

# **DATA ETHICS LECTURE 2**

**RECAP DATA COLLECTION**

**PREVIEW PROMISES**

---

Ali Alkhatib

@\_alialkhatib || [hi@al2.in](mailto:hi@al2.in)

March 17, 2022

# ROADMAP FOR TODAY

- Administrivia
- Recap Data Collection
- Preview Promises
- Preview readings for 1-2 topics

# **ADMIN-Y THINGS**

- **Canvas**

everyone should have access now, if that's not the case then let me know!

- **Readings**

More readings available on Canvas as PDFs

- **Reading time check**

How long did readings take?

→ google docs noisy survey

*check the zoom chat for a link*

# **DATA COLLECTION (RECAP)**

---

# CONSENT

legally  
ambiguous data  
collection



The illustration depicts a red mobile application screen. At the top, there are two white buttons: "What Is Depression?" on the left and "Message Us" on the right. Below these are two larger white buttons: "Message A Crisis Counselor On WhatsApp" in the center and "Text A Crisis Counselor" on the left. To the right of the center button is a partially visible button labeled "Symptoms". The background is a textured red color.

POLITICO

TECHNOLOGY

Suicide hotline shares data with for-profit spinoff, raising ethical questions

The Crisis Text Line's AI-driven chat service has gathered troves of data from its conversations with people suffering life's toughest situations.

By ALEXANDRA S. LEVINE  
01/28/2022 04:30 AM EST  
Updated: 01/27/2022 05:16 PM EST

Crisis Text Line is one of the world's most prominent mental health support

# CONSENT

legally  
ambiguous data  
collection

June 15, 2021 12:00AM EDT

Available In English [\[more\]](#)

## UN Shared Rohingya Data Without Informed Consent

Bangladesh Provided Myanmar Information that Refugee Agency Collected

[f](#) [t](#) [g](#) [e](#) [\[share\]](#)



Rohingya refugees headed to Bhasan Char island prepare to board navy vessels from the southeastern port city of Chittagong, Bangladesh on February 15, 2021. © 2021 AP Photo

# CONSENT

legally  
ambiguous data  
collection



Adam Ferriss

## The Secretive Company That Might End Privacy as We Know It

A little-known start-up helps law enforcement match photos of unknown people to their online images — and “might lead to a dystopian future or something,” a backer says.

Give this article         1.2K

---

 By **Kashmir Hill**

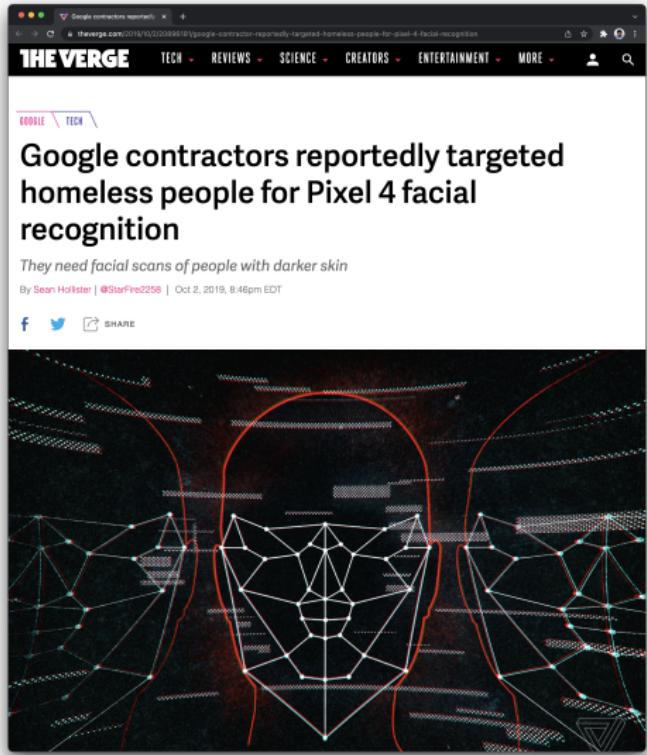
Published Jan. 18, 2020 Updated Nov. 2, 2021

Leer en español

Special offer. Subscribe for \$4.99 \$1 a week.

# CONSENT

legally  
ambiguous data  
collection



# CONSENT

legally  
ambiguous data  
collection

Screenshot of a web browser showing the Wikipedia page for "General Data Protection Regulation". The page title is "General Data Protection Regulation" and it is described as "From Wikipedia, the free encyclopedia". The page content discusses the GDPR as a regulation in EU law on data protection and privacy in the European Union (EU) and the European Economic Area (EEA). It highlights the GDPR's importance as a privacy law and its relationship to other EU laws like the Charter of Fundamental Rights of the European Union. The page also notes its supersession of the Data Protection Directive 95/46/EC.

The right side of the screen displays a summary of the "Regulation (EU) 2016/679" (GDPR) under the heading "Regulation (EU) 2016/679". The summary includes:

- Title:** Regulation on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (Data Protection Directive)
- Made by:** European Parliament and Council of the European Union
- Journal reference:** L119, 4 May 2016, p. 1–88<sup>6</sup>
- Date made:** 14 April 2016
- Implementation date:** 25 May 2018
- Preparative texts:** COM(2012)010 final – 2012/010 (CDD)
- Other legislation:** Data Protection Directive
- Replaces:** Data Protection Directive
- Current legislation:** California Consumer Privacy Act (CCPA), adopted on 28 June 2018, has many similarities with the GDPR.<sup>7</sup>

At the bottom of the page, there is a "Contents" section with links to "1 Contents" and "2 Contents".

# CONSENT

legally  
ambiguous data  
collection

Screenshot of a Wikipedia page about the California Consumer Privacy Act (CCPA). The page includes a sidebar with the Wikipedia logo, navigation links, and a "Contents" box. The main content area features the title "California Consumer Privacy Act" and a summary of the law's purpose and history. A box on the right provides detailed legislative information, and a "Status: Current legislation" box is highlighted.

Not logged in | Talk | Contributions | Create account | Log in

Article | Talk | Read | Edit | View history | Search Wikipedia |

WIKIPEDIA  
The Free Encyclopedia

Main page  
Contents  
Current events  
Random article  
About Wikipedia  
Contact us  
Donate  
Contribute  
Help  
Learn to edit  
Community portal  
Recent changes  
Upload file  
Tools  
What links here  
Related changes  
Special pages  
Permanent link  
Page information  
Cite this page  
Wikidata item  
Print/export  
Download as PDF  
Printable version  
Languages  
Esperanto  
فارسی  
Français  
Português  
ไทย  
Edit links

California Consumer Privacy Act

From Wikipedia, the free encyclopedia

The California Consumer Privacy Act (CCPA) is a state statute intended to enhance privacy rights and consumer protection for residents of California, United States. The bill was passed by the California State Legislature and signed into law by Jerry Brown, Governor of California, on June 28, 2018, to amend Part 4 of Division 3 of the California Civil Code.<sup>[1]</sup> Officially called AB-375, the act was introduced by Ed Chau, member of the California State Assembly, and State Senator Robert Hertzberg.<sup>[3][4]</sup>

Amendments to the CCPA, in the form of Senate Bill 1121, were passed on September 13, 2018.<sup>[5][6]</sup> Additional substantive amendments were signed into law on October 11, 2019.<sup>[7]</sup> The CCPA became effective on January 1st, 2020.<sup>[8]</sup> In November 2020, California voters passed Proposition 24, also known as the California Privacy Rights Act, which amends and expands the CCPA.<sup>[9]</sup>

California Consumer Privacy Act

California State Legislature

Full name California Consumer Privacy Act of 2018<sup>[1]</sup>

Introduced January 3, 2018

Signed into law June 28, 2018

Governor Jerry Brown

Code California Civil Code

Section 1798.100

Resolution AB-375 (2017–2018 Session)

Website Assembly Bill No. 375<sup>[5]</sup>

Status: Current legislation

Contents [hide]

- 1 Intentions of the Act
  - 1.1 Compliance
  - 1.2 Responsibility and accountability
  - 1.3 Sanctions and remedies
- 2 Definition of personal data
- 3 History
- 4 Exemptions
- 5 See also
- 6 References
- 7 Further reading
- 8 External links

Intentions of the Act [edit]

The intentions of the Act are to provide California residents with the right to:

1. Know what personal data is being collected about them.

# SURVEILLANCE

coercive  
settings

The New York Times

CRITIC'S NOTEBOOK

## Dance, I Said — Dance! And Leave the Package on the Porch.

The combination of next-day delivery, Ring surveillance footage and TikTok has put a spotlight on Amazon drivers. But it's also created a new main character: the package itself.

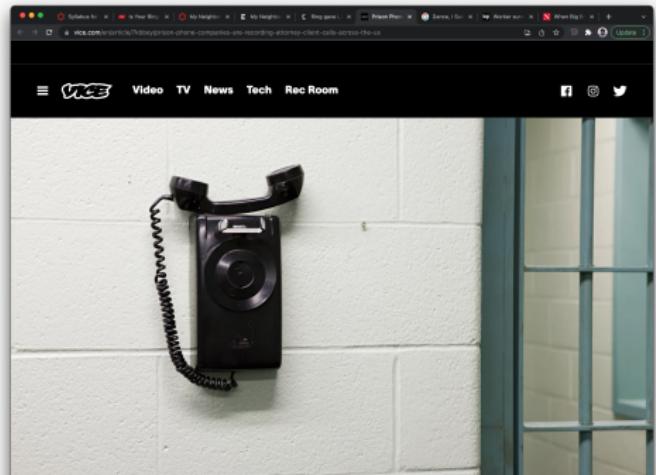
09:22

Give this article 29

Special Offer. Subscribe and enjoy unlimited articles with Basic Digital Access.

# SURVEILLANCE

coercive  
settings



A black and white photograph of a payphone mounted on a light-colored brick wall in a prison setting. A metal door with bars is visible on the right.

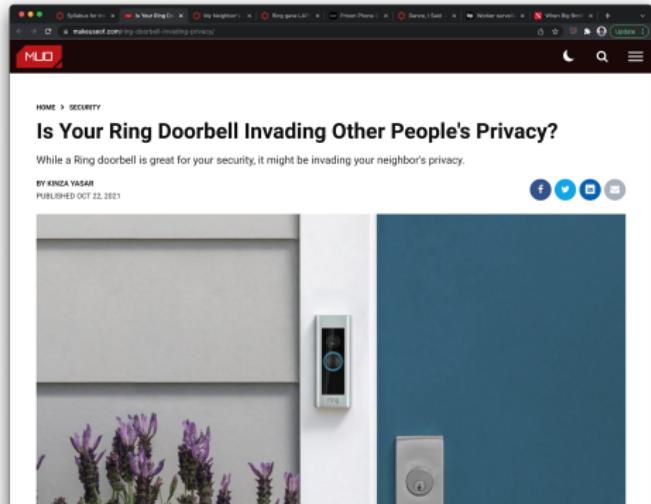
MOTHERBOARD  
TECH BY VICE

## Prison Phone Companies Are Recording Attorney-Client Calls Across the US

Lawyers say their conversations with incarcerated people are being recorded and analyzed by private companies in at least nine US states.

# SURVEILLANCE

coercive  
settings



HOME > SECURITY

## Is Your Ring Doorbell Invading Other People's Privacy?

While a Ring doorbell is great for your security, it might be invading your neighbor's privacy.

BY KINZA YASAR  
PUBLISHED OCT 22, 2021

A doctor in the UK recently won a case and a possible £100,000 pay-out after a judge ruled that a neighbor's Ring doorbell breached her right to privacy.

Most homeowners want to secure their homes from burglars and thieves. As a result, the use of outdoor surveillance camera systems including Ring doorbells is mushrooming around neighborhoods. But sadly, many people do not take their neighbors into consideration when installing high-tech gadgets around their properties.

So, does a Ring doorbell actually risk other people's privacy, and how? Should there be rules regarding the way your Ring doorbell is installed so it doesn't infringe on your neighbor's privacy?

[Can Your Ring Doorbell Invade Other's Privacy?](#)

# SURVEILLANCE

coercive  
settings

The New York Times

ASK REAL ESTATE

## My Neighbor's Door Camera Faces My Apartment. Is That Legal?

Rental tenants typically cannot install cameras — or anything else — in common hallways. But landlords can.

Give this article       311



Nadia Pilon

By Ronda Kaysen

Aug. 28, 2021

**Q:** I live in a six-story rental building in Washington Heights, with five apartments per floor. My neighbor across the hall installed a [Ring camera](#) that captures the entire floor. It faces my apartment directly, providing a clear view inside whenever I open the door. Aside from the fact that it's uncomfortable knowing that all my comings and goings are being recorded, I wonder if this is legal. What can I do about it?

**A:** Your neighbor does not have the right to place anything in the hallway, including a door camera, without the landlord's consent.

Special Offer. Subscribe and enjoy unlimited articles with Basic Digital Access.

# SURVEILLANCE

coercive  
settings

The image features a white and black Ring Video Doorbell camera centered in the foreground. In the background, a screenshot of a Los Angeles Times article is displayed. The headline reads "Ring tapped a network of influencers to promote its cameras. They were LAPD officers". Below the headline, there's a photograph of a Los Angeles Police Department badge. The article's content discusses how Ring used police officers as influencers to promote its products.

Los Angeles Times illustration; photograph by Rick Meyer / Los Angeles Times

BY JOHANA BHUYAN | LOS ANGELES TIMES EXCLUSIVE

JUNE 17, 2023 5 AM PT

FOR SUBSCRIBERS

[f](#) [t](#) [r](#)

# SURVEILLANCE

coercive  
settings

The Washington Post logo is visible at the top right of the browser window.

**Tech at Work**

## Keystroke tracking, screenshots, and facial recognition: The boss may be watching long after the pandemic ends

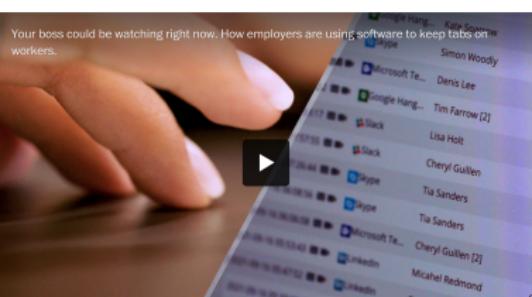
What workers should know about corporate surveillance software as companies consider permanent remote work policies

By Danielle Abril and Drew Harwell

September 24, 2021 at 7:00 a.m. EDT

Listen to article 8 min

Your boss could be watching right now. How employers are using software to keep tabs on workers.



Businesses are turning to software that can track remote employees' productivity. But the tools can also record their keystrokes, screens and even audio. (Jonathan Borba/The Washington Post)

Share, Print, Email icons at the bottom.

# CONTEXT

data without  
context

The New York Times

## *Why Stanford Researchers Tried to Create a 'Gaydar' Machine*

Give this article    69



Michal Kosinski and Yilun Wang, co-authors of a study that claims to show that a computer program can detect sexual orientation from photos of faces. Christie Hemm Klok for The New York Times

By Heather Murphy

# CONTEXT

data without  
context

Screenshot of a news article from the Thomson Reuters Foundation website.

The article title is: **Sentenced for a selfie: Middle East police target LGBTQ+ phones**.

The byline reads: **by Maya Gebelly and Avi Asher-Schapiro | [@GebellyM](#) | Thomson Reuters Foundation**

The date is: **Monday, 7 March 2022 01:00 GMT**



A photograph showing two individuals sitting on a bench outdoors. They are positioned in front of a large, horizontal rainbow flag. The flag is composed of several distinct horizontal stripes of different colors. The people appear to be in a public space, possibly a park or a street, with some foliage visible in the background.

WhatsApp, Grindr and Facebook were once a place that gay, bisexual and trans Arabs could find

# CONTEXT

data without  
context

**See Through Walls with Wi-Fi!**

Fadel Adib and Dina Katabi  
Massachusetts Institute of Technology  
[fadel,dk]@mit.edu

**ABSTRACT**

Wi-Fi signals are typically information carriers between a transmitter and a receiver. In this paper, we show that Wi-Fi can also extend our senses, enabling us to see moving objects through walls and behind closed doors. In particular, we can use such signals to identify the presence of people and objects in locations far from their locations. We can also identify simple gestures made behind a wall, and combine a sequence of gestures to communicate messages to a wireless receiver without carrying any transmitting device. The paper introduces two main innovations. First, it shows how one can use MIMO antennas to eliminate reflections from metallic objects and focus the receiver on a moving target. Second, it shows how one can track a human by creating a motion of a human body as an antenna array and tracking the resulting RF beam. We demonstrate the validity of our design by building it into USRP software radio and testing it in office buildings.

**Categorization and Subject Descriptors:** C.2.2 [Computer Systems Organization]: Computer Communications; Networks; H.5.2.5 [Information Interfaces and Presentation]: User interfaces - Input devices and strategies.

**Keywords:** Seeing Through Walls, Wireless, MIMO, Gesture-based User Interface

**1. INTRODUCTION**

Can Wi-Fi signals enable us to see through walls? For many years humans have fantasized about X-ray vision and played with the concept in comic books and sci-fi movies. This paper explores the potential of using Wi-Fi signals and recent advances in MIMO communications to build a device that can capture the motion of humans behind a wall and in closed rooms. Law enforcement personnel can use the device to avoid walking into an ambush, and minimize casualties in standoffs and hostage situations. Emergency responders can use it to navigate through collapsed structures. Ordinary users can leverage the device for gaining intrusion detection, privacy-enhanced monitoring of children and elderly, or personal security when stepping into dark alleys and unknown places.

The challenge of seeing through opaque materials is similar to radar and sonar imaging. Specifically, when there is no non-metallic wall, a fraction of the RF signal would penetrate the wall, reflect off objects and humans, and come back imprinted with a signature of what is inside a closed room. By capturing these reflections, we can image objects behind a wall. Building a device that can capture such reflections, however, is difficult because the signal power after traversing the wall twice (in and out of the room) is reduced by three to five orders of magnitude [11]. Even more challenging are the reflections from the wall itself, which are much stronger than the reflections from objects inside the room [11, 27]. Reflected off the wall overwhelm the receiver's analog-to-digital converter (ADC), preventing it from registering the minute variations due to reflections from objects behind the wall. This behavior is called the "Flash Effect" since it is analogous to how a mirror in front of the camera reflects the camera's flash and prevents it from capturing objects in the scene.

So how can one overcome these difficulties? The radar community has been investigating these issues, and has recently introduced a few other techniques. One approach can involve placing a thin metal plate behind the wall, and show them as black moving in a dim background [27, 41] (see the video at [6] for a reference). Today's state-of-the-art system requires 2 GHz of bandwidth, a large power source, and a 4-8 foot-long antenna array (2.4 meters) [12, 27].

Given the bulkiness of the device, operating power in such a wide spectrum is infeasible and impractical for other applications. The requirement for multi-GHz transmission is at the heart of how these systems work: they separate reflections off the wall from reflections from objects behind the wall based on their arrival times. They also need to identify sub-microsecond differences in multi-GHz bandwidth to filter the flash effect.<sup>1</sup> To address these limitations, an initial attempt was made in 2012 to see Wi-Fi to see through a wall [13]. However, to mitigate the flash effect, this post proposal needs to install an additional receiver behind the wall, and connect the two receivers behind and in front of the wall to a front end via wires [13].

The objective of this paper is to enable a see-through-wall technology that is low-bandwidth, low-power, compact, and accessible to ordinary users. To this end, the paper introduces Wi-Vi, a see-through-wall device that enjoys Wi-Fi signals in the 2.4 GHz ISM band. Wi-Vi limits itself to a 20 MHz-wide Wi-Fi channel, and avoids ultra-wideband solutions used today to address the flash effect. It also dispenses of the multi-GHz bandwidth, typical in past systems, and instead uses a smaller 3-antenna MIMO.

So, how does Wi-Vi eliminate the flash effect without using GHz of bandwidth? We observe that we can adapt recent advances in MIMO communications to through-wall imaging. In MIMO, multiple antennas are used to send multiple signals to the same receiver. If the signal is nulled (i.e., sums up to zero) at a particular receive antenna, MIMO uses this capability to eliminate interference to unwanted receivers. In contrast, we use nulling to eliminate reflections from static objects, including the wall. Specifically, a Wi-Vi receiver starts with two antennas and a ground plane. Wi-Vi operates in two stages. In the first stage, it measures the channels from each of its two transmit antennas to its receive antenna. In stage 2, the two transmit antennas use the channel measurements from stage 1 to null the signal at the receive antenna. Since wireless signals (including reflections) combine linearly over the medium, only reflect-

Permissions to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyright for components of this work owned by others than the author(s) must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers, to e-mail to lists, or to redistribute to lists, requires prior specific permission and/or a fee. Request permission from permissions@acm.org.

©2012 ACM 0001-0782/12/0101-0001-11 \$15.00

# CONTEXT

data without  
context

arXiv:1803.09010v8 [cs.DB] 1 Dec 2021



The image shows a computer screen with a white background. At the top right, there is a small window titled "1803.09010.pdf (page 1 of 18)". Below this, the main content area has a dark header bar with the title "Datasheets for Datasets". The header also includes the names of the authors: TIMNIT GEBRU, Black in AI; JAMIE MORGENSTERN, University of Washington; BRIANA VECCHIONE, Cornell University; JENNIFER WORTMAN VAUGHAN, Microsoft Research; HANNA WALLACH, Microsoft Research; HAL DAUMÉ III, Microsoft Research; University of Maryland; and KATE CRAWFORD, Microsoft Research. The main body of the text starts with a section titled "1 Introduction". The text discusses the critical role of machine learning models in society and the potential for them to reflect unwanted societal biases. It mentions examples from criminal justice, hiring, and infrastructure. The text concludes by suggesting that entities should document the provenance, creation, and use of machine learning datasets to avoid discriminatory outcomes.

**Datasheets for Datasets**

TIMNIT GEBRU, Black in AI  
JAMIE MORGENSTERN, University of Washington  
BRIANA VECCHIONE, Cornell University  
JENNIFER WORTMAN VAUGHAN, Microsoft Research  
HANNA WALLACH, Microsoft Research  
HAL DAUMÉ III, Microsoft Research; University of Maryland  
KATE CRAWFORD, Microsoft Research

**1 Introduction**

Data plays a critical role in machine learning. Every machine learning model is trained and evaluated using data, quite often in the form of static datasets. The characteristics of these datasets fundamentally influence a model’s behavior: a model is unlikely to perform well in the wild if its deployment context does not match its training or evaluation datasets, or if these datasets reflect unwanted societal biases. Mismatches like this can have especially severe consequences when machine learning models are used in high-stakes domains, such as criminal justice [1, 13, 24], hiring [19], critical infrastructure [11, 21], and finance [18]. Even in other domains, mismatches may lead to loss of revenue or public relations setbacks. Of particular concern are recent examples showing that machine learning models can reproduce or amplify unwanted societal biases reflected in training datasets [4, 5, 12]. For these and other reasons, the World Economic Forum suggests that all entities should document the provenance, creation, and use of machine learning datasets in order to avoid discriminatory outcomes [25].

Although data provenance has been studied extensively in the databases community [3, 8], it is rarely discussed in the machine learning community. Documenting the creation and use of datasets has received even less attention. Despite the importance of data to machine learning, there is currently no standardized process for documenting machine learning datasets.

To address this gap, we propose *datasheets for datasets*. In the electronics industry, every component, no matter how simple or complex, is accompanied with a datasheet describing its operating characteristics, test results, recommended usage, and other information. By analogy, we propose that every

# CONTEXT

data without  
context

The screenshot shows a Mac OS X desktop with a window titled "GROUP\_0001\_design\_fiction\_Footer.pdf [page 1 of 151]". The main content of the window is a research paper. At the top right of the paper is the number "249". The title of the paper is "Ethical Considerations for Research Involving (Speculative) Public Data" by CASEY FIESLER, University of Colorado Boulder, USA. The abstract discusses the increasing prevalence of researchers having access to rich data about human behavior and how design fiction can frame current inquiry and debate into the ethics of using public data for research. Below the abstract, under "CCS Concepts", is a note about security and privacy. Under "Additional Key Words and Phrases", it lists design fiction; ethics; lifelogging; privacy; public data; social computing; research ethics; research methods; quantified self. Under "ACM Reference Format", it provides the citation: Casey Fiesler. 2019. Ethical Considerations for Research Involving (Speculative) Public Data. *Proc. ACM Hum.-Comput. Interact.* 3, GROUP, Article 249 (December 2019), 13 pages. <https://doi.org/10.1145/3370271>. A section titled "1 Author's Introductory Notes" begins with a paragraph about high-profile cases like the Facebook emotional contagion study and challenges to traditional notions of research ethics. The text continues to discuss the scope and scale of publicly available data and its potential for harm, referencing work in the HCI research community. It concludes by encouraging technologists to consider the possible negative consequences of their work through speculative designs.

Ethical Considerations for Research Involving (Speculative) Public Data

CASEY FIESLER, University of Colorado Boulder, USA

As the process of creating and sharing data about ourselves becomes more prevalent, researchers have access to increasingly rich data about human behavior. Framed as a fictional paper published at some point in the not-so-distant future, this design fiction draws from current inquiry and debate into the ethics of using public data for research, and speculatively extends this conversation into even more robust and more personal data that could exist when we design new technologies in the future. By looking to how the precedents of today might impact the practices of tomorrow, we can consider how we might design policies, ethical guidelines, and technologies that are forward-thinking.

CCS Concepts • **Security and privacy** → Social aspects of security and privacy;

Additional Key Words and Phrases: design fiction; ethics; lifelogging; privacy; public data; social computing; research ethics; research methods; quantified self

ACM Reference Format:

Casey Fiesler. 2019. Ethical Considerations for Research Involving (Speculative) Public Data. *Proc. ACM Hum.-Comput. Interact.* 3, GROUP, Article 249 (December 2019), 13 pages. <https://doi.org/10.1145/3370271>

**1 Author's Introductory Notes**

High profile cases in recent years such as the Facebook emotional contagion study [33], university researchers collecting facial recognition data from students without consent [31], and photos mined from dating sites used to train algorithms to predict sexual orientation [52] have challenged traditional notions of research ethics, particularly within the computing research community. Research ethics in terms of both regulation and training has focused largely on human subjects research, where harm is conceptualized via direct interaction with research participants [61]. However, the type of research now possible due to the scope and scale of publicly available data not only falls outside of these traditional regulatory schemes [71], but harms are often more indirect and less foreseeable. Within the human-computer interaction (HCI) research community, there have been calls to more carefully consider the possible negative consequences of our work [35], though this type of speculation about future harms can be challenging.

One possible avenue for addressing this challenge is through design fiction, which has been used to explore the potential outcomes of new design work, including the creation of fictional stories or papers that provide a space for critique [9]. Design fiction methods can encourage anticipation of and reflection about the potential downsides of technology design, research, and implementation [64]; indeed, reflection about speculative designs has been successful in encouraging technologists to consider how their practices might play out in the future [77]. Drawing from these ideas, the fictional paper that follows tackles the issue of research ethics and possible harms by exploring a

Author's address: Casey Fiesler, University of Colorado Boulder, Department of Information Science, Boulder, CO, 80309,

LEGAL ≠ ETHICAL

**LEGAL ≠ ETHICAL**

**...but...**

LEGAL  $\neq$  ETHICAL

...but...

law **can be** informative

LOTS OF GREAT REFLECTIONS

REPUGNANCE

REPUGNANCE  
POTENTIAL FOR  
HARM

REPUGNANCE  
POTENTIAL FOR  
HARM  
MISLEADING

REPUGNANCE  
POTENTIAL FOR  
HARM  
**MISLEADING**

REPUGNANCE  
POTENTIAL FOR  
HARM  
**MISLEADING**  
FALSE  
PRETENSES

REPUGNANCE  
POTENTIAL FOR  
HARM

EXPLOITATION

**MISLEADING**  
FALSE  
PRETENSES

REPUGNANCE  
POTENTIAL FOR  
HARM  
**MISLEADING**  
FALSE  
PRETENSES

EXPLOITATION  
FIRING  
PERSONNEL

REPUGNANCE  
POTENTIAL FOR  
HARM  
**MISLEADING**  
FALSE  
PRETENSES

EXPLOITATION  
FIRING  
PERSONNEL  
CYA

REPUGNANCE  
POTENTIAL FOR  
HARM  
**MISLEADING**  
FALSE  
PRETENSES

EXPLOITATION  
FIRING  
PERSONNEL  
CYA  
SPEED OF TECH

REPUGNANCE  
POTENTIAL FOR  
HARM  
**MISLEADING**  
FALSE  
PRETENSES

EXPLOITATION  
FIRING  
PERSONNEL  
CYA  
SPEED OF TECH

INTENT VS  
OUTCOME

REPUGNANCE  
POTENTIAL FOR  
HARM  
**MISLEADING**  
FALSE  
PRETENSES

EXPLOITATION  
FIRING  
PERSONNEL  
CYA  
SPEED OF TECH

INTENT VS  
OUTCOME  
INCENTIVES

REPUGNANCE  
POTENTIAL FOR  
HARM  
**MISLEADING**  
FALSE  
PRETENSES

EXPLOITATION  
FIRING  
PERSONNEL  
CYA  
SPEED OF TECH

INTENT VS  
OUTCOME  
INCENTIVES  
VULNERABILITY

REPUGNANCE  
POTENTIAL FOR  
HARM  
**MISLEADING**  
FALSE  
PRETENSES

EXPLOITATION  
FIRING  
PERSONNEL  
CYA  
SPEED OF TECH

INTENT VS  
OUTCOME  
INCENTIVES  
**VULNERABILITY**

REPUGNANCE  
POTENTIAL FOR  
HARM  
**MISLEADING**  
FALSE  
PRETENSES

EXPLOITATION  
FIRING  
PERSONNEL  
CYA  
SPEED OF TECH

INTENT VS  
OUTCOME  
INCENTIVES  
**VULNERABILITY**  
MISUSE

REPUGNANCE		INTENT VS
POTENTIAL FOR	EXPLOITATION	OUTCOME
HARM	FIRING	INCENTIVES
<b>MISLEADING</b>	PERSONNEL	<b>VULNERABILITY</b>
FALSE	CYA	MISUSE
PRETENSES	SPEED OF TECH	APPARENT PLAN (OR LACK OF?)

REPUGNANCE		INTENT VS
POTENTIAL FOR	EXPLOITATION	OUTCOME
HARM	FIRING	INCENTIVES
<b>MISLEADING</b>	PERSONNEL	<b>VULNERABILITY</b>
FALSE	CYA	MISUSE
PRETENSES	SPEED OF TECH	APPARENT PLAN (OR LACK OF?)

“SHOULDN’T REGULATORS HAVE GOTTEN INVOLVED?”

REPUGNANCE		INTENT VS
POTENTIAL FOR	EXPLOITATION	OUTCOME
HARM	FIRING	INCENTIVES
<b>MISLEADING</b>	PERSONNEL	<b>VULNERABILITY</b>
FALSE	CYA	MISUSE
PRETENSES	SPEED OF TECH	APPARENT PLAN (OR LACK OF?)

“SHOULDN’T REGULATORS HAVE GOTTEN INVOLVED?”

“...THE LAWS WE HAVE TODAY ARE FROM TO 1970’S?”

**THE ISSUES YOU ENCOUNTER  
WILL BE REAL**

# PHILOSOPHICAL FRAMEWORKS

CONSEQUENTIALISM

DEONTOLOGY

VIRTUE ETHICS

# PHILOSOPHICAL FRAMEWORKS

CONSEQUENTIALISM

EVALUATE BY OUTCOMES

DEONTOLOGY

VIRTUE ETHICS

# PHILOSOPHICAL FRAMEWORKS

CONSEQUENTIALISM

EVALUATE BY OUTCOMES

DEONTOLOGY

ASPIRE TO RULES

VIRTUE ETHICS

# PHILOSOPHICAL FRAMEWORKS

CONSEQUENTIALISM

EVALUATE BY OUTCOMES

DEONTOLOGY

ASPIRE TO RULES

VIRTUE ETHICS

ASPIRE TO VIRTUES

# PHILOSOPHICAL FRAMEWORKS

CONSEQUENTIALISM

EVALUATE BY OUTCOMES

DEONTOLOGY

ASPIRE TO RULES

VIRTUE ETHICS

ASPIRE TO VIRTUES

HOW DO THESE PHILOSOPHIES INFORM...

CTL? RING? GAYDAR? GOOGLE?

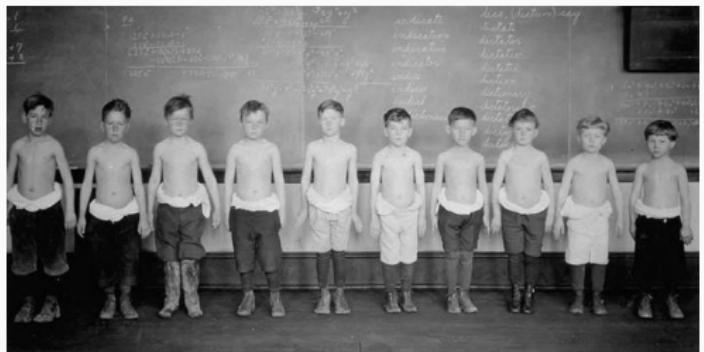
# HISTORICAL CONTEXTUALIZATION

Henrietta Lacks



# HISTORICAL CONTEXTUALIZATION

Quaker Oats



# HISTORICAL CONTEXTUALIZATION

Tuskegee  
experiments



# HISTORICAL CONTEXTUALIZATION

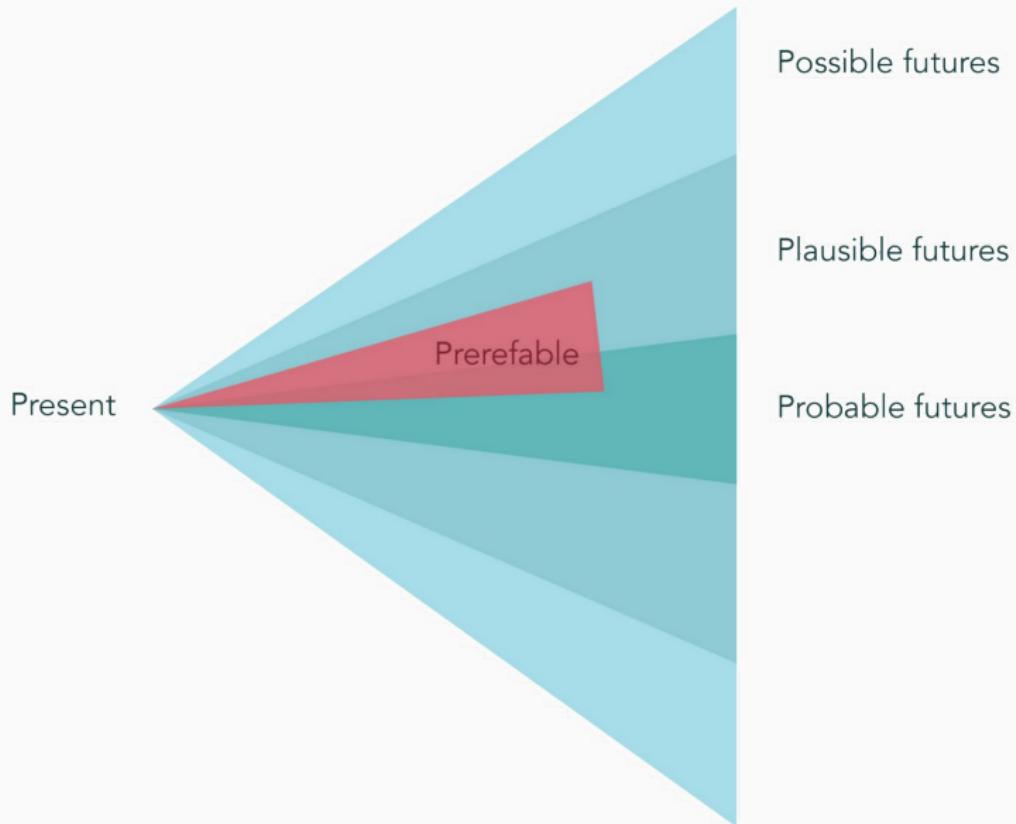
HUMAN DIGNITY AND AUTONOMY

# HISTORICAL CONTEXTUALIZATION

HUMAN DIGNITY AND AUTONOMY

INFORMED CONSENT

# SPECULATIVE DESIGN



# **SOME “PROVOCATIONS”**

a quick caveat about “provocations”

# SOME “PROVOCATIONS”

What are the risks of allowing the private sector to gather so much sensitive data?

Does anyone else feel uncomfortable about statements about suicide prevention efforts using phrases like “piloting a tailored solution” and “evaluating data trends”?

When do we know that an issue having to do with privacy and surveillance has been adequately addressed?

At what point do the negatives of a technology that gathers data outweigh the positives? or vice versa?

# PROMISES

---

# PROMISES OF DATA SCIENCE

- AI will **understand** the world better than humans can
- AI can make **more objective** or **fairer** decisions than people can