Privacy as Contextual Integrity

Helen Nissenbaum

November 5 • 2025

Devices & Apps

GreenGoose — Toothbrush Sensor. A pliable ring that slides onto a toothbrush. Once connected to a GreenGoose base station (little green egg), it measures when your kids start brushing and communicates to apps on your mobile phone. See cartoon video at **www.greengoose.co...**

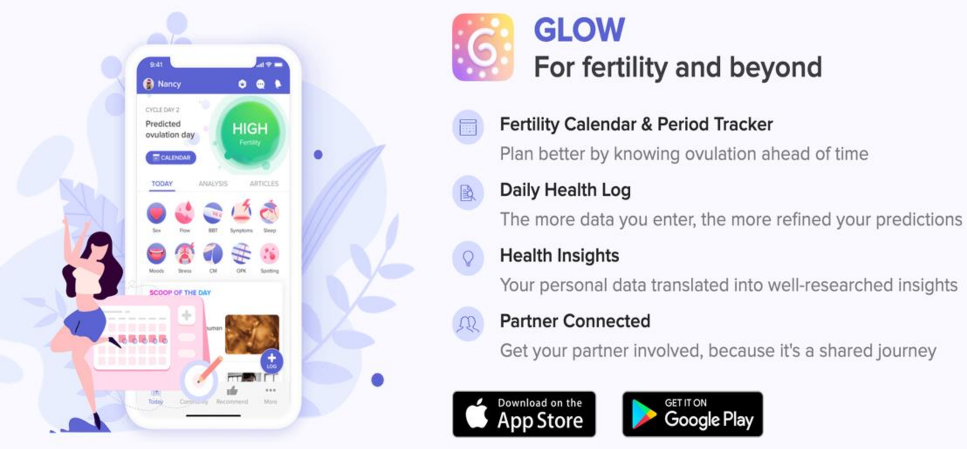
Sun exposure

Baby

iBGStar blood **#glucose** meter for **#diabetes** management. Can be used on its own or connected directly to an iPhone or iPod touch to display, manage and communicate information. The FDA cleared device is manufactured by AgaMatrix and available through Sanofi.

The Gluco(M) Wristband. [concept from 2009] "Medical device that offers 3 major functions to diabetics: non-invasive and instant glucose reading, storing previous readings history with averages, and an extremely useful insulin chamber with loaded syringe cartridge." **#diabetes**

VeBand. Wristband that monitors
xposure to the sun's UVA and UVB
ys (it doesn't just detect sunlight)
brat
insc
argi



GLOW

For fertility and beyond

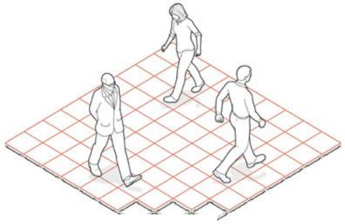
Fertility Calendar & Period Tracker
Plan better by knowing ovulation ahead of time

Daily Health Log
The more data you enter, the more refined your predictions

Health Insights
Your personal data translated into well-researched insights

Partner Connected
Get your partner involved, because it's a shared journey

ngestible event markers (IEMs) from roteus. The digestible sensors, made om food ingredients, are activated by tomach fluids after swallowing, reating a digital signal detected by a nicroelectronic recorder configured as ither a small bandage style skin-patch r a tiny device inserted under the kin. The detector decodes and ecords information such as type of rug and dose, and measures hysiologic parameters such as heart ate, activity, and respiratory rate.

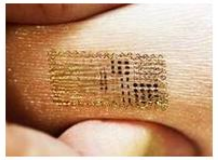


Fitness

Fertility+Period

Mental health

Withings blood pressure monitor
www.withings.com



Sensor tattoos (Epidermal Electronics) Electrophysiological, temperature, and strain sensors; transistors, light-emitting diodes, photodetectors, radio frequency inductors, capacitors, oscillators, and rectifying diodes. From the journal Science, work done by John Rodgers. See also **mc10inc.com/**

PillCam - ESO (esophagus) and SB (Small bowel). The video capsule contains an imaging device and light source and transmits images at a rate of 2 (SB) to 18 (ESO) images per second. The capsule endoscopy is used to visualize and detect disorders of the GI tract. **#crohns**
www.givenimaging.com

ChatGPT

Digital Technologies Threaten Privacy!

GPS, mobile, implantable devices, RFID, CCTV, Sensors, networked sensors, image, video and audio, Web cookies, flash cookies, web b tracking

Collect, Track, Surveil, Monitor,

My privacy has been violated!

“Big 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

Privacy

What do we mean?
Why do we care?

Privacy

What do we mean?
Why do we care?

Right to control [private]

No access [to private]

Right to withhold [private]

Dignity

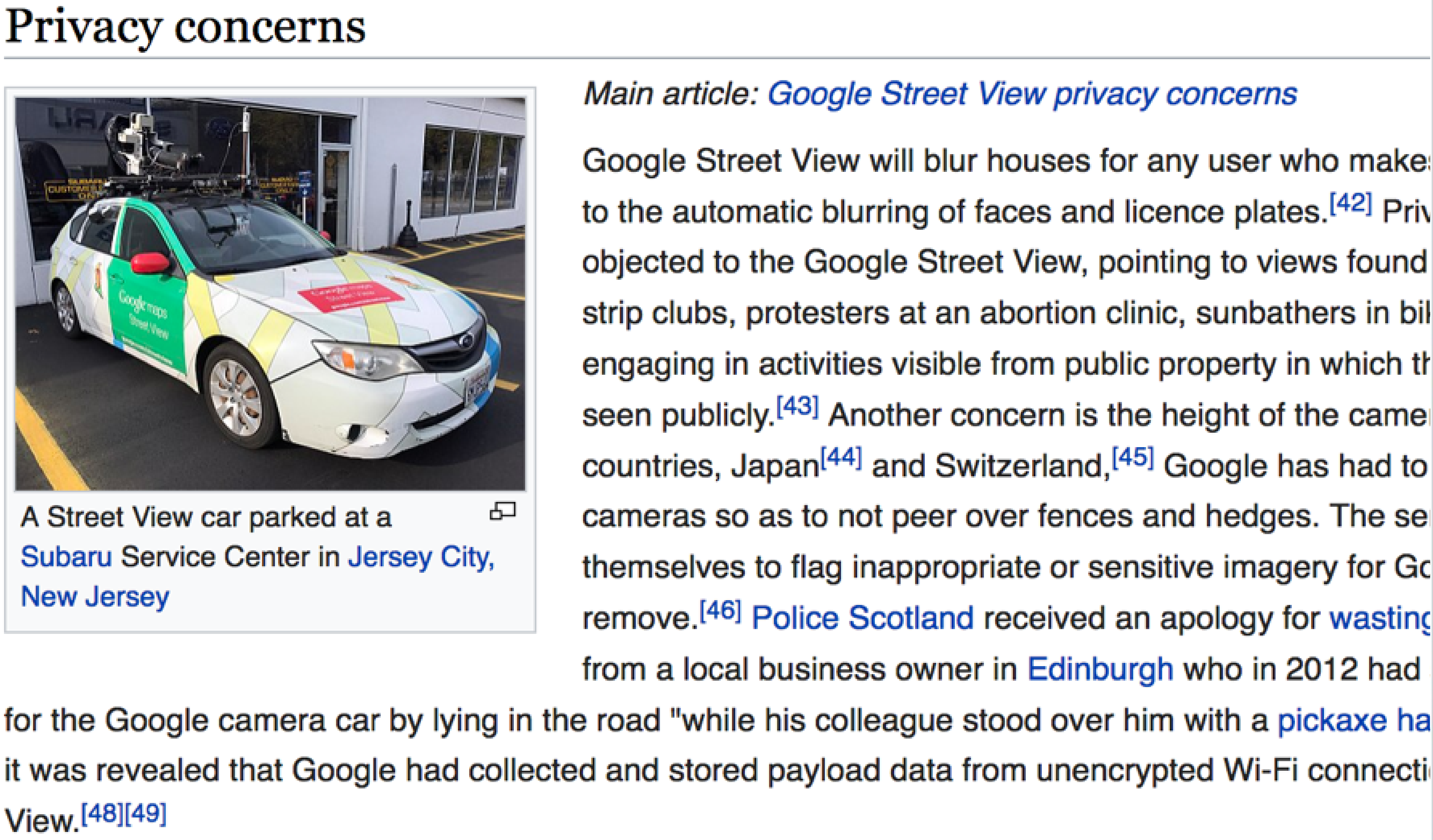
Autonomy

Harm

Why do we need ANOTHER definition of privacy?

1. Threats from digital tech that cannot be handled
2. A regulatory approach – “notice & choice” -- that is broken
3. Allowing “anything goes” for data that is unsecured (think scraping; think taking stuff from an unlocked house)
4. Suggesting the “privacy paradox” is real

Google Maps Street View, launched 2007



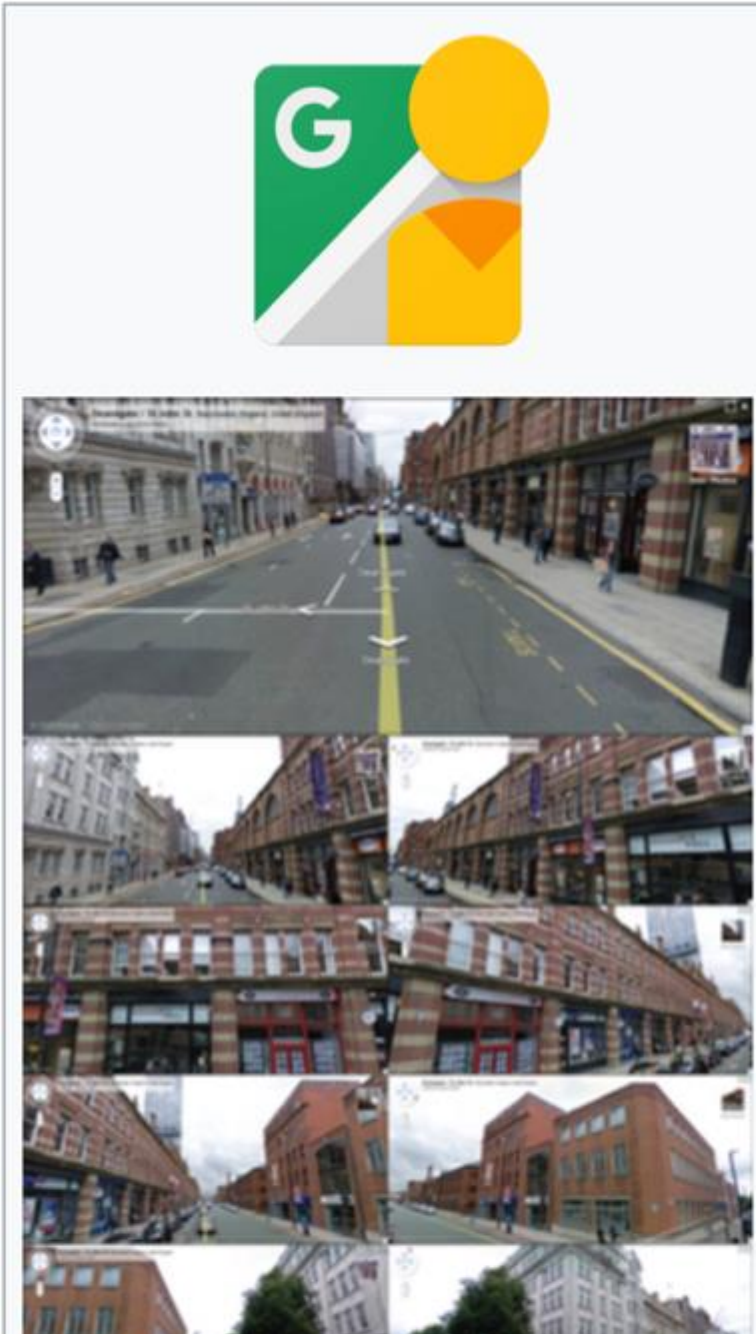
Privacy concerns

A Street View car parked at a Subaru Service Center in Jersey City, New Jersey

Main article: Google Street View privacy concerns

Google Street View will blur houses for any user who make
to the automatic blurring of faces and licence plates.[42] Priv
objected to the Google Street View, pointing to views found
strip clubs, protesters at an abortion clinic, sunbathers in bi
engaging in activities visible from public property in which t
seen publicly.[43] Another concern is the height of the came
countries, Japan[44] and Switzerland,[45] Google has had to
cameras so as to not peer over fences and hedges. The se
themselves to flag inappropriate or sensitive imagery for G
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 Street View



Clearview AI

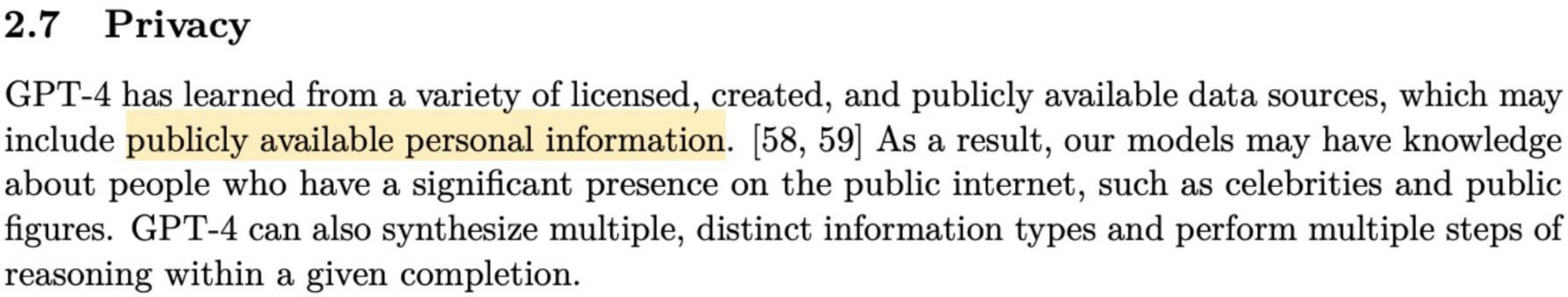
Scraped over **30 billion** photos from social media & other public websites.

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**

Only "public!"

Large Language Models

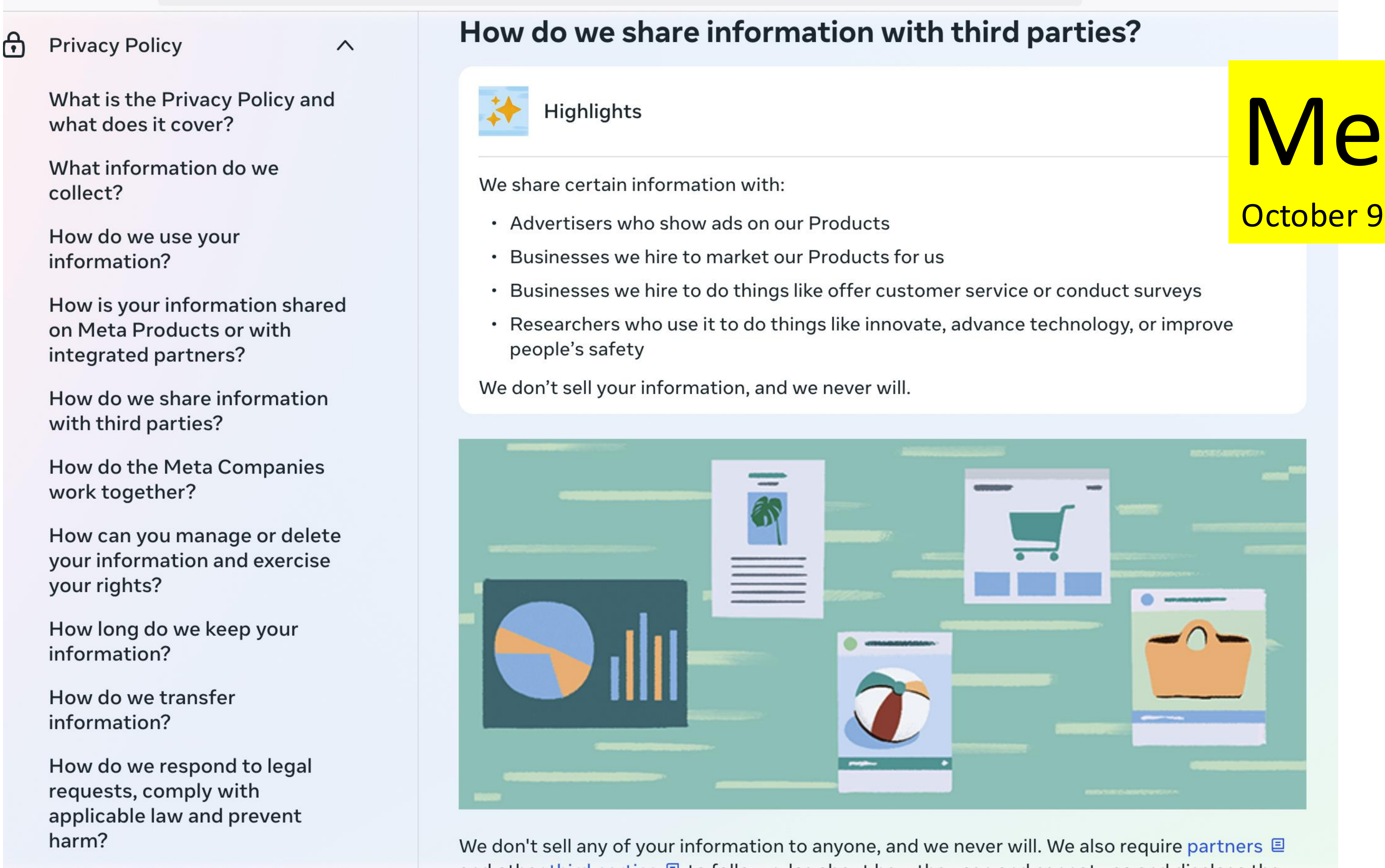


2.7 Privacy

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.

Meta

October 9, 2024



How do we share information with third parties?

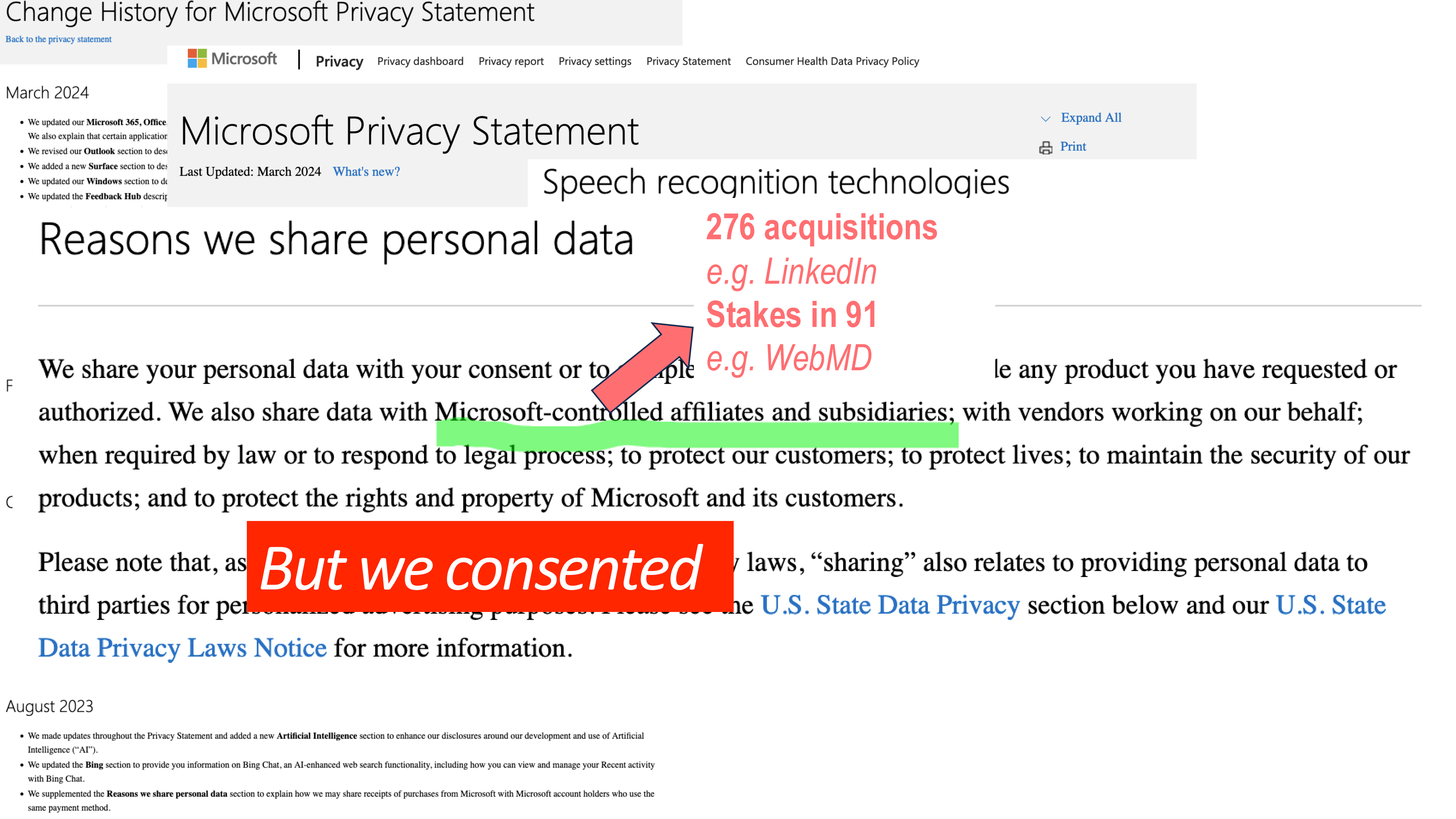
Highlights

We share certain information with:

- Advertisers who show ads on our Products
- Businesses we hire to market our Products for us
- Businesses we hire to do things like offer customer service or conduct surveys
- Researchers who use it to do things like innovate, advance technology, or improve people's safety

We don't sell your information, and we never will.

We don't sell any of your information to anyone, and we never will. We also require partners



Change History for Microsoft Privacy Statement

Back to the privacy statement

March 2024

- We updated our **Microsoft 365, Office** We also explain that certain application
- We revised our **Outlook** section to desc
- We added a new **Surface** section to des
- We updated our **Windows** section to de
- We updated the **Feedback Hub** descrip

Microsoft Privacy Statement

Last Updated: March 2024 What's new?

Speech recognition technologies

Reasons we share personal data

We share your personal data with your consent or to complete le any product you have requested or authorized. We also share data with Microsoft-controlled affiliates and subsidiaries; with vendors working on our behalf; when required by law or to respond to legal process; to protect our customers; to protect lives; to maintain the security of our products; and to protect the rights and property of Microsoft and its customers.

Please note that, as y laws, "sharing" also relates to providing personal data to third parties for pe the U.S. State Data Privacy section below and our U.S. State Data Privacy Laws Notice for more information.

276 acquisitions

e.g. LinkedIn

Stakes in 91

e.g. WebMD

But we consented

August 2023

- We made updates throughout the Privacy Statement and added a new **Artificial Intelligence** section to enhance our disclosures around our development and use of Artificial Intelligence ("AI").
- We updated the **Bing** section to provide you information on Bing Chat, an AI-enhanced web search functionality, including how you can view and manage your Recent activity with Bing Chat.
- We supplemented the **Reasons we share personal data** section to explain how we may share receipts of purchases from Microsoft with Microsoft account holders who use the same payment method.

Benchmarks for a meaningful conception of privacy

Faithful to common use

Clear and rigorous

Reveals privacy's ethical significance (why care?)

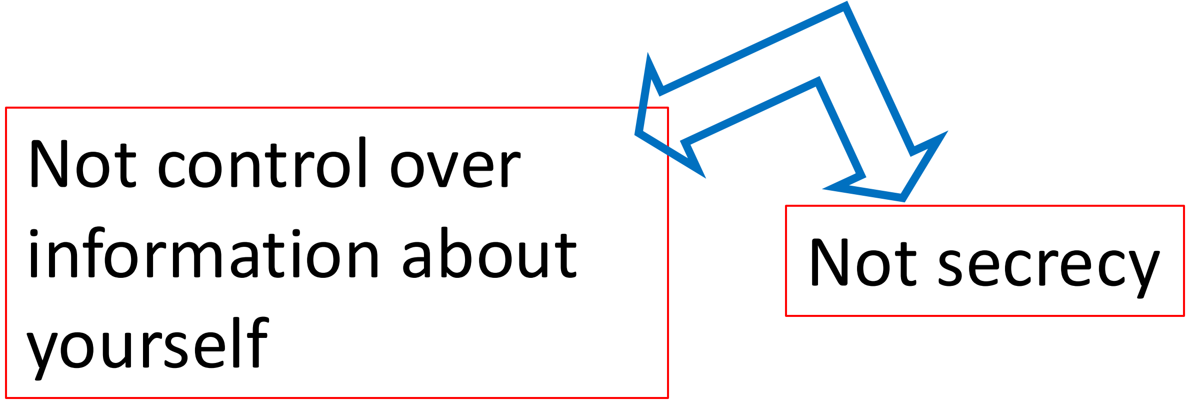
&

Solid grounding for technology and regulation

Contextual Integrity (CI): The one-liner

privacy is

Appropriate information flow

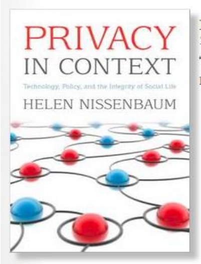


Not control over information about yourself

Not secrecy

Key ideas

Privacy as Contextual Integrity



PRIVACY
IN CONTEXT
Technology, Policy, and the Integrity of Social Life
HELEN NISSENBAUM

… a different way of thinking about privacy

Contextual Integrity (CI): The one-liner

privacy is

appropriate information flow

Why flow?

Contextual Integrity (CI) Definition

appropriate information flow

= conforms with legitimate contextual norms/rules

- Social Contexts
- Contextual informational norms
- Contextual values ends purpose

2-300B
1-302
BOARD OF ELECTIONS IN THE CITY OF NEW YORK
VOTE

Contexts

- Differentiated social spheres
  - E.g. health, education, family, politics, commerce
- Defined by purposes, goals, values
- Associated functions; practices; ontologies of roles and information types
- Governed by contextual norms & rules
  - Specifically, data flow norms, rules

Structure of CI Norms

The CI-tuple: Five parameters

<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**

Capacities, ontologies, Transmission Principles

Ontologies of roles: student, physician, policeman.

Ontologies of attributes: consider forms such as IRS, Census, bank loan, medical insurance, admissions applications, job applications

Transmission principles: With consent (“control”), With notice, With payment, With authorization of <xyz>, By law

<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 compelled to show contents of their luggage to the TSA agents upon request.

All the parameters matter!

A rule must specify values for all parameters!

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

What difference does this make?

Privacy as Contextual Integrity Defined **(First approximation)**

CI Is satisfied iff information flows conform with entrenched informational norms. (We may say, “meets privacy expectations.”)

Benchmarks for a meaningful conception of privacy

Faithful to common use

Clear and rigorous

Reveals privacy's ethical significance (why care?)

&

Solid grounding for technology and regulation

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

*K. Martin and H. Nissenbaum (2017) "Measuring Privacy: An Empirical Test Using Context to Expose Confounding Variables," *Columbia Science and Technology Law Review* 18, 176-218.
K. Martin and H. Nissenbaum (2017) "Privacy Interests in Public Records: An Empirical Investigation," *Harvard Journal of Law and Technology* 31:1, 111-143.
K. Martin and H. Nissenbaum (2020) "What is it about Location?" Berkeley Technology Law Journal

Discovering Norms: Factorial Vignette Questions template

- Is it acceptable for the **<sender>** to share the **<subject>’**s **<attribute>** with **<recipient> <transmission principle>**?
- E.G. Is it acceptable for a professor to share a student’s poor record of attendance with the department chair without student’s consent?

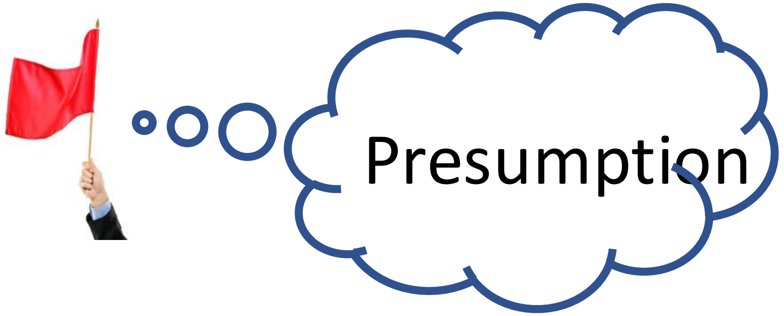
Contextual Integrity (CI) Definition

appropriate information flow

= conforms with legitimate contextual norms/rules

CI Heuristic to evaluate tech or to inform tech design

- Describe data flows in terms of all 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
- Check conformance
  - Yes +
  - No X
  - Other ?



Benchmarks for a meaningful conception of privacy

Faithful to common use

Clear and rigorous

Reveals privacy's ethical significance (why care?)

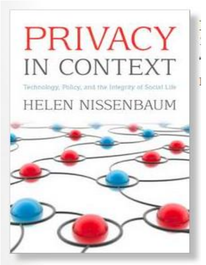
&

Solid grounding for technology and regulation

Seeking ethical legitimacy

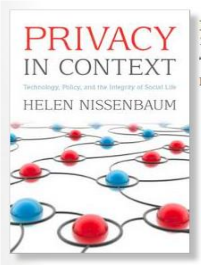
When tech practices challenge norms, norms are unclear, contested, or don’t exist

Appropriateness? Alignment?



Consider the consequences

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



Consider the consequences

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

CI Parameters + Purposes and Values

Actors: Subject, Sender, Recipient

Acting in contextual capacities

Attribute: Types of information

Per contextual ontologies

Transmission Principle: Constraints on flow

Contextual ends, purposes, values: Ethical Justification

Contextual functions, purposes and values

healthcare: cure disease, alleviate pain and suffering, equity …

politics: democracy, autonomy, accountability, justice

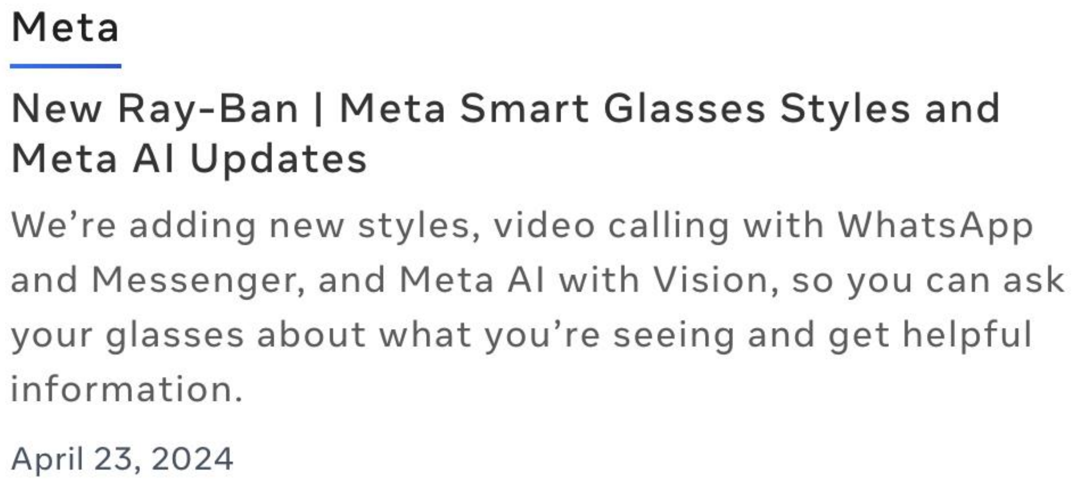
home and social: trust, autonomy, stability

education: knowledge, intellect, creativity, fair distribution

commercial marketplace: sell, buy, compete, profit, trust, honesty

(and more)

RAY-BAN META SMART GLASSES

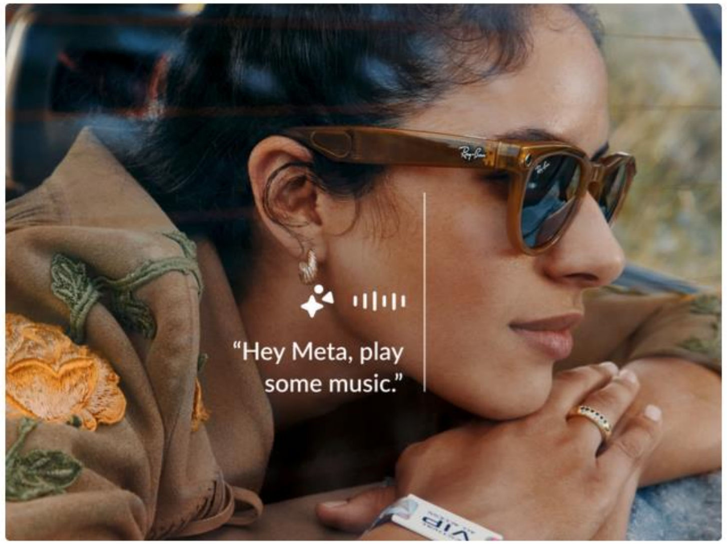


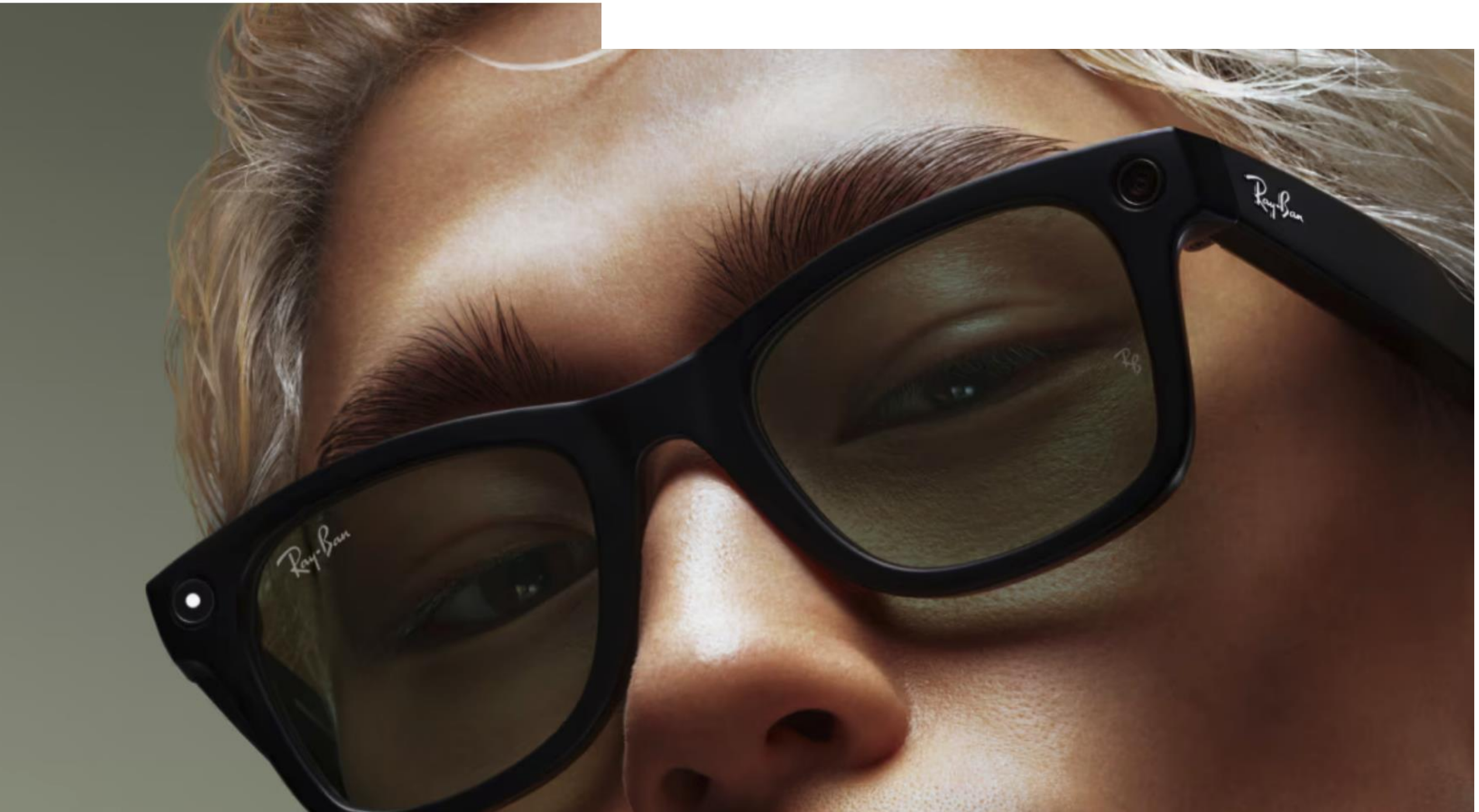
Meta

New Ray-Ban | Meta Smart Glasses Styles and Meta AI Updates

We're adding new styles, video calling with WhatsApp and Messenger, and Meta AI with Vision, so you can ask your glasses about what you're seeing and get helpful information.

April 23, 2024





?

TAKEAWAYS

- CI offers **positive** conception of privacy
- Societies *and* individuals benefit
- Serves societal and contextual ends and values:
  fairness, justice, autonomy, security, health, liberty, utility
- **Appropriate flow IS NOT a privacy tradeoff**

Benchmarks for a meaningful conception of privacy

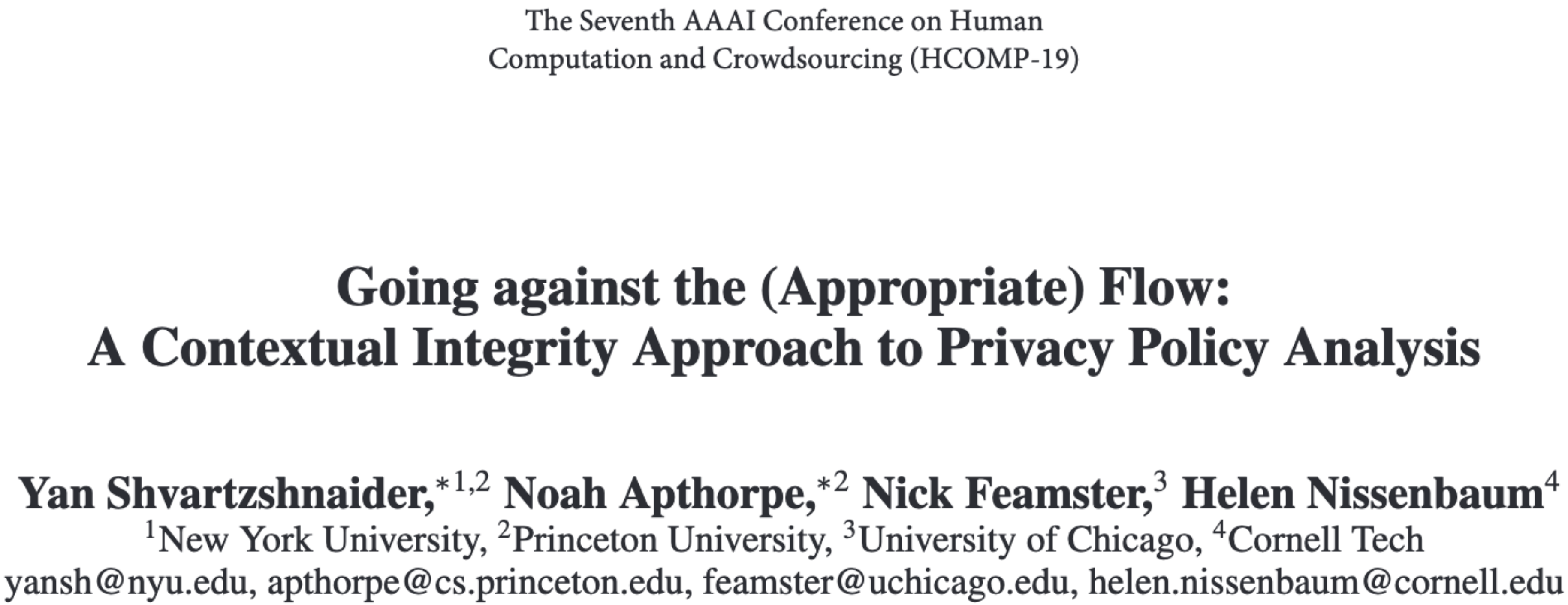
Faithful to common use

Clear and rigorous

Reveals privacy's ethical significance (why care?)

&

Solid grounding for technology and regulation

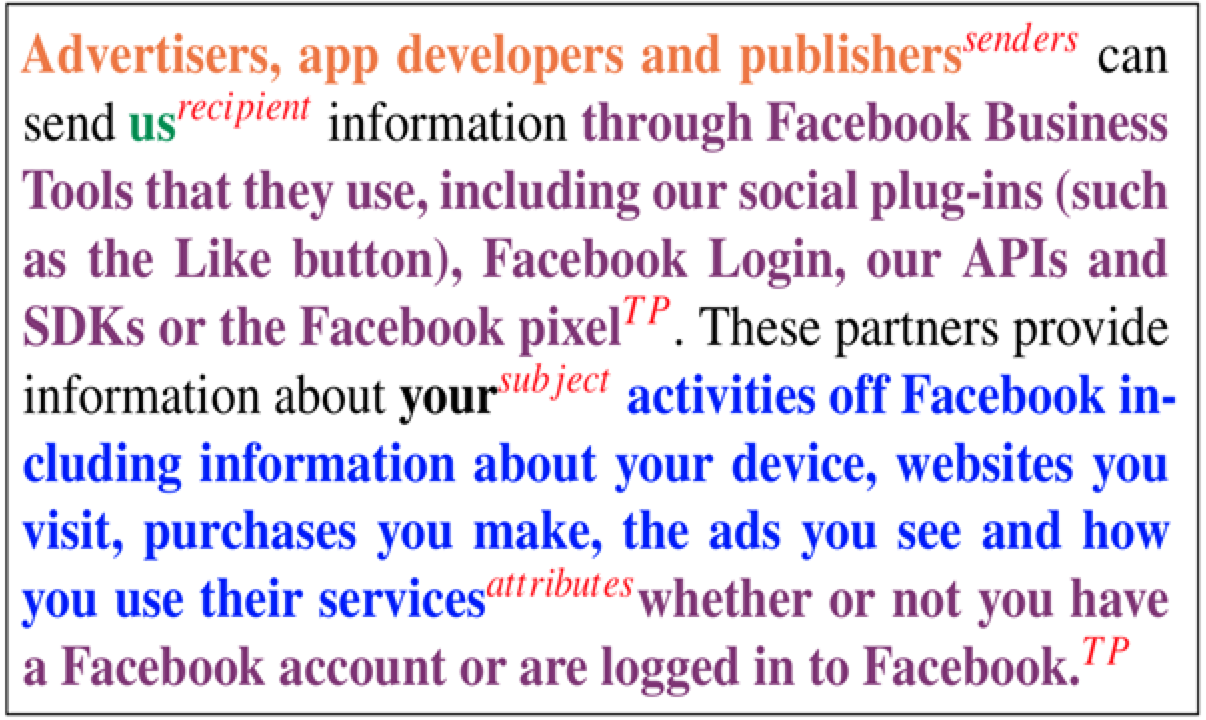


The Seventh AAAI Conference on Human
Computation and Crowdsourcing (HCOMP-19)

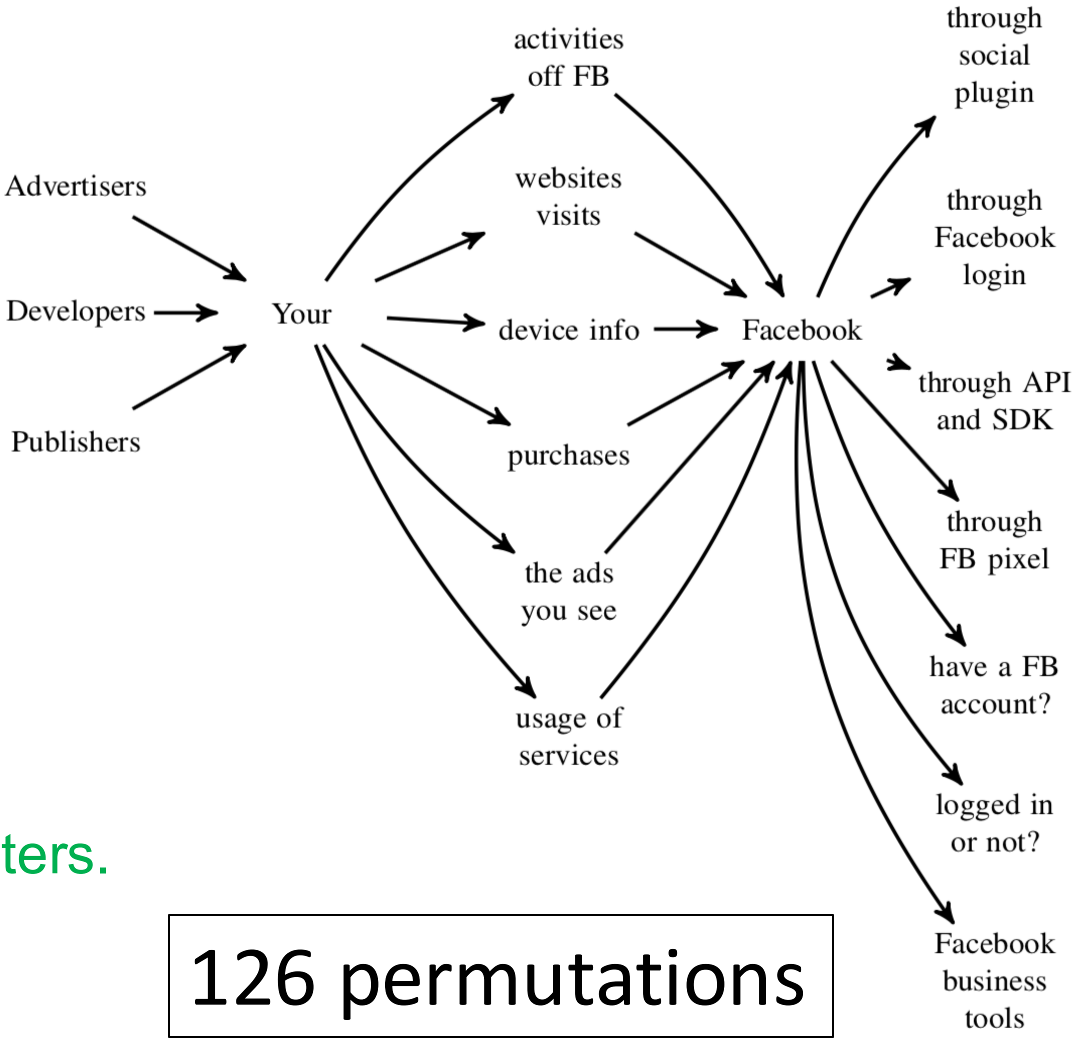
Going against the (Appropriate) Flow: A Contextual Integrity Approach to Privacy Policy Analysis

Yan Shvartzshnaider,[*1,2] **Noah Apthorpe,**[*2] **Nick Feamster,**[3] **Helen Nissenbaum**[4]
[1]New York University, [2]Princeton University, [3]University of Chicago, [4]Cornell Tech
yansh@nyu.edu, apthorpe@cs.princeton.edu, feamster@uchicago.edu, helen.nissenbaum@cornell.edu

Analysis: CI Parameter Bloating



Advertisers, app developers and publishers^{senders} can send us^{recipient} information through Facebook Business Tools that they use, including our social plug-ins (such as the Like button), Facebook Login, our APIs and SDKs or the Facebook pixel^{TP}. These partners provide information about your^{subject} activities off Facebook including information about your device, websites you visit, purchases you make, the ads you see and how you use their services^{attributes} whether or not you have a Facebook account or are logged in to Facebook.^{TP}



New work automates tagging operation for parameters.

126 permutations

Reject!

Privacy puts the brakes on good things

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

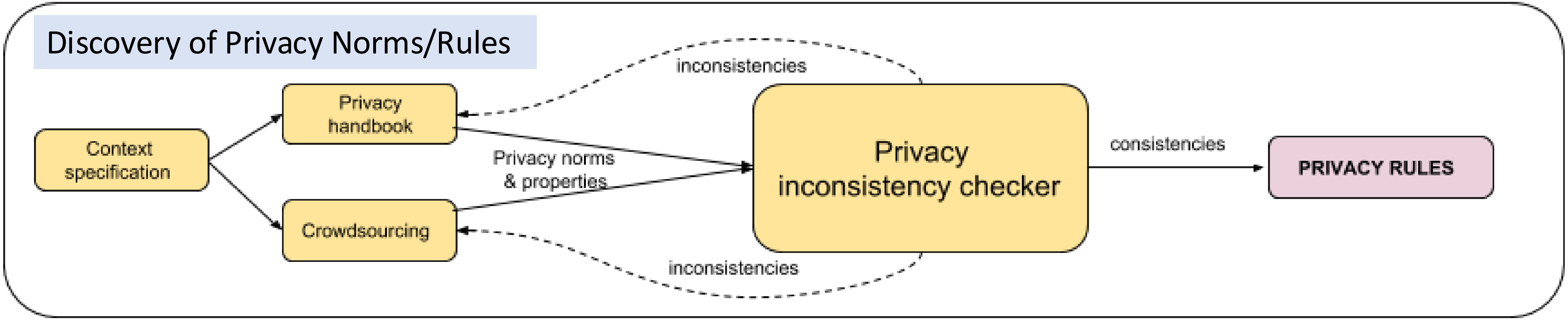
>Yes ✓

>No ✗

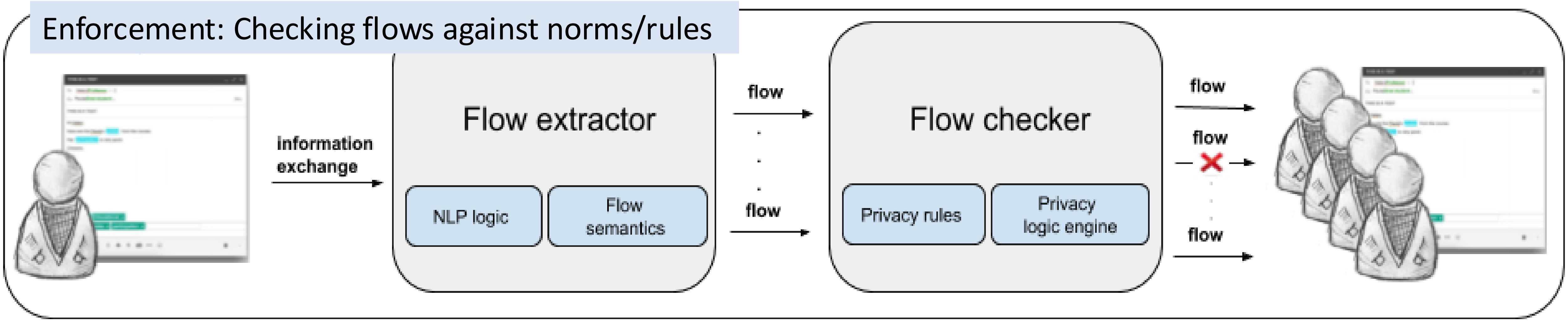
>other ?

VACCINE Data Governance for Institutional settings

detecting and expressing

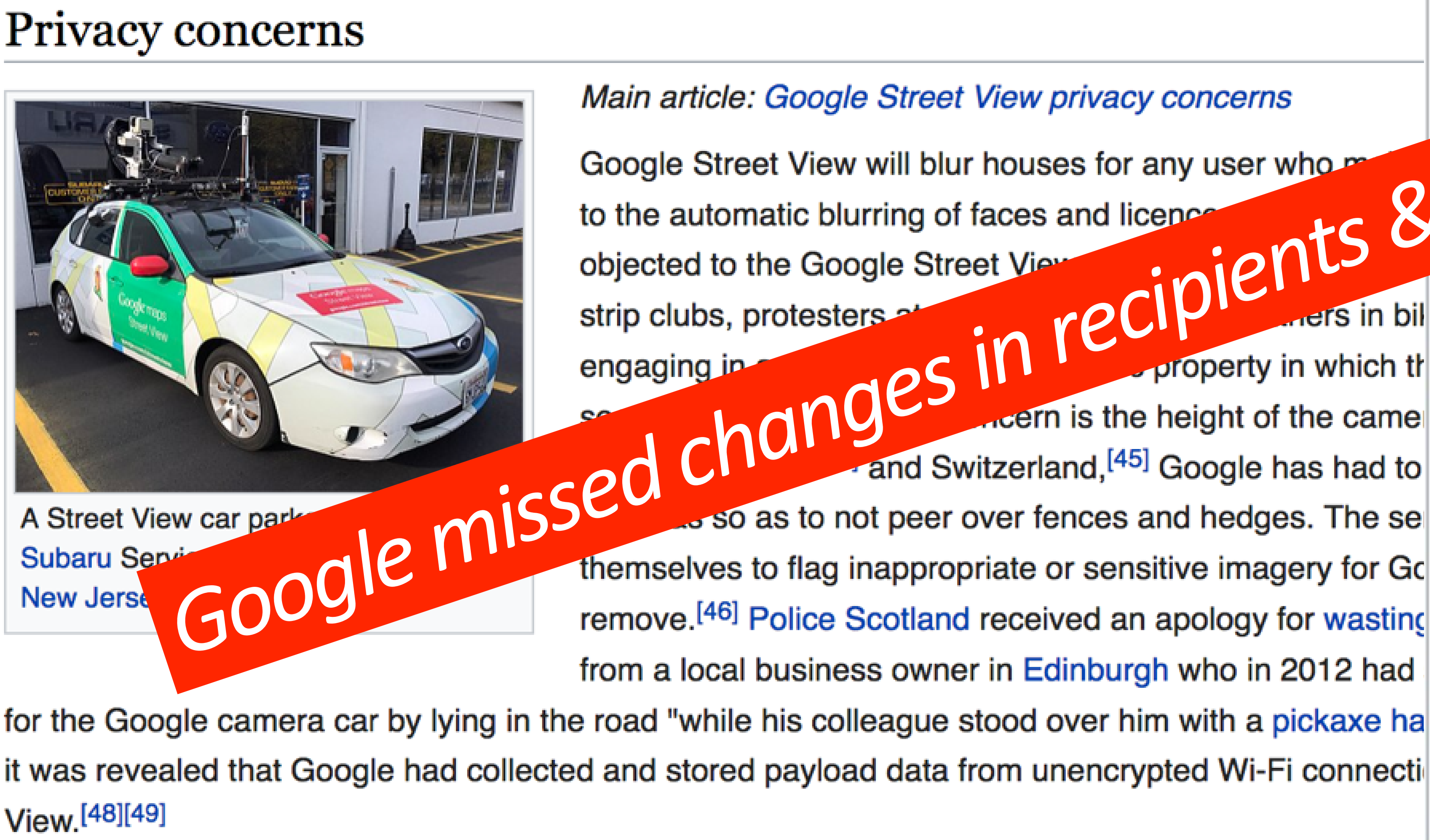


Discovery of Privacy Norms/Rules



Enforcement: Checking flows against norms/rules

Google Maps Street View, launched 2007



Privacy concerns

A Street View car park
Subaru Servi
New Jerse

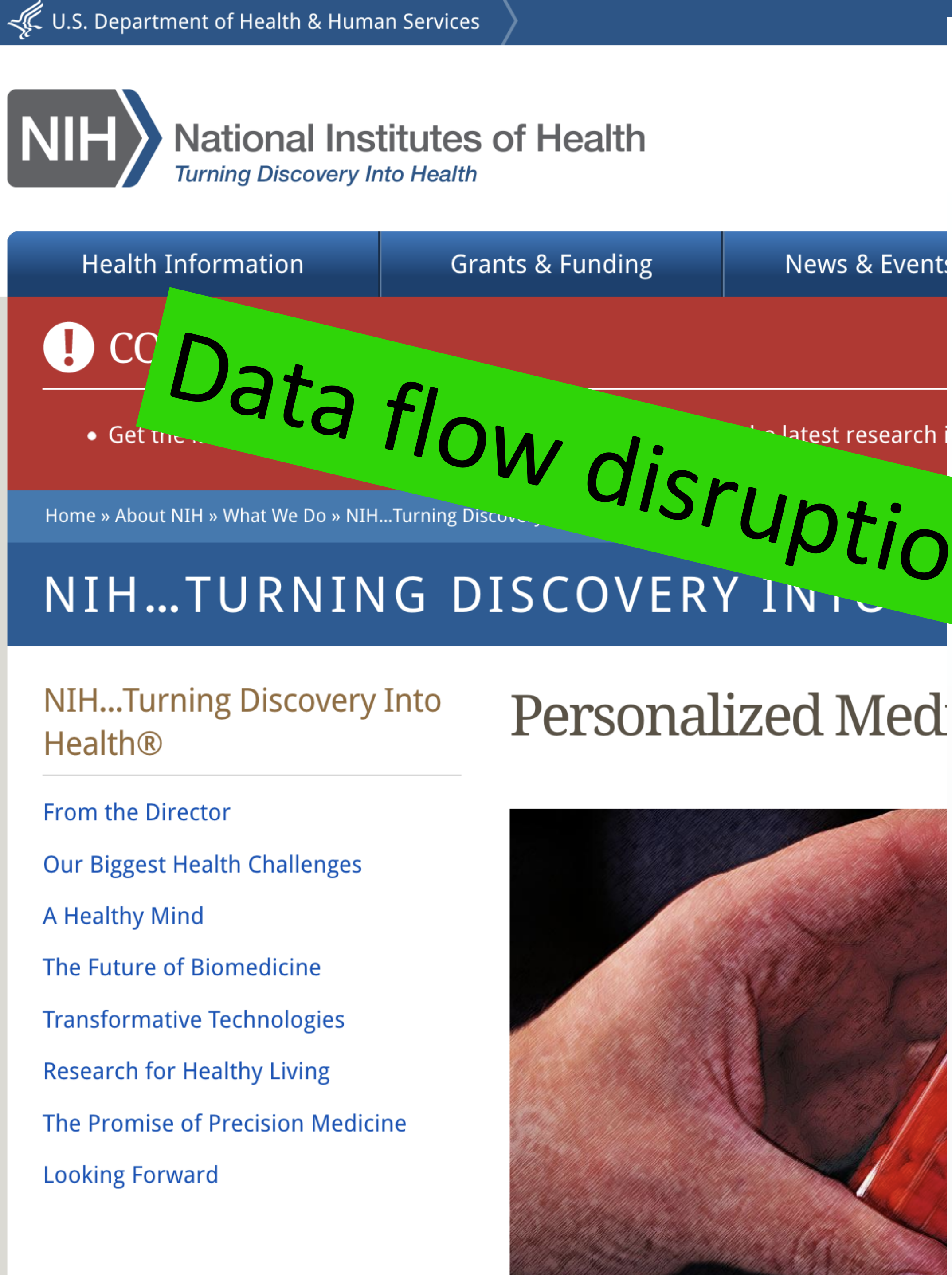
Main article: Google Street View privacy concerns

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
engaging in a
property in which th
s
ncern is the height of the came
and Switzerland,[45] Google has had to
s 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 wasting
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

Data flow disruptions: data types, recipients



U.S. Department of Health & Human Services

NIH National Institutes of Health
Turning Discovery Into Health

Health Information | Grants & Funding | News & Events

CO

- Get the latest research i

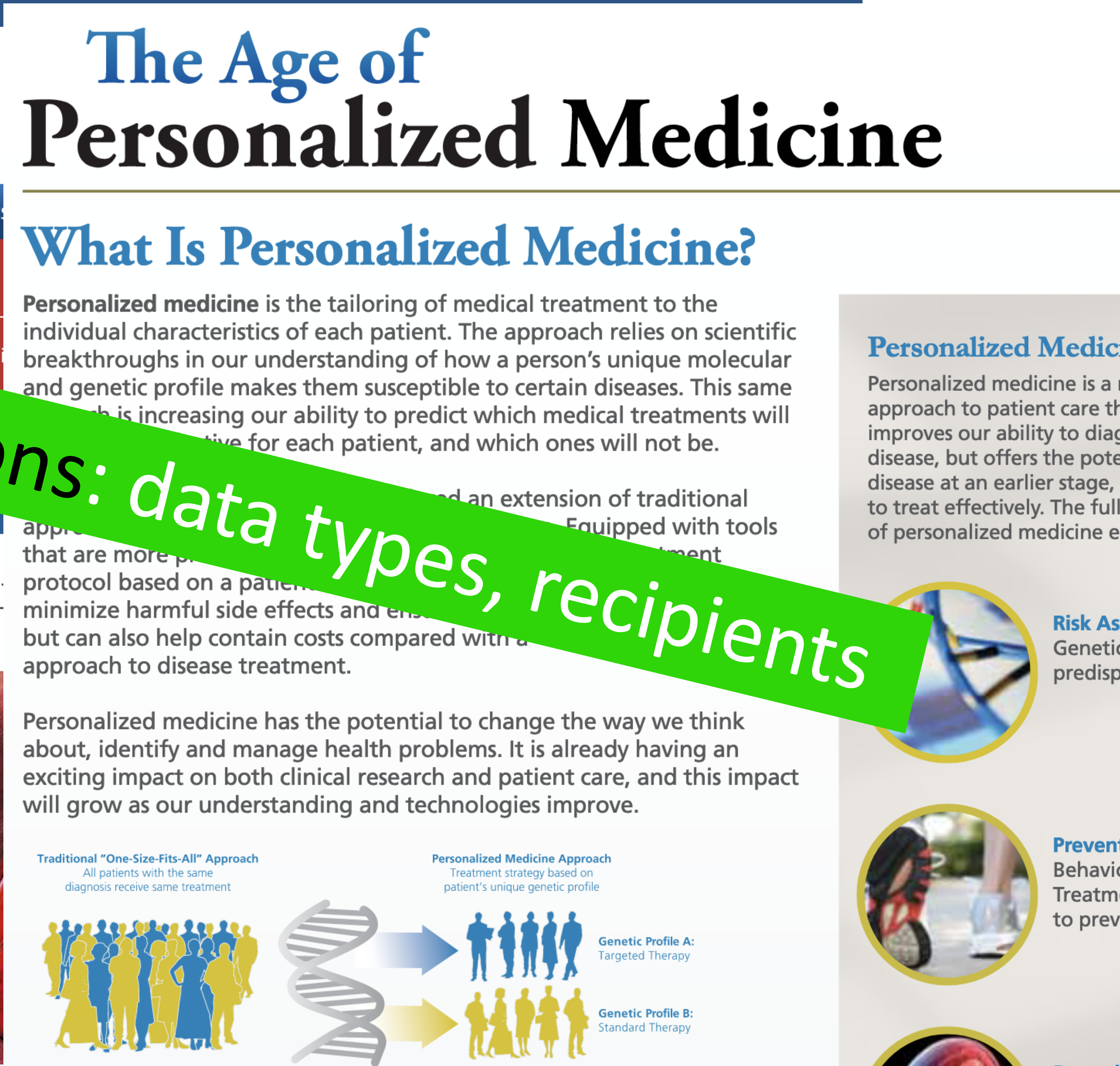
Home » About NIH » What We Do » NIH...Turning Discove

NIH...TURNING DISCOVERY INTO

NIH...Turning Discovery Into Health®

- From the Director
- Our Biggest Health Challenges
- A Healthy Mind
- The Future of Biomedicine
- Transformative Technologies
- Research for Healthy Living
- The Promise of Precision Medicine
- Looking Forward

Personalized Med



The Age of Personalized Medicine

What Is Personalized Medicine?

Personalized medicine is the tailoring of medical treatment to the individual characteristics of each patient. The approach relies on scientific breakthroughs in our understanding of how a person's unique molecular and genetic profile makes them susceptible to certain diseases. This same h is increasing our ability to predict which medical treatments will tive for each patient, and which ones will not be.

d an extension of traditional appr Equipped with tools that are more p ment protocol based on a patie minimize harmful side effects and en but can also help contain costs compared with a approach to disease treatment.

Personalized medicine has the potential to change the way we think about, identify and manage health problems. It is already having an exciting impact on both clinical research and patient care, and this impact will grow as our understanding and technologies improve.

Traditional "One-Size-Fits-All" Approach
All patients with the same diagnosis receive same treatment
Personalized Medicine Approach
Treatment strategy based on patient's unique genetic profile
Genetic Profile A: Targeted Therapy
Genetic Profile B: Standard Therapy

Personalized Medic

Personalized medicine is a
approach to patient care th
improves our ability to diag
disease, but offers the pote
disease at an earlier stage,
to treat effectively. The full
of personalized medicine e

Risk As
Geneti
predisp

Prevent
Behavi
Treatm
to prev

Contextual Integrity – NOT

No flow, no collection, secrecy [access]

……..of sensitive information

Control over personal information [control]

…….that is sensitive

Balance and trade off

Contextual Integrity – NOT

No flow, no collection, secrecy

…….of sensitive information

Control over personal information

…….that is sensitive

Balance and trade off

Privacy at What Cost? Using Electronic Medical Records to Recover Lapsed Patients Into HIV Care

Laura Derksen, Anita McGahan and Leandro Pongeluppe*

May 3, 2022

Abstract

We show that Malawian healthcare staff save lives by tracking down HIV patients lapsed from care – even against their wishes – using data made accessible with the implementation of an electronic medical records (EMR) system. HIV patients in Malawi receive antiretroviral therapy (ART), a highly effective treatment that also prevents transmission, for free at clinics. Yet patients frequently lapse from care, resulting in increased community transmission and unnecessary deaths. The introduction of EMR allowed health providers to manage patient data, trace lapsed patients, and encourage lapsed patients to reinitiate treatment. We implement an event study analysis using data from 106 clinics that adopted EMR between 2007 and 2019 and find that the introduction of EMR leads to an immediate increase in the number of patients actively in care and to a decline in patient deaths. After five years of implementation, facilities with EMR have approximately 34 percent more patients in care and 28 percent fewer patient deaths than facilities without EMR. These effects are concentrated among patients under 50, and are larger among young children. Effects are also concentrated among patients who do not wish to be traced; these patients are in fact more likely to lapse from care and require tracing. Robust to additional specifications and supported by interview findings, the results demonstrate that an initial preference for privacy gives way to patient reinstatement in care when the health consequences are critical.

lapsed from care – even against their wishes – using data made accessible with the implementation of an electronic medical records (EMR) system. HIV patients in Malawi receive antiretroviral therapy (ART), a highly effective treatment that also prevents transmission, for free at clinics. Yet patients frequently lapse from care, resulting in increased community transmission and unnecessary deaths. The introduction of EMR allowed health providers to manage patient data, trace lapsed patients, and encourage lapsed patients to reinitiate treatment. We implement an event study analysis using data from 106 clinics that adopted EMR between 2007 and 2019 and find that the introduction of EMR leads to an immediate increase in the number of patients actively in care and to a decline in patient deaths. After five years of implementation, facilities with EMR have approximately 34 percent more patients in care and 28 percent fewer patient deaths than facilities without EMR. These effects are concentrated among patients under 50, and are larger among young children. Effects are also concentrated among patients who do not wish to be traced; these patients are in fact more likely to lapse from care and require tracing. Robust to additional specifications and supported by interview findings, the results demonstrate that an initial preference for privacy gives way to patient reinstatement in care when the health consequences are critical.

Challenging the relevance of the private/public dichotomy **for 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

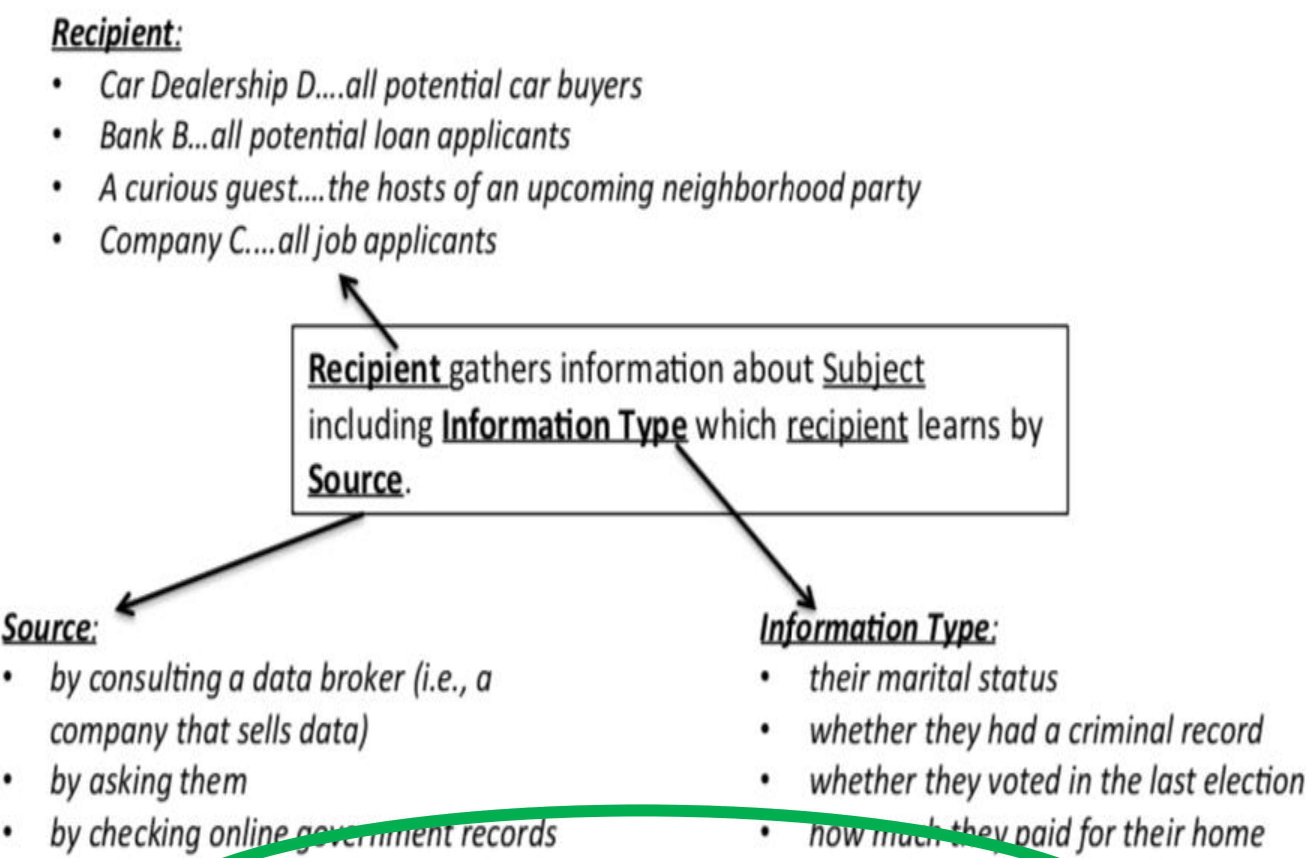
Benchmarks for a meaningful conception of privacy

Faithful to common use

Clear and rigorous

Reveals privacy’s ethical significance

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**.

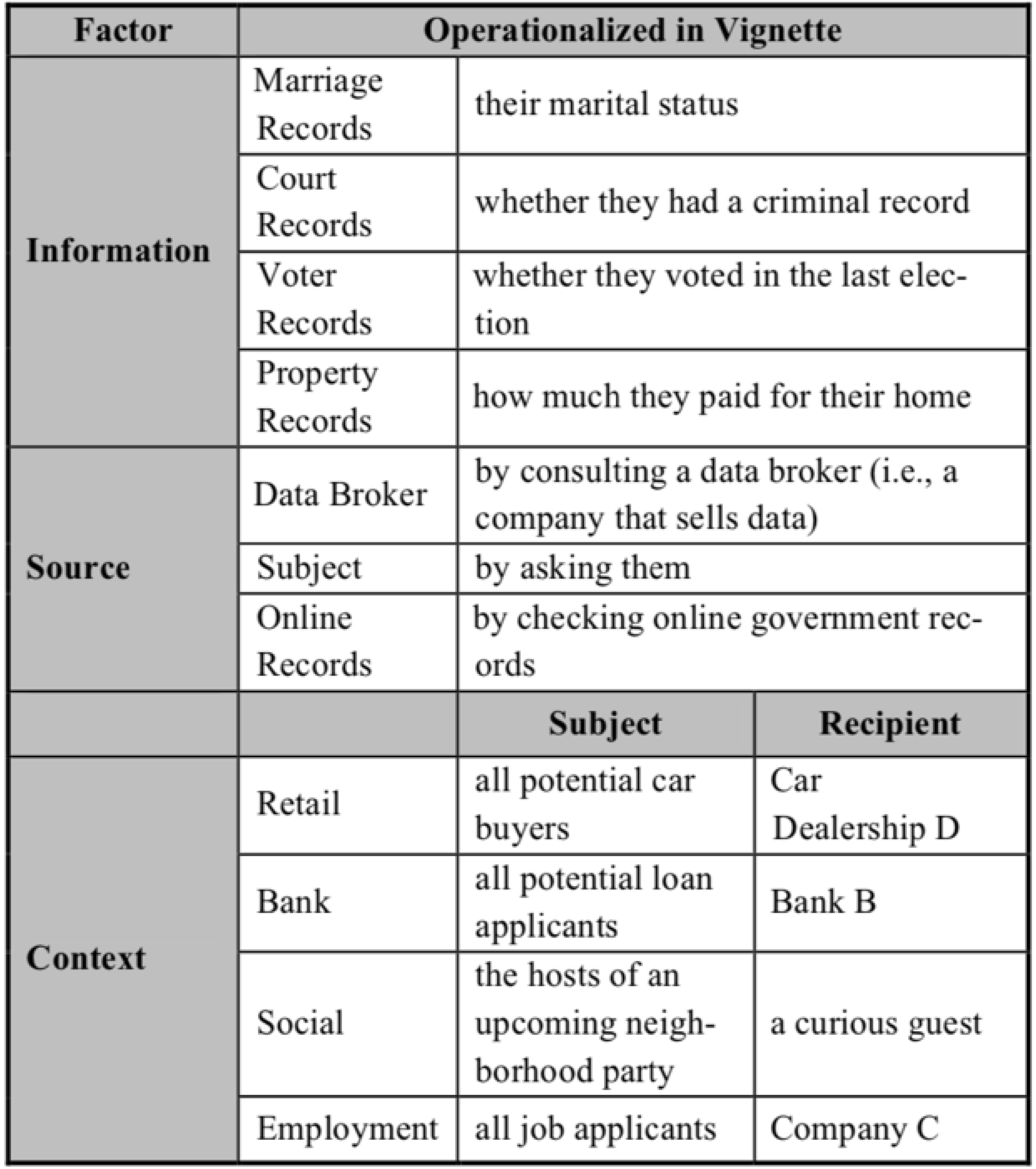
Source:

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

Information Type:

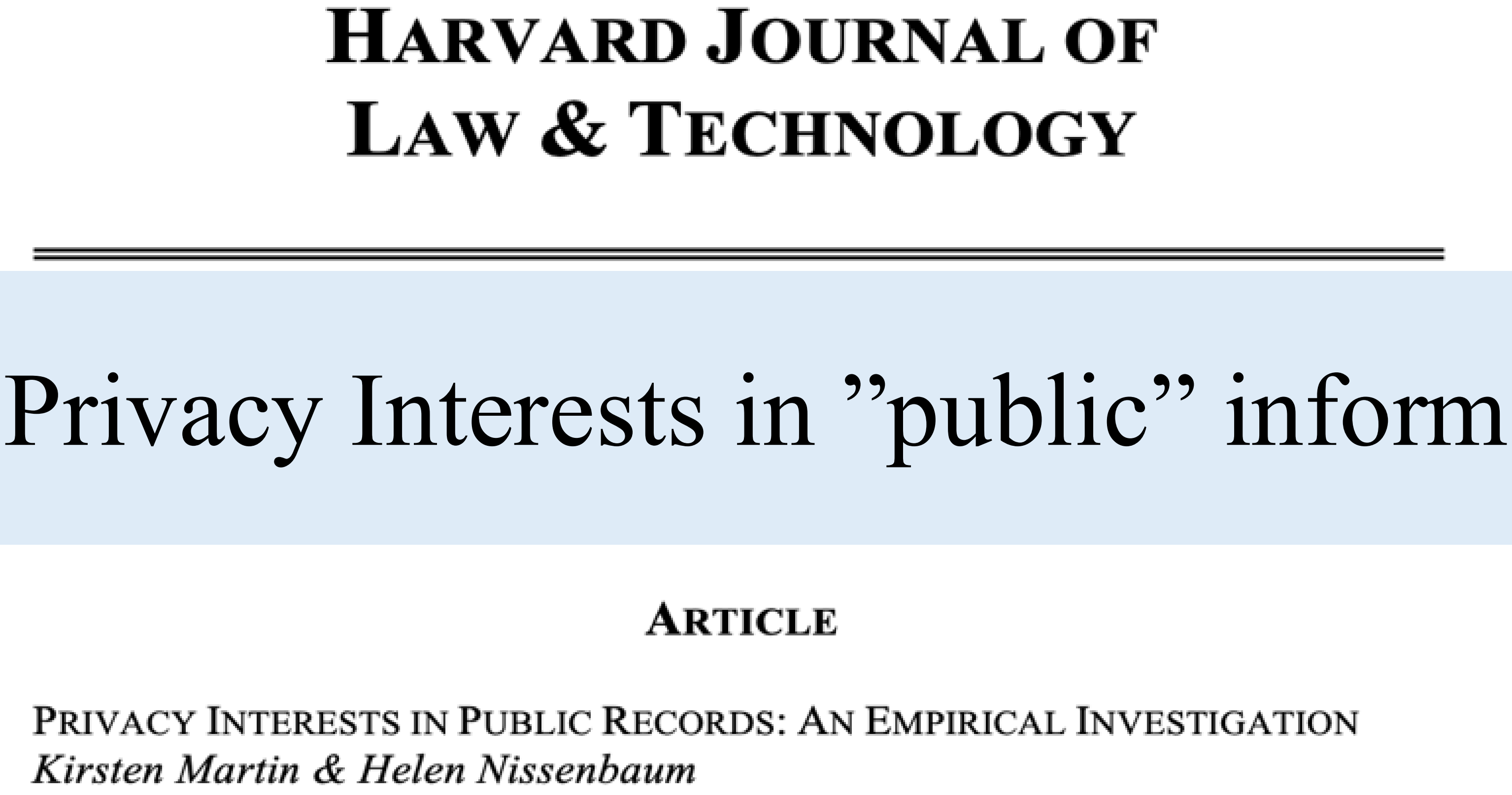
- *their marital status*
- *whether they had a criminal record*
- *whether they voted in the last election*
- *how much they paid for their home*

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

II. Privacy Interests in ”public” information

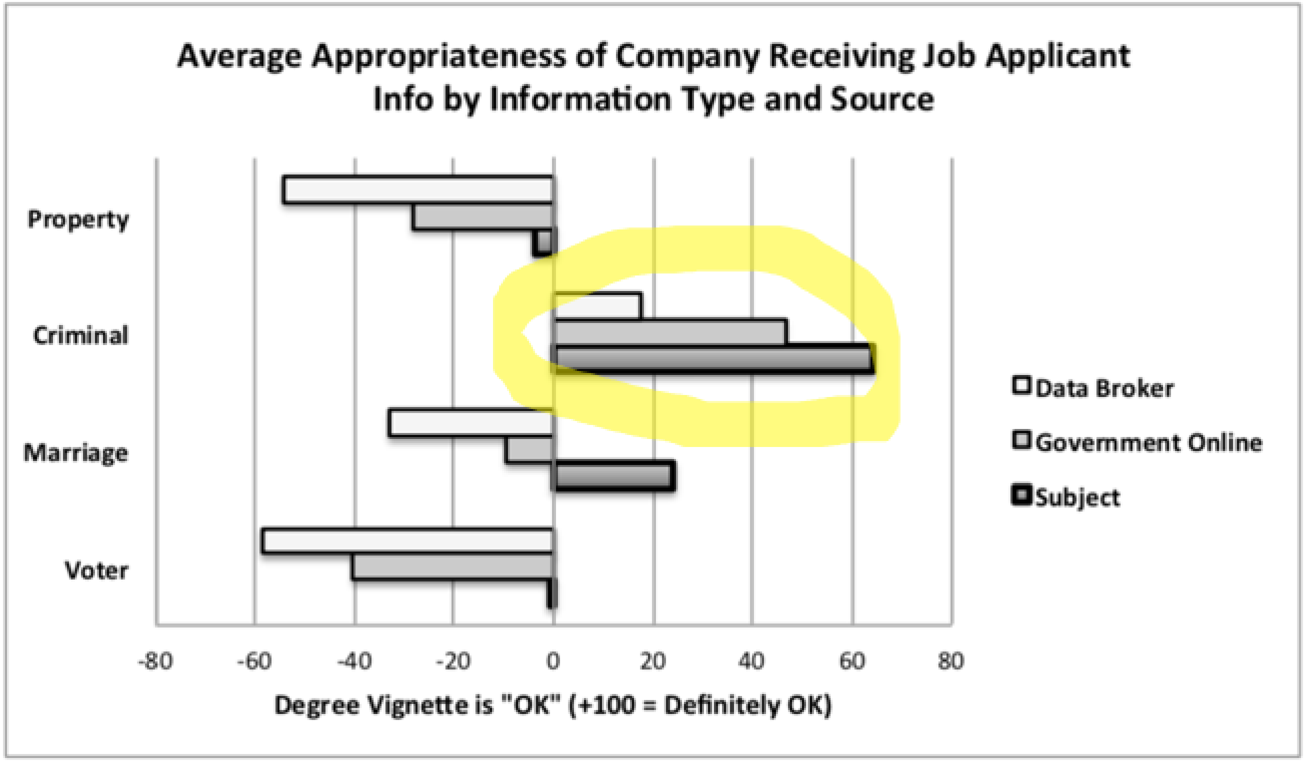


HARVARD JOURNAL OF
LAW & TECHNOLOGY

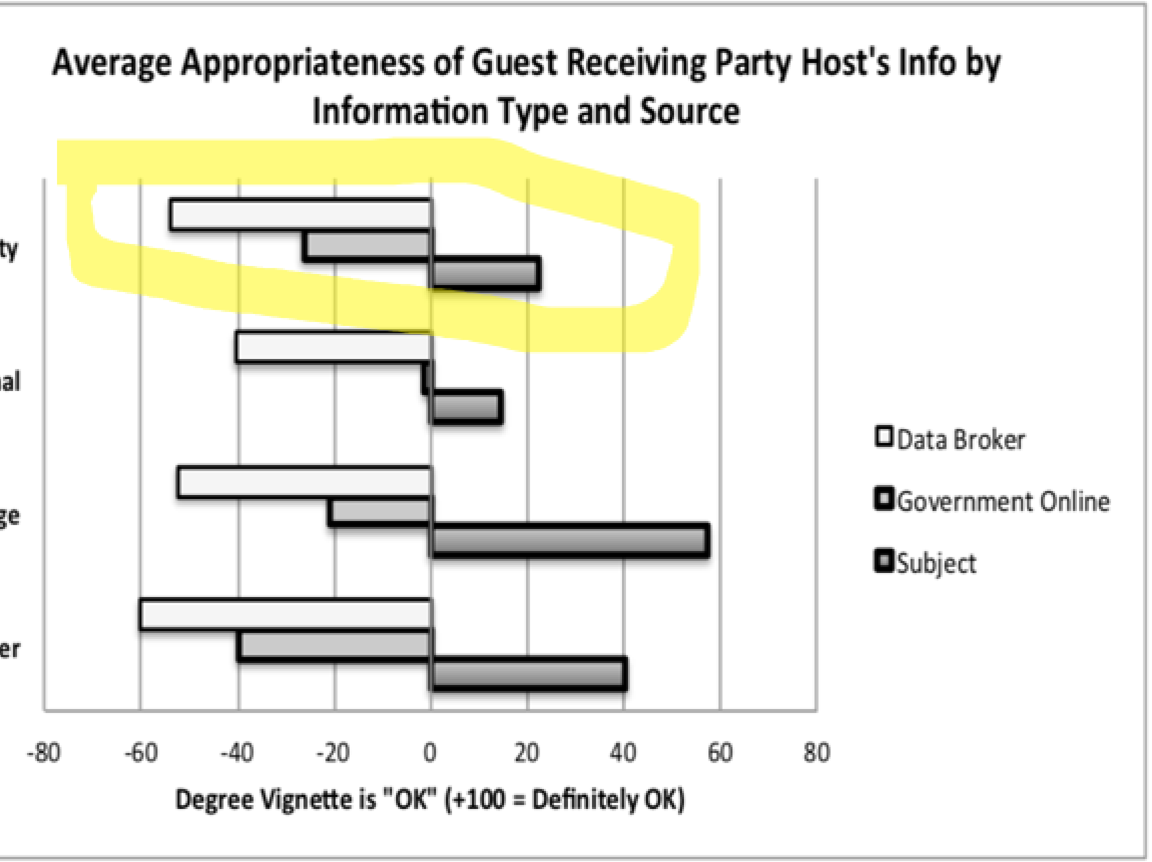
ARTICLE

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

NOT ”Anything goes!”

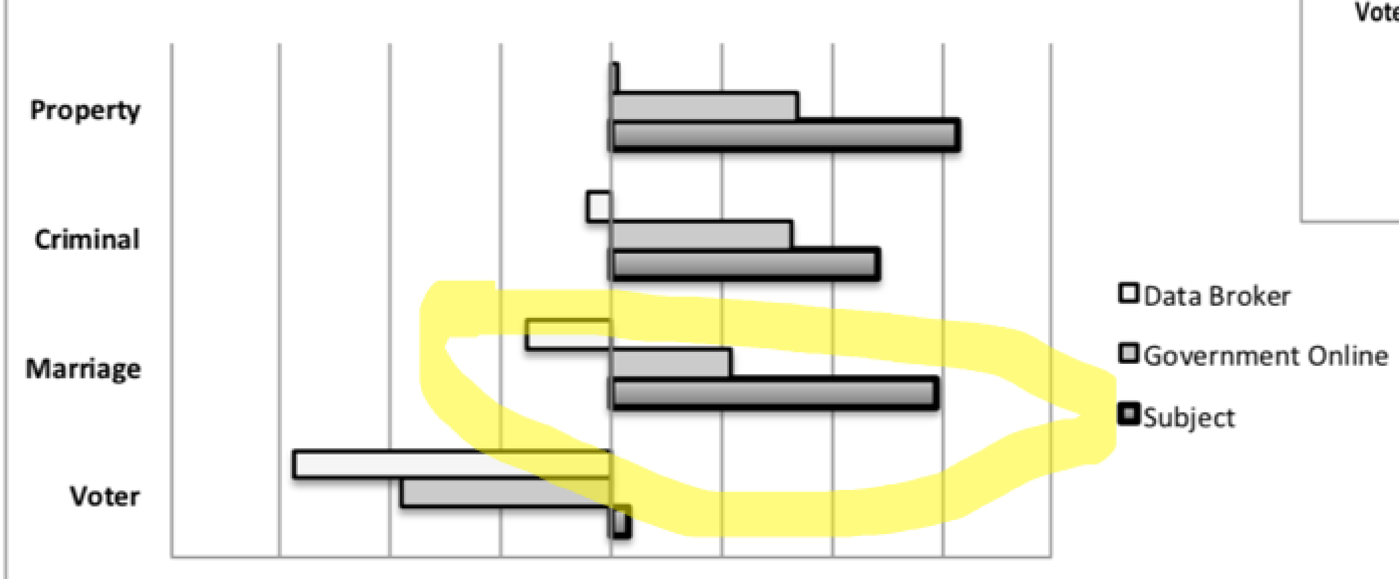


Average Appropriateness of Company Receiving Job Applicant Info by Information Type and Source



Average Appropriateness of Guest Receiving Party Host's Info by Information Type and Source

Average Appropriateness of Bank Receiving Loan Applicant Info by Information Type and Source



In sum: Even if data is available in public records, respondents cared about the sources of the data not merely that it was public, viz. other parameters matter.

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

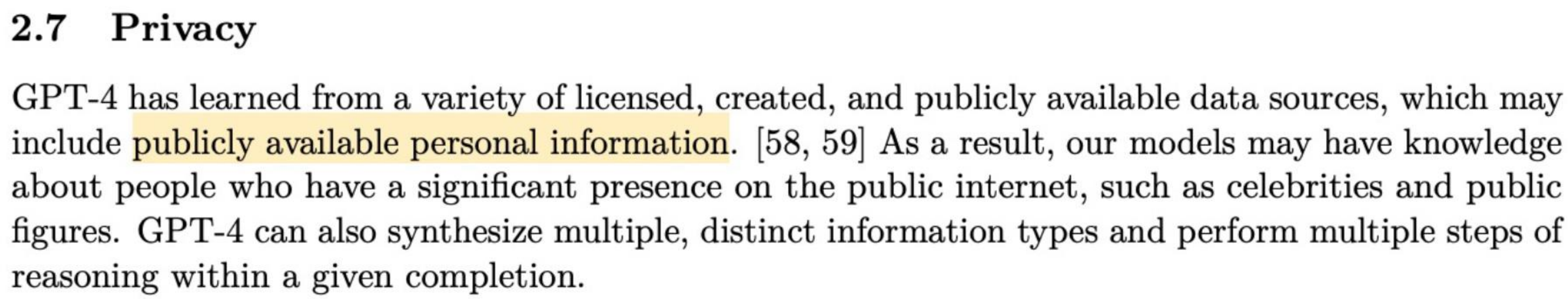
Clearview AI

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.

Contextual Integrity – NOT

No flow, no collection, secrecy

……..of sensitive information

Control over personal information

…….that is sensitive

Balance and trade off

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

“notice + choice”

“informed consent”

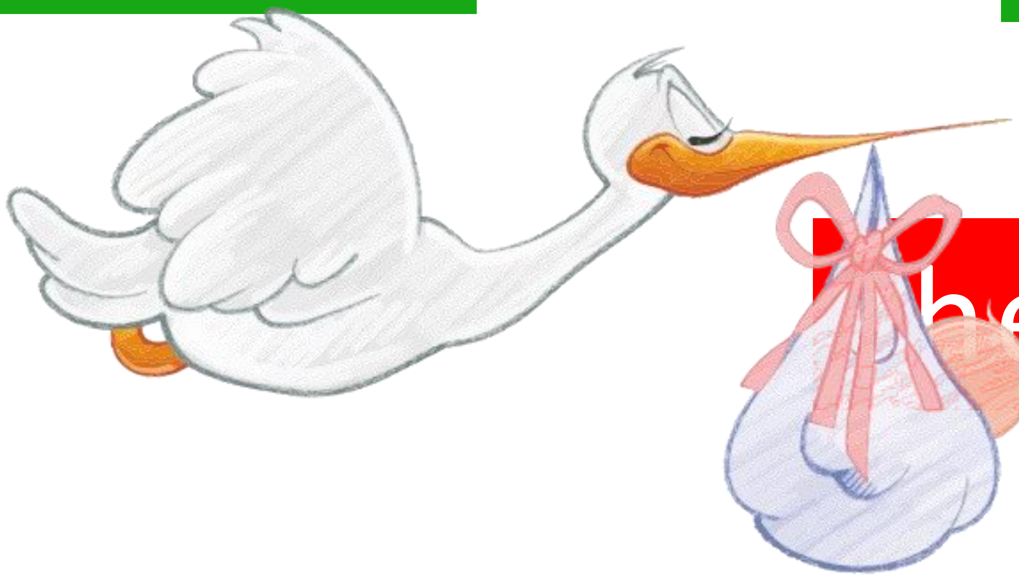
present-day

privacy nightmare

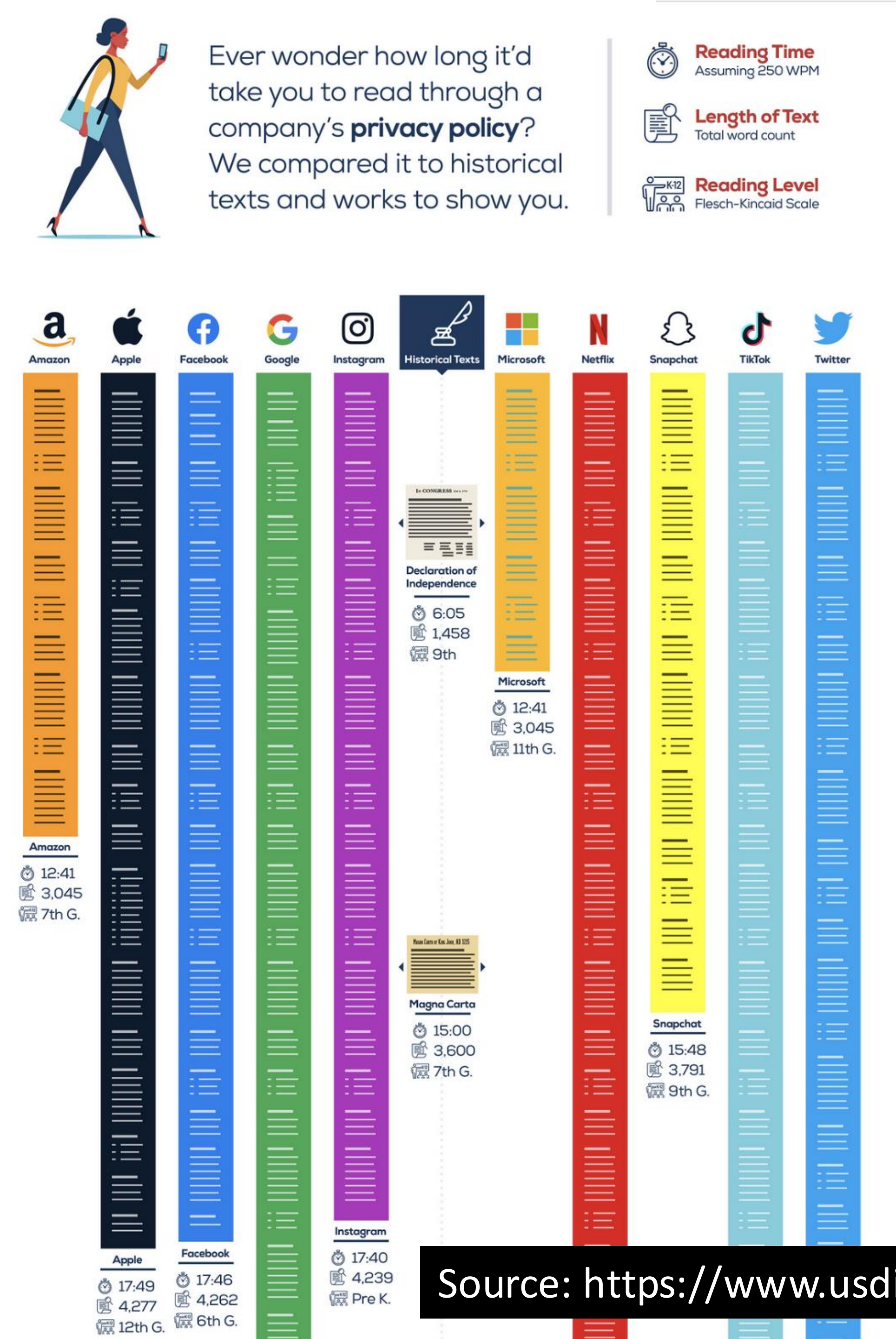
Guided by Fair Information Principles

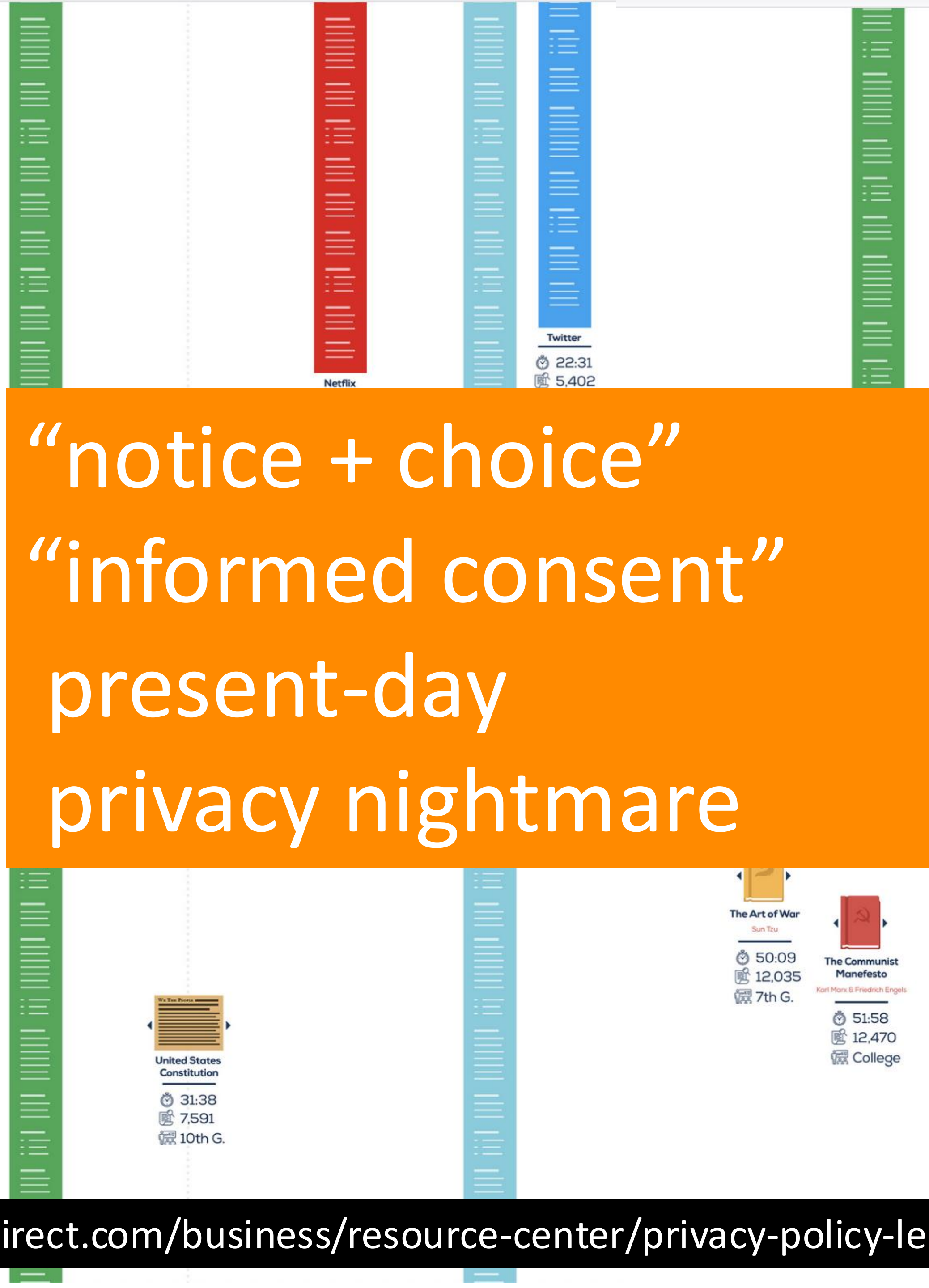
No secret databases
Know content/use
Purpose/use limit
Correction
Security/reliability

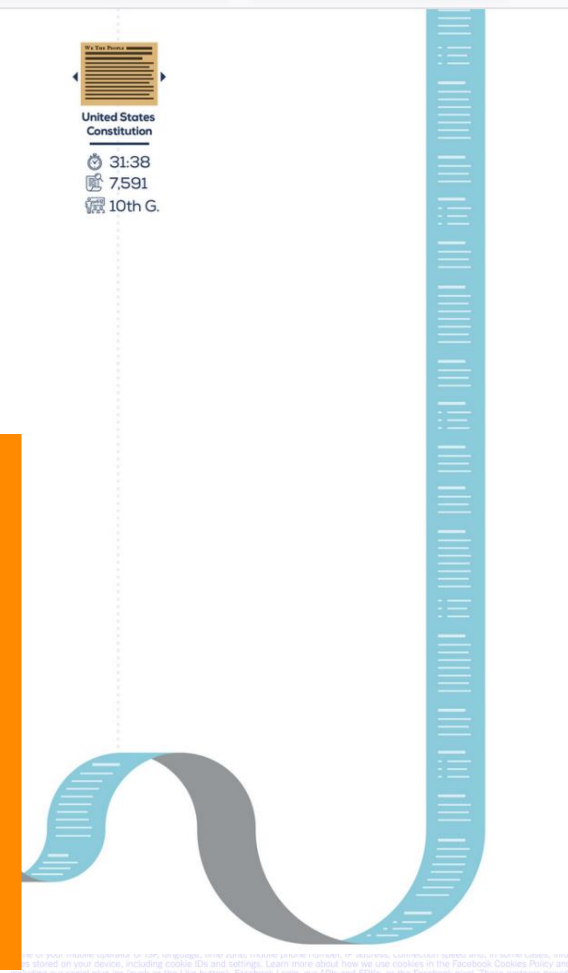
Control = **Notice & Choice**



The privacy policy…





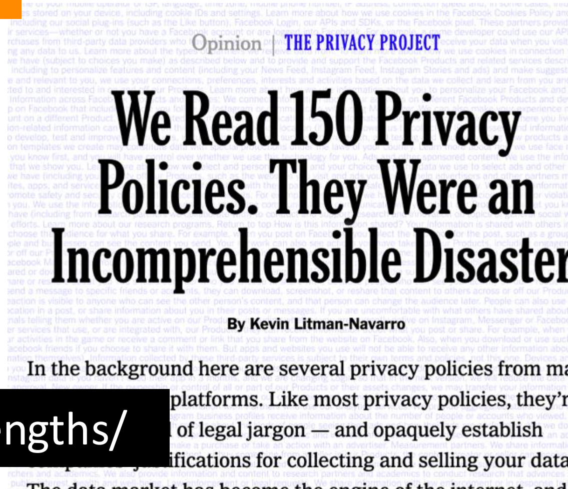


“notice + choice”

“informed consent”

present-day

privacy nightmare



Opinion | THE PRIVACY PROJECT

We Read 150 Privacy Policies. They Were an Incomprehensible Disaster

By Kevin Litman-Navarro

In the background here are several privacy policies from ma
platforms. Like most privacy policies, they'r
of legal jargon — and opaquely establish
ifications for collecting and selling your data

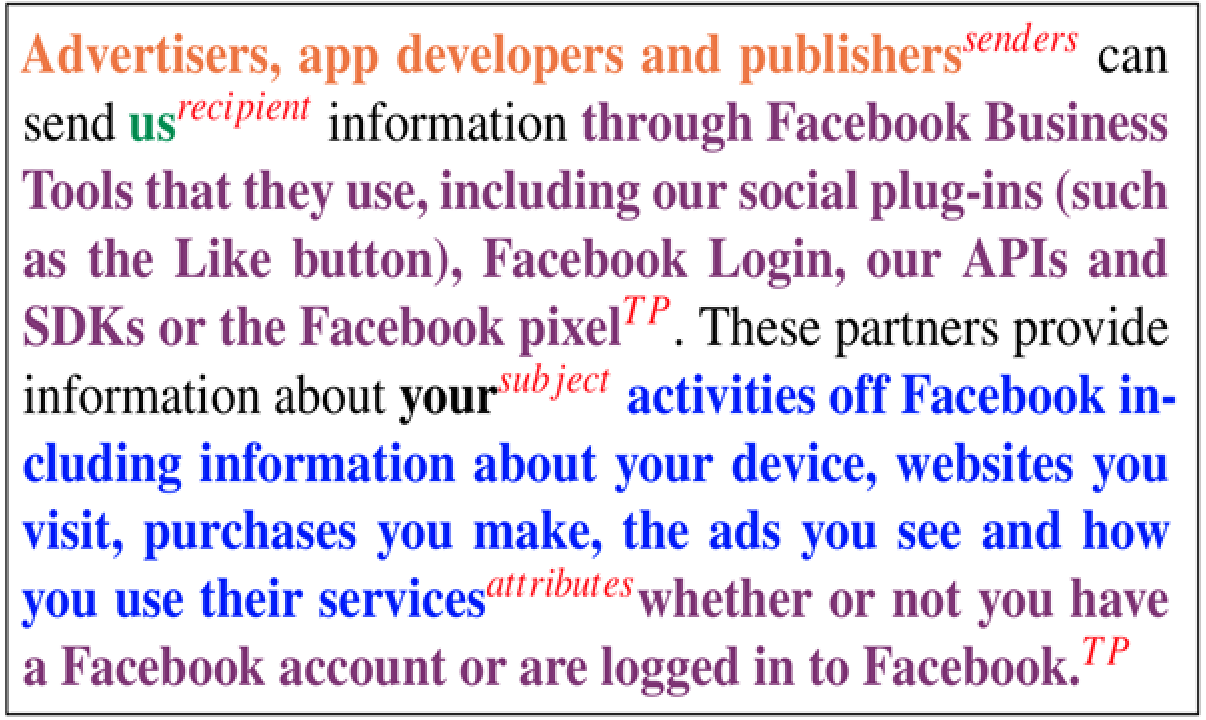
Source: https://www.usdirect.com/business/resource-center/privacy-policy-lengths/

The Seventh AAAI Conference on Human
Computation and Crowdsourcing (HCOMP-19)

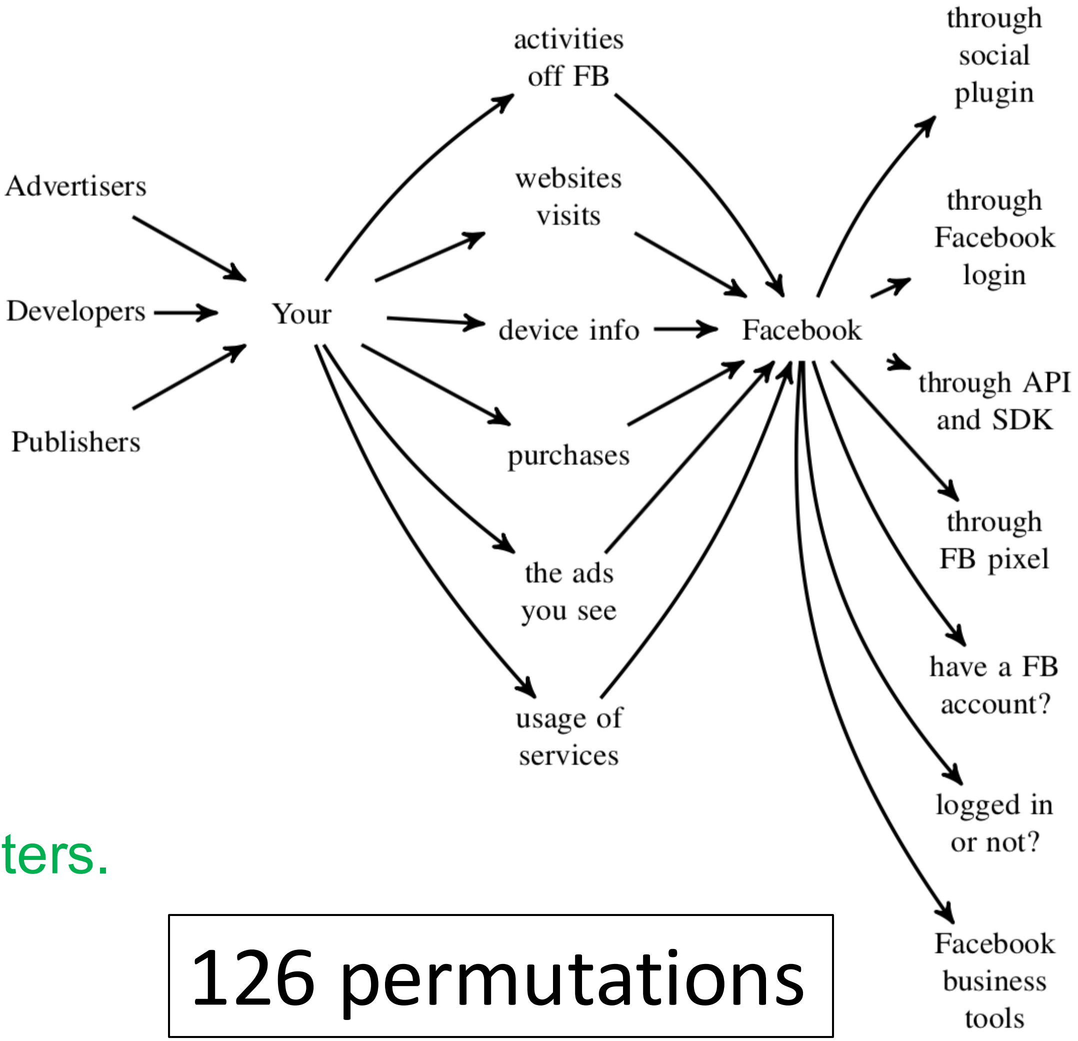
Going against the (Appropriate) Flow:
A Contextual Integrity Approach to Privacy Policy Analysis

Yan Shvartzshnaider,[*1,2] **Noah Apthorpe,**[*2] **Nick Feamster,**[3] **Helen Nissenbaum**[4]
[1]New York University, [2]Princeton University, [3]University of Chicago, [4]Cornell Tech
yansh@nyu.edu, apthorpe@cs.princeton.edu, feamster@uchicago.edu, helen.nissenbaum@cornell.edu

Analysis: CI Parameter Bloating



Advertisers, app developers and publishers^{senders} can send **us**^{recipient} information **through Facebook Business Tools that they use, including our social plug-ins (such as the Like button), Facebook Login, our APIs and SDKs or the Facebook pixel**^{TP}. These partners provide information about **your**^{subject} **activities off Facebook including information about your device, websites you visit, purchases you make, the ads you see and how you use their services**^{attributes}**whether or not you have a Facebook account or are logged in to Facebook.**^{TP}



New work automates tagging operation for parameters.

126 permutations

Consent regime punts decisions to data subjects

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

Q: Isn’t this about implementation alone?

ENVIRONMENTAL CHANGE

SCIENTIFIC DISCOVERIES

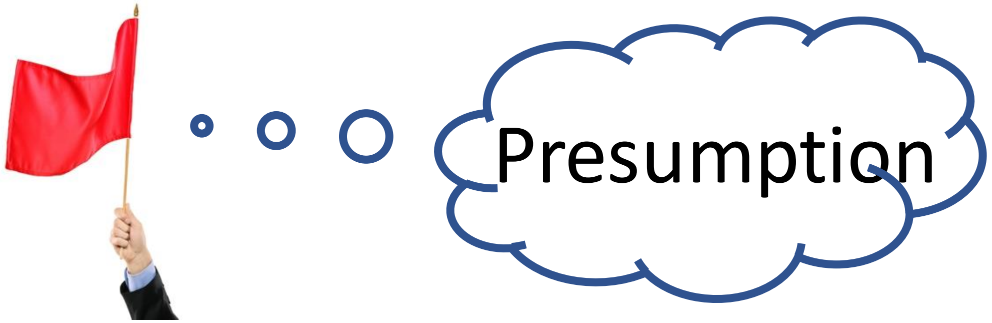
TYRANNY OF CONVENTION

NO NORMS?

CULTURAL SHIFT

Heuristic (1st approximation)

- 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
- Check conformance
  - ➢Yes ✓
  - ➢No ✗
  - ➢Other ?



what if

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

or

No relevant entrenched norm(al) guide or shape expectations

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

Benchmarks for a meaningful conception of privacy

Faithful to common use

Clear and rigorous

Reveals privacy's ethical significance

PART TWO: The ethical argument

- Social Contexts
- Contextual informational norms
- Contextual values ends purpose

When tech practices are unprecedented

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)

When tech practices are unprecedented

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)

"Privacy harms"

Privacy harms

Liberties

Speech

Association

Autonomy

Fairness

Equity

Justice

Security

Informational benefits

Profit

Security

Efficiency

Risk reduction (banks, ads)

Speech

A contextual approach to privacy

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)

Data flow disruptions: data types, recipients

Improved health outcomes

U.S. Department of Health & Human Services

NIH National Institutes of Health
Turning Discovery Into Health

Health Information | Grants & Funding | New

! COVID-19

- Get the latest public health information from CDC
- Get the lates

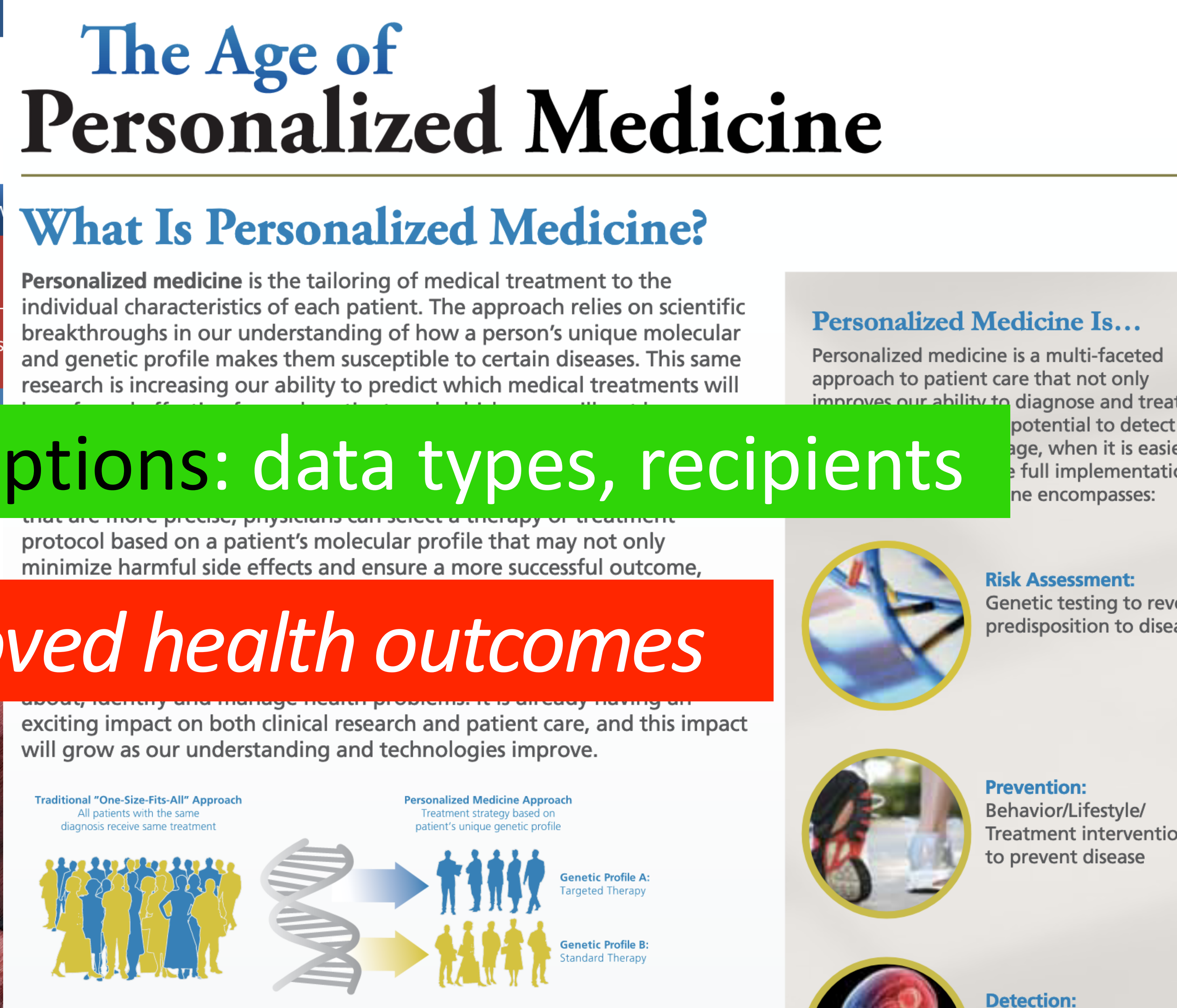
Home » About

NIH...

NIH...Turning Discovery Into Health®

- From the Director
- Our Biggest Health Challenges
- A Healthy Mind
- The Future of Biomedicine
- Transformative Technologies
- Research for Healthy Living
- The Promise of Precision Medicine
- Looking Forward

Personalized



The Age of
Personalized Medicine

What Is Personalized Medicine?

Personalized medicine is the tailoring of medical treatment to the individual characteristics of each patient. The approach relies on scientific breakthroughs in our understanding of how a person's unique molecular and genetic profile makes them susceptible to certain diseases. This same research is increasing our ability to predict which medical treatments will

protocol based on a patient's molecular profile that may not only minimize harmful side effects and ensure a more successful outcome,

exciting impact on both clinical research and patient care, and this impact will grow as our understanding and technologies improve.

Traditional "One-Size-Fits-All" Approach
All patients with the same diagnosis receive same treatment

Personalized Medicine Approach
Treatment strategy based on patient's unique genetic profile

Genetic Profile A:
Targeted Therapy

Genetic Profile B:
Standard Therapy

Personalized Medicine Is…

Personalized medicine is a multi-faceted approach to patient care that not only improves our ability to diagnose and trea

potential to detect

age, when it is easie

full implementati

ne encompasses:

Risk Assessment:
Genetic testing to reve
predisposition to disea

Prevention:
Behavior/Lifestyle/
Treatment interventio
to prevent disease

Detection:

Contextual functions, purposes and values

healthcare: cure disease, alleviate pain and suffering, equity …

E.g. how confidentiality functions in healthcare contexts [intelligence of the Hippocratic Oath]

Contextual functions, purposes and values

healthcare: cure disease, alleviate pain and suffering, equity …

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)

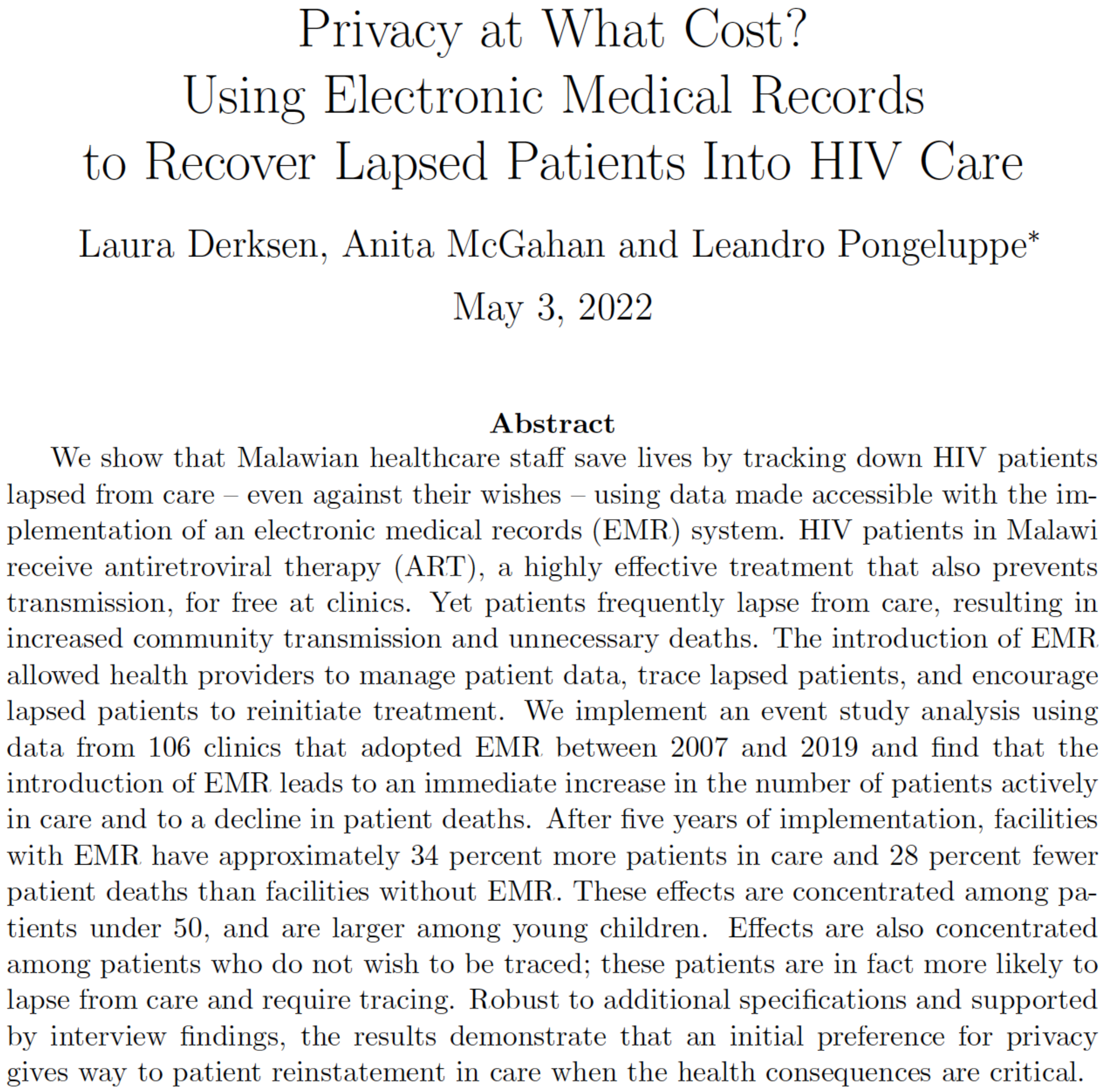
Is not only only about harm to the **individual (P. Regan)**
Not contrary to **societal** values (typical: security)
Not contrary to **utility*** (research, personalization)

Not this

“Need to trade off privacy for other goods!”

$Providing\ information \neq giving\ up\ privacy$
$Limiting\ data\ subjects'\ control \neq giving\ up\ privacy$

Legitimacy (”appropriate flow”) runs deeper, is more tailored



Privacy at What Cost? Using Electronic Medical Records to Recover Lapsed Patients Into HIV Care

Laura Derksen, Anita McGahan and Leandro Pongeluppe*

May 3, 2022

Abstract

We show that Malawian healthcare staff save lives by tracking down HIV patients lapsed from care – even against their wishes – using data made accessible with the implementation of an electronic medical records (EMR) system. HIV patients in Malawi receive antiretroviral therapy (ART), a highly effective treatment that also prevents transmission, for free at clinics. Yet patients frequently lapse from care, resulting in increased community transmission and unnecessary deaths. The introduction of EMR allowed health providers to manage patient data, trace lapsed patients, and encourage lapsed patients to reinitiate treatment. We implement an event study analysis using data from 106 clinics that adopted EMR between 2007 and 2019 and find that the introduction of EMR leads to an immediate increase in the number of patients actively in care and to a decline in patient deaths. After five years of implementation, facilities with EMR have approximately 34 percent more patients in care and 28 percent fewer patient deaths than facilities without EMR. These effects are concentrated among patients under 50, and are larger among young children. Effects are also concentrated among patients who do not wish to be traced; these patients are in fact more likely to lapse from care and require tracing. Robust to additional specifications and supported by interview findings, the results demonstrate that an initial preference for privacy gives way to patient reinstatement in care when the health consequences are critical.

Here, privacy as secrecy!

Privacy as Contextual Integrity Defined

Contextual Integrity requires that information flows conform with justifiable (legitimate) informational norms.

Privacy as Contextual integrity

- A positive conception of privacy
- Offers benefits to societies and individuals
- Supports societal and contextual goods: fairness, justice, autonomy, security, health, liberty, utility, etc.

Why data governance?

What we need

I. We need to know more

- More about contexts
- Ends, purposes and values
    - We cannot avoid semantics
- Informational norms: make the implicit explicit
- Improve methods to uncover, map, and visualize
- About impacts of data flows on societal & contextual ends as well as on data subjects and other stakeholders

II. Sensible regulation

- Require data flows to be mapped with values for all parameters
- Map flows against contextual ends and values
- Impose substantive constraints (where necessary)*
- Revisit sectoral privacy laws, e.g. HIPAA, FERPA, GLBA*
- Avoid the "privacy – utility" trap
- Invite domain experts to the table

*Data subject consent may be neither necessary nor sufficient

*Novel tech and regulatory dodges

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*