Review • Special Issue 1 - COVID-19: Unprecedented Challenges and Chances

Individual Acceptance of Using Health Data for Private and Public Benefit: Changes During the COVID-19 Pandemic

Frederic Gerdon, Helen Nissenbaum, Ruben L. Bach, Frauke Kreuter, Stefan Zins

Published on: Apr 06, 2021

60

Contextual Integrity – NOT

Only only about harm to the **individual (Pris Regan)**
Contrary to **societal** values (typical: security)
Is not a tradeoff with **utility*** (research, personalization)

*Recall the case for differential privacy – tradeoff between "privacy and utility"

61

Why Privacy as CI?

- Offers a positive conception of privacy
- Good for societies and for individuals
- Supports societal and contextual goods: fairness, justice, autonomy, security, health, liberty, utility

62

PRIVACY → DATA GOVERNANCE

Governing (personal) data: What to do?
Articulate purposes and values of social contexts
Discover and uncover contextual norms: make the implicit explicit
Require data processors to reveal data flows with values for all the CI parameters
Work with domain experts to understand impacts of data flows on interests, values, and contextual ends (e.g. does surveillance help students learn?
Be ready to impose substantive constraints in service of stakeholder interests and social integrity

63

Bringing contextual integrity into privacy regulation

"It's too complicated for regulators!!"

64

Informational Norms Embedded in Law: 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

Exactly as **CI** says!

In our formal computer language,

$$\Box\forall p_1, p_2, q : P.\forall m : M.\forall t : T.$$
$$\text{incontext}(p_1, c) \wedge \text{send}(p_1, p_2, m) \wedge \text{contains}(m, q, t) \rightarrow$$
$$\text{inrole}(p_1, \textit{institution}) \wedge \text{inrole}(p_2, \textit{non-affiliate}) \wedge \text{inrole}(q, \textit{consumer}) \wedge (t \in \textit{npi}) \rightarrow$$
$$\Diamond\text{send}(p_1, q, \textit{privacy-notice}) \vee \Diamond\text{send}(p_1, q, \textit{privacy-notice})$$

With, Adam Barth, Anupam Datta, John Mitchell

65

Social policy for the sake of privacy, as CI

Identify contextual (sectoral) ends, purposes, and values
Ends, purposes and values as guidance for data governance

education: knowledge, intellect, creativity, fair distribution
FERPA Education Privacy 1974

healthcare: cure disease, alleviate pain and suffering, equity …
HIPAA Health Privacy Rules ~2000

finance: invest, bank, sell, buy, compete, profit, trust, honesty
FCRA Fair credit reporting Act 1970; GLBA Privacy rules ~2000

66

California Consumer Privacy Act (CCPA)

Home / Privacy / *California Consumer Privacy Act (CCPA)*

Updated on February 15, 2023

The California Consumer Privacy Act of 2018 (CCPA) gives consumers more control over the personal information that businesses collect about them and the CCPA regulations provide guidance on how to implement the law. This landmark law secures new privacy rights for California consumers, including:

- The right to know about the personal information a business collects about them and how it is used and shared;
- The right to delete personal information collected from them (with some exceptions);
- The right to opt-out of the sale or sharing of their personal information; and
- The right to non-discrimination for exercising their CCPA rights.

GENERAL DATA PROTECTION REGULATION – EU GDPR

Still heavy on individual control, as consent, with FIPPS their bone structure

Omnibus vs. Sectoral? Both!

67

Health tracking tech Mobile & Web

"The Great Regulatory Dodge," with Kathy Strandburg and Salome Viljoen – A contextual approach to revising policy (Forthcoming)

Fertility + Period

Mental health

68

Art. 5 GDPR Principles relating to processing of personal data

1.Personal data shall be:

1. processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');
2. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation');
3. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');
4. accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');
5. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation');
6. processed in a manner that ensures appropriate security of the personal data, …

69

Art. 6 GDPR Lawfulness of processing

1.[1]Processing shall be lawful only if and to the extent that at least one of the following applies:

1. the data subject has given consent to the processing of his or her personal data for one or more specific purposes;
2. processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
3. processing is necessary for compliance with a legal obligation to which the controller is subject;
4. processing is necessary in order to protect the vital interests of the data subject or of another natural person;
5. processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
6. processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

…

70

Art. 6 GDPR Lawfulness of processing, contin.

1.[2]The purpose of the processing shall be determined in that legal basis or, as regards the processing referred to in point (e) of paragraph 1, shall be necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. ···. [4]The Union or the Member State law shall meet an objective of public interest and be proportionate to the legitimate aim pursued.

2.Where the processing for a purpose other than that for which the personal data have been collected is not based on the data subject's consent or on a Union or Member State law which constitutes a necessary and proportionate measure in a democratic society to safeguard the objectives referred to in Article 23(1), the controller shall, in order to ascertain whether processing for another purpose is compatible with the purpose for which the personal data are initially collected, take into account, inter alia:

1. any link between the purposes for which the personal data have been collected and the purposes of the intended further processing;
2. the context in which the personal data have been collected, in particular regarding the relationship between data subjects and the controller;
3. the nature of the personal data, in particular whether special categories of personal data are processed, pursuant to Article 9, or whether personal data related to criminal convictions and offences are processed, pursuant to Article 10;
4. the possible consequences of the intended further processing for data subjects;

71

Collaborators （合作人：以下为一些美国的著名教授的名字）

Solon Barocas, Adam Barth, Sebastian Benthall, Madiha Choksi, Amanda Conley, Anupam Datta, Serge Egelman, Deborah Estrin, Jake Goldenfein, Seda Guerses, Daniel Howe, Paula Kift, Kirsten Martin, Lee McGuigan, John Mitchell, Heather Patterson, Madelyn Sanfilippo, Divya Sharma, Ido Sivan-Sevilla, Yan Shvartzshnaider, Katherine Strandburg, Vitaly Shmatikov, Lakshmi Subramanian, Vincent Toubiana, Michael Tschantz, Thomas Wies, Salome Viljoen, Elana Zeide

https://nissenbaum.tech.cornell.edu/

With research support from: NSA H98230-18-D-006, NSF: CNS-1801501, *CNS-1704527, SES-1537324, SES-1650589; MacArthur Foundation*

72