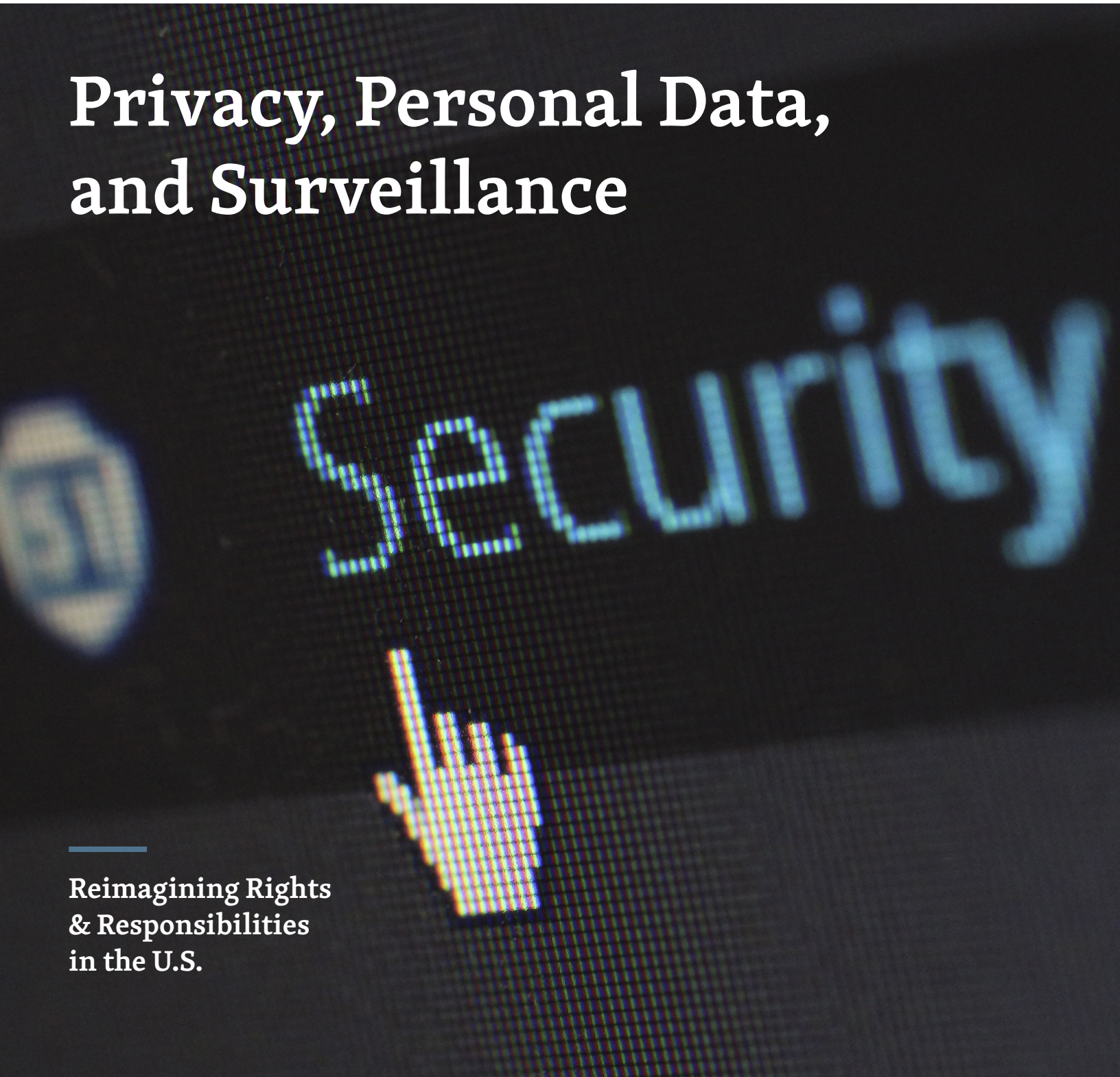
Reimagining Rights and Responsibilities in the United States: Privacy, Personal Data, and Surveillance

HARVARD Kennedy School
CARR CENTER
for Human Rights Policy

SPRING 2021
ISSUE 016

CARR CENTER FOR HUMAN RIGHTS POLICY
HARVARD KENNEDY SCHOOL

Privacy, Personal Data, and Surveillance



Reimagining Rights & Responsibilities in the U.S.

Reimagining Rights & Responsibilities in the United States: Privacy, Personal Data, and Surveillance

Carr Center for Human Rights Policy
Harvard Kennedy School, Harvard University
February 26, 2021

John Shattuck

Carr Center Senior Fellow; Former US Assistant Secretary of State for Democracy, Human Rights, and Labor; Professor of Practice, Fletcher School, Tufts University

Mathias Risse

Lucius N. Littauer Professor of Philosophy and Public Administration; Director for the Carr Center for Human Rights Policy

The authors' institutional affiliations are provided for purposes of author identification, not as indications of institutional endorsement of the report. This report is part of a Carr Center project on Reimagining Rights and Responsibilities in the United States, directed by John Shattuck. The project has been overseen by a faculty committee chaired by Mathias Risse, with the collaboration of Executive Director Sushma Raman, and the support of the Carr Center staff. This research paper was drafted by Toby Voght (RA). The authors are grateful to Michael Blanding and Philip Hamilton for editing, and Alexandra Geller for editorial and design.

Table of Contents

Introduction

Alyssa LeMay heard music.

The eight-year-old was playing in her home in Mississippi while her father worked in another room. She wondered if it was her sister singing the playful notes of "Tiptoe Through the Tulips" in their shared bedroom. It wasn't.

When Alyssa entered her bedroom, the music abruptly stopped, and an unrecognized voice began to speak. In a disturbing and surreal exchange, the voice began using racial epithets, then encouraging Alyssa to repeat them and challenging her to engage in destructive behavior such as breaking the television in her room. The bizarre event was even more disconcerting for Alyssa, due to intermittent pleas that the voice was her "best friend" or "Santa Claus." Confused and frightened, Alyssa left the room and reported the incident to her father.[1]

The LeMay family does not know the culprit of this gross invasion of their daughters' sanctum, but they know the vehicle by which the invasion occurred: two Ring cameras, supported by Amazon, which the family bought only weeks earlier. When Alyssa's mother reported the breach to Amazon, the company chided her decision not to use dual-factor identification to protect the security of the account as the cause, but provided no further information. In the months since the occurrence at the end of 2019, Amazon has still provided no further details related to the source of the breach, the duration of time during which the camera's feed may have been compromised, or the identity of the culprit.[2]

Meanwhile similar crimes were occurring elsewhere. *The Washington Post* identified four such incidents across the country over a single weekend in early December 2019, where internal security camera and smart speakers were hacked to harass or threaten the occupants of a home.[3]

These incursions represent a new threat to privacy in America. The last several decades have brought dramatic technological change to our society. This change has shifted conceptions of what a "right to privacy" entails and the government's role in protecting that right. The severity of privacy violations, and their often disturbing details, have created a rare area of common ground. A poll conducted by Morning Consult in December 2019 found 79% of Americans favor a new bill protecting online consumer data in 2020, and 65% of Americans identified data privacy as "one of the biggest issues our society faces."[4] An encouraging component of this consensus is its bi-partisan nature, with 83% of Democrats and 82% of Republicans favoring stronger data privacy protections.[5] Privacy and control of personal information is an issue that cuts across demographic groups and provides a unique opportunity for renewing rights and responsibilities.[6]

How did we get to this point? Historically, privacy rights in the US have been focused on protecting individuals from government overreach, but recent trends indicate modern protections must target both the public and private sectors.

An analysis of privacy in America must also acknowledge the enormous popularity and economic importance of the companies and organizations that enthusiastically collect personal data. The five most valuable companies in the world at the end of 2019 all either collect and monetize data as their central business model, or are significantly growing that portion of their business.[7] The economic infrastructure around these companies employs millions of Americans. Additionally, despite constant negative reporting, social media usage remains constant in the United States.[8] Google continues to hold a 92.5% market share of internet searches.[9] Government directories and public data sets, such as the Department of Justice's National Sex Offender Public Website, empower citizens to live and work safely in their communities. Americans clearly value these services and have integrated them into their lives.

1. A more complete account and a disturbing video of the interaction can be found here: Chiu, Allyson. "She Installed a Ring Camera in Her Children's Room for 'Peace of Mind.' A Hacker Accessed it and Harassed Her 8-Year-Old Daughter." *Washington Post*, 12 Dec. 2019, https://www.washingtonpost.com/nation/2019/12/12/she-installed-ring-camera-her-childrens-room-peace-mind-hacker-accessed-it-harassed-her-year-old-daughter/?arc404=true.

2. DeSantis, Rachel. "Families Are Suing Ring Over Hacked Home Security Cameras: 'It Was from a Horror Film.'" *Yahoo!*, 31 Jan. 2020, https://www.yahoo.com/entertainment/families-suing-ring-over-hacked-195243756.html.

3. Chiu, Allyson. "She Installed a Ring Camera in Her Children's Room for 'Peace of Mind.' A Hacker Accessed it and Harassed Her 8-Year-Old Daughter." *Washington Post*, 12 Dec. 2019, https://www.washingtonpost.com/nation/2019/12/12/she-installed-ring-camera-her-childrens-room-peace-mind-hacker-accessed-it-harassed-her-year-old-daughter/?arc404=true.

4. Sabin, Sam. "Most Voters Say Congress Should Make Privacy Legislation a Priority Next Year." *Morning Consult*, 18 Dec. 2019, https://morningconsult.com/2019/12/18/most-voters-say-congress-should-make-privacy-legislation-a-priority-next-year/.

5. Ibid.

6. Ibid.

7. These companies are Apple ($1.3 trillion), Microsoft ($1.2 trillion), Alphabet ($0.9 trillion), Amazon ($0.9 trillion), and Facebook ($0.6 trillion).

8. "The Infinite Dial 2019." *Edison Research*, 6 Mar. 2019, https://www.edisonresearch.com/infinite-dial-2019/.

9. "Search Engine Market Share Worldwide, Dec 2019 - Dec 2020." *Statcounter,* https://gs.statcounter.com/search-engine-market-share. Accessed 11 Jan. 2021.

Constitutional protections bar law enforcement agencies from directly violating a person's privacy by searching their personal property without judicial authorization. Judicial precedent has established that the government must not violate a person's "reasonable expectation of privacy." The collection and sale of personal data in the private sector, however, is almost completely unregulated. There is very little national legislative protection of personal data, and most of it predates the digital era: The Fair Credit Reporting Act of 1970, The Privacy Act of 1974, The Health Insurance Portability and Accountability Act of 1996 (HIPAA), The Children's Online Privacy Protection Act of 1998, and the Financial Services Modernization Act of 1999 (also known as the Gramm-Leach-Bliley Act). Ambitious corporations have seized on technological advances and the absence of regulation to collect, utilize, and sell personal data in ways that would have been unimaginable when most of our current privacy protections were enacted into law.

The little privacy regulation that exists is inconsistent and decentralized. The Federal Trade Commission (FTC) is broadly considered to be the principal regulator of the collection, sale, and storage of personal data by companies. Despite the explosive growth in the personal data business sector, only 5% of FTC employees support the agency's mission of "Privacy and Identity Protection."[10] Over 15 other federal agencies are responsible for enforcing regulations on personal data, often in unclear or contradictory contexts. Three states have passed comprehensive privacy laws of their own and 13 states currently have similar bills in committee in their state legislatures.[11] The variance of state legislation further complicates the ability to effectively regulate the personal data market in either the private or public sectors. The rapid arrival of technological ubiquity and a lack of effective regulation have created a privacy crisis.

Crafting and implementing privacy protections presents many challenges. Those seeking to avoid a repeat of the LeMays' nightmarish scenario face opposition from two powerful fronts. Data gained from customer surveillance is valuable for improving business operations and resale to other parties, so companies have a strong incentive to protect their practices. It is in the interest of technology companies such as Amazon, Facebook, and Google to limit government regulation and conceal the extent to which their security measures have been circumvented or defeated. The enormous amount of capital possessed by personal data companies and their singular focus on reducing individual privacy and autonomy have enabled them to prevail repeatedly in courthouses and legislatures. In the few instances in which these companies have not succeeded, they have still won de facto victories against regulation by mounting lengthy and expensive appeals processes and obstruction.

Government, on the other hand, is beholden to law enforcement agencies who see an opportunity to reduce crime through constant, invasive surveillance in collaboration with private companies. The government of Washington, DC provides an example of this through a "private security camera system incentive program" with its Office of Victim Services and Justice Grants. The program offers rebates of up to $500 for families who install security camera systems around their homes and give local police archival access to recordings.[12]

While big business and the government have perverse incentives to increase the amount of data collected on citizens in the United States, Americans are increasingly falling prey to a voyeuristic impulse to spy on and evaluate neighbors. A survey of over 50 Ring customers by *The Washington Post* found that most enjoyed the use of their cameras for non-criminal behavior as well as security protection. Respondents described spying on domestic workers and nannies, often without their knowledge, with one commenting "I know maybe I should tell them but [then] they won't be as candid."[13]

This voyeuristic urge is combining with innovations in social media to create toxic environments. Ring's Neighbors app is a sharing space where Ring users can post videos captured at their home. The videos sometimes capture criminal behavior, such as package theft and hit and runs. Often they capture innocuous or annoying behavior and provide an immediate outlet for public shaming. More sinister concerns are related to the unvetted ability to label an individual "suspicious." An investigative report published in *Boston Magazine* found that "people who are poor, non-white, or both are often unfairly labeled by Ring users as 'dangerous.'"[14]

One of the worst examples of this combination of social media impulses and the unregulated flow of personal data can be found on the mugshot posting website florida.arrests.org. The website posts the full legal name and mugshots of arrested individuals within minutes of processing and encourages users to label them with tags such as "Hotties," "Transgender," "Grills," "Celebrity," "Handicap," and "WTF."[15]

10. *Fiscal Year 2021 Congressional Budget Justification*. Federal Trade Commission, 10 Feb. 2020, https://www.ftc.gov/system/files/documents/reports/fy-2021-congressional-budget-justification/fy_2021_cbj_final.pdf.

11. Noordyke, Mitchell. "US State Comprehensive Privacy Law Comparison." *International Association of Privacy Professionals*, 6 July 2020, https://iapp.org/resources/article/state-comparison-table/.

12. "Private Security Camera Rebate Program FAQs." *Office of Victim Services and Justice Grants*, https://ovsjg.dc.gov/page/private-security-camera-rebate-program-faqs. Accessed 11 Jan. 2021.

13. Quoted from the comments section of Chiu, Allyson. "She Installed a Ring Camera in Her Children's Room for 'Peace of Mind.' A Hacker Accessed it and Harassed Her 8-Year-Old Daughter." *Washington Post*, 12 Dec. 2019, https://www.washingtonpost.com/nation/2019/12/12/she-installed-ring-camera-her-childrens-room-peace-mind-hacker-accessed-it-harassed-her-year-old-daughter/?arc404=true.

14. Buell, Spencer. "Ring's Neighborhood Watch Feature Is Bringing Out the Worst in Boston." *Boston Magazine*, 27 Jan. 2020, https://www.bostonmagazine.com/news/2020/01/27/ring-cameras-neighbors-app/.

15. "Most Recent Florida Bookings." *Florida Arrests*, https://florida.arrests.org/. Accessed 11 Jan. 2021.

Privacy has always been one of the most precarious rights of American life because it lacks clear protections in the U.S.

The lack of oversight within private industry practices has led more tightly regulated government agencies to outsource to, or collaborate with, private companies that can execute surveillance without legal objection. The National Security Agency and other intelligence agencies now utilize close connections with technology companies to access information and surveil individuals at a level and scale that would have been impossible only a few years ago. Immigration and law enforcement agencies increasingly use social media and internet data mining to gather information about individuals which is fed to complex algorithms for threat assessments. The leaks of Edward Snowden revealed some of these practices and recent concerns regarding the oversight of FISA courts has brought attention to the conduct of these agencies, but meaningful regulation or oversight is still lacking. The current administration's reduction of privacy protections for non-citizens has accelerated this erosion of rights.[16]

The emergence of the COVID-19 pandemic in 2020 has emboldened both private and public entities to increase efforts to collect private personal information. The new environment requires balancing public health priorities with human rights concerns. The track record of technology companies and the federal government with regard to data collection is a critical component of this consideration. As data has become digitized, both have rushed to gather personal data with little oversight for programs that are later revealed as ineffective.[17, 18] Policymakers must have access to the expertise that can provide a more robust evaluation of the benefits and costs of data collection. Additionally, the continued authorization of the USA FREEDOM Act (an update to the USA PATRIOT Act passed in response to the 9/11 attacks) reveal the reticence of private industry, intelligence, and law enforcement to end data collection, accumulation, and analysis long after it is a public safety or public health concern.

Perhaps most importantly, personal data has emerged as the central deterministic feature of life in the 21st century. Credit scores determine peoples' ability to purchase a home or car. Social media algorithms create the connections that establish the growing hierarchy of social "influencers." In the post-pandemic economy employment may be dictated by medical history, behavior in personal time off, and even genetic predispositions. As data has become our destiny, individuals have ever decreasing control over its flow in favor of secretive companies and government organizations. This is reflected in polling conducted by Pew Research. Four in five Americans feel that they have no control over the data corporations and the government collect about them.[19] The same percentage feel that the risks outweigh the benefits of that collection for companies and three in five share that sentiment for government collection.[20]

Privacy has always been one of the most precarious rights of American life because it lacks clear protections in the U.S. Constitution. The right to privacy is under attack in this moment in our history like no other previous moment. Privacy defenders are attempting to fight a two-front war, as increasing incursions are made by private industry and government law enforcement.

The Emergence of the Personal Data Economy

An increasing variety of companies are collecting, selling, or analyzing data as a critical component of their business model. Vermont and California, the only states to regulate these data brokers, define them as companies that buy and sell the personal data of individuals or groups of individuals without any direct relationship with the consumers whose data they sell for profit. Both Vermont and California have created public listings in which companies that fall into these categories must register.

The definition of data brokers provided by these two states focuses on an important component of the modern data economy—the lack of awareness of individuals that their personal data is being collected, stored, and sold. The European General Data Protection Regulation addresses this issue by mandating an agreement of consent from data subjects, but still leaves unaddressed the concern of awareness. We provide three categories of personal data that capture the concepts of consent and awareness: Discrete data, behavioral data, and indefinite data. We will use these terms for the remainder of this paper and encourage their use for industry clarity.

Discrete data is data that is directly solicited from consumers by companies with whom the customer has an ongoing relationship. Phone number requests at a retail store counter or online fill-in-the-blank forms are examples of this form of data. So are social

16. United States, Executive Office of the President [Donald J. Trump]. Executive Order: Enhancing Public Safety in the Interior of the United States. 25 Jan. 2017. *The White House*, https://www.whitehouse.gov/presidential-actions/executive-order-enhancing-public-safety-interior-united-states/.

17. Nakashima, Ellen. "NSA Has Halted a Counterterrorism Program Relying on Phone Records Amid Doubts About its Utility." *Washington Post*, 5 Mar. 2019, https://www.washingtonpost.com/world/national-security/nsa-has-halted-a-counterterrorism-program-relying-on-phone-records-amid-doubts-about-its-utility/2019/03/05/f2d2793e-3f80-11e9-922c-64d6b7840b82_story.html.

18. Warzel, Charlie. "All this Dystopia, and for What?" *New York Times*, 18 Feb. 2020, https://www.nytimes.com/2020/02/18/opinion/facial-recognition-surveillance-privacy.html.

19. Auxier, Brooke, et al. "Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over their Personal Information." *Pew Research Center*, 15 Nov. 2019, https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/.

20. Ibid.

media posts and other user created content that is directly and intentionally shared for publication. The definition of "ongoing relationship" is important and worthy of further discussion. For clarity purposes, we define "ongoing relationship" as direct contact between consumer and company within a year. This classification of data is the most straightforward. Consumers generally understand what data they are sharing, who they are sharing it with and the purpose for which it is being shared.

Behavioral data is gathered by acts that would traditionally be characterized as surveillance. The customer is not consciously aware of data transmission in this instance, even having previously acknowledged a privacy policy. The tracking cookies deployed by companies such as Facebook and Google are examples of this behavioral data surveillance, as are recordings of smart speakers, security cameras, and cell phone location tracking data. Behavioral data is also increasingly being collected in physical retail environments. Companies such as SAS are utilizing facial recognition and other technologies to track purchases, movements, and even moods of shoppers within client stores.[21]

The collection of behavioral data has fundamentally different implications than discrete collection. The information that is subject to collection by behavioral observation has potential uses that are still unclear even to experts in the computer science and data analysis fields, and the inferences behavioral observation can allow companies to form are even more ambiguous. Companies frequently engage in behavioral collection under concealed or false pretenses. For the purposes of our definition, behavioral collection only occurs when the customer and collecting company have an ongoing relationship.

The final category of personal information is **indefinite data**. Indefinite data refers to data collected outside an ongoing relationship with the customer. Companies would qualify for this category of data collection if they have not had direct contact with relevant consumers within a year or if they have never had direct contact with a consumer at all. Examples of this range from retailers that collect individuals' phone numbers and e-mail addresses to genome mapping companies like 23andMe or Ancestry.com, when the companies retain that data for longer than one year. Data brokers fall within this category.

Credit agencies were some of the first companies to adopt the indefinite data business model and it has grown rapidly in recent years. Equifax was founded in the 19th century, and the late 1960's brought the significant growth of a credit data collection model when firms such as TransUnion and Experian were founded. Federal regulation followed shortly after, with the Fair Credit Reporting Act of 1970 (itself an amendment to the Consumer Credit Protection Act of 1968).

Over the years, the purposes of indefinite data collection have been expanded and justified by technological advances and changing business models. In a 2014 report on the data broker industry, the Federal Trade Commission outlined six primary functions of data brokerage companies that deal in individuals' information, none of which was the original purpose of credit evaluation.[22]

Classes of Data Collected in the Data Economy			
	Discrete Data	Behavioral Data	Indefinite Data
Direct Relationship with customer	Yes	Yes	Not within a year
Customer has clear understanding of information collected	Yes	No	Maybe
Customer has clear understanding of purpose and future use of collected information	Yes	No	No
Governed by privacy policy	Yes	Maybe	Yes

21. "New Technology Allows Retailers to Track Customers' Every Move." *Today*, 21 Feb. 2020, https://www.today.com/video/new-technology-allows-retailers-to-track-customers-every-move-79151685521.

22. The categories are direct marketing, online marketing, marketing analytics, identity verification, fraud detection, and people search. *Data Brokers: A Call for Transparency and Accountability*. Federal Trade Commission, May 2014, https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf.

The practices of companies are in direct opposition to public opinion about what is "reasonable" data retention. Polling by Pew revealed that over 50% of Americans believe it is not reasonable for most organizations to keep records of their activity for over one year.[23] The only organizations excepted from that expectation were government agencies and credit card companies.[24] In practice, nearly every consumer-facing company now retains customer data for as long as possible.

An important part of understanding the nature of indefinite data is understanding the importance of user awareness in consent. The distinction between discrete data and behavioral data highlights the lack of awareness of data subjects (and resulting lack of consent) at the moment of collection. Indefinite data highlights the lack of awareness and consent of data subjects through the process of retention.

COLLECTION, BUYING, AND SELLING OF BEHAVIORAL DATA

The principal class of behavioral data is metadata, defined by the National Information Standards Organization as "structured information that describes, explains, locates, or otherwise makes it easier to retrieve, use, or manage an information resource."[25] To date, the collection and sale of metadata is largely regulation free.

For example, investigative journalists have found that it is surprisingly easy to purchase both the real-time and historic location of consumer cell phones, information that is supposed to be available only to law enforcement agencies in criminal investigations.[26] In December 2019, *The New York Times*' Privacy Project acquired a dataset containing the locations of over 12 million phones from a private data brokerage company.[27] It took the reporters only minutes to re-identify the supposedly anonymous data, using algorithms, and to specifically identify senior officials, such as President Trump and children. Telecom companies have pledged to tighten restrictions governing access to phone location data, but no regulatory enforcement compels compliance and the companies have not revealed the frequency or scale at which consumer location data is openly purchasable.[28]

One of the reasons that metadata has thus far eluded regulation is that the harm caused by its collection and dissemination is not always plainly clear. For example, when the computerized vacuum company iRobot began compiling the metadata records of its robots in customer homes, it seemed to be a harmless dataset that could help to enhance their business operations. The use of algorithms and large datasets allowed iRobot to turn that information into a collection of blueprints of customers' homes. The company's CEO has stated iRobot's intent to sell these diagrams to technology companies such as Google and Facebook without additional customer consent.[29][30] Metadata and behavioral data can provide companies information that individual consumers cannot imagine or expect, and over which they have no control.

Another reason metadata collection and sale are difficult to regulate is that they are anonymized or de-identified. These terms are ill-defined, however, and create a lack of understanding among consumers. The term anonymization suggests that data is either anonymous or not. In practice, statisticians and technologists have found that anonymity is a spectrum instead of a binary distinction. Data is often re-identified in unexpected ways. For example, a hypothetical local pharmacy collects data about customers and sorts it by the number of times they visit a store location within a month. Such "anonymous" data could be paired with facial recognition data, already provided by companies such as SAS, to identify an individual person or small group of persons who visited the store ten times in one month. This example only uses two datasets, but increasingly companies and organizations have many data sets with which re-identification is a relatively simple task.

Harvard computer science professor LaTanya Swinney drove this point home in 1997 when she re-identified Massachusetts Governor Bill Weld's personal health information using an "anonymized" open data set she purchased for $20 with only his residential zip code and his birth date. In a dramatic flourish, Swinney mailed then-Governor Weld's personal health records, including diagnoses and prescriptions, to his office. Algorithmic

23. Madden Mary, and Lee Rainie. "Americans' Views About Data Collection and Security." *Pew Research Center*, 20 May 2015, https://www.pewresearch.org/internet/2015/05/20/americans-views-about-data-collection-and-security/.

24. Ibid.

25. *Understanding Metadata*, National Information Standards Organization Press, 2004, https://www.niso.org/publications/understanding-metadata-2017.

26. Whittaker, Zach. "Despite Promises to Stop, US Cell Carriers Are Still Selling Your Real-Time Phone Location Data." *Techcrunch*, 9 Jan. 2019, https://techcrunch.com/2019/01/09/us-cell-carriers-still-selling-your-location-data/.

27. Thompson, Stuart A., and Charlie Warzel. "Twelve Million Phones, One Dataset, Zero Privacy." *New York Times*, 19 Dec. 2019, https://www.nytimes.com/interactive/2019/12/19/opinion/location-tracking-cell-phone.html.

28. Bode, Karl. "In Letters to Senate, Wireless Carriers Downplay their Latest Location Data Scandal." *Vice*, 18 Apr. 2019, https://www.vice.com/en_us/article/43jdqn/in-letters-to-senate-wireless-carriers-downplay-their-latest-location-data-scandal.

29. Reuters has run a correction that implies CEO Colin Angle was misquoted and the company intends to "share maps for free with customer consent" instead of "sell maps." The business benefit of this strategy is not clear and Reuters reports in a separate article both that iRobot stock surged as a result of this reporting and that the company could reach a deal to "sell its maps in the next couple of years" elsewhere. Zuboff also writes about this incident (pg. 235-36). Wolfe, Jan. "Roomba Vacuum Maker iRobot Betting Big on the 'Smart' Home." *Reuters*, 24 July 2017, https://www.reuters.com/article/us-irobot-strategy-idUSKBN1A91A5.

30. Wen, Melissa. "iRobot Shares Surge on Strong Sales of Roomba Vacuum Cleaners." *Reuters*, 26 July 2017, https://www.reuters.com/article/us-irobot-stocks-idUSKBN1AB2QW.

and computational power have dramatically improved during the interceding two decades. Companies' claims on anonymized data should be judged with the sharpest scrutiny and the burden of proof should require them to support such claims as valid.[31]

REDUCED DATA AUTONOMY

Dr. Janese Trimaldi thought she had put her past behind her. In July 2011, she was the victim of a domestic violence incident.[32] When the police responded, she was booked after her then boyfriend asserted that she had struck him with a knife.[33] Dr. Trimaldi maintains that the cut on her boyfriend was the result of an accidental scratch by fingernail.[34] The state attorney decided to drop any potential charges against her.[35] Months later her mugshot appeared on a Florida-based mugshot aggregator along with the dropped charges and another booking photograph from fifteen years prior.[36]

Dr. Trimaldi has never been convicted of a crime, yet she was still faced with the prospect of paying a $30 fee to have the two photographs removed from the website in question.[37] Shortly after her payment the images appeared on other sites, one of which demanded a $400 fee to remove them.[38]

Unlike many of the other stories of technology and privacy in this paper, there have been positive developments related to the dissemination of mugshots in the past decade. After *The New York Times* completed an investigative report that detailed Dr. Trimaldi's and several others' experiences being extorted by online mugshot aggregators, search engines such as Google worked to adjust their algorithm so that archived mugshots would be moved back in search results over time, and both MasterCard and PayPal refuse to process payments to such sites.[39] Additionally, a number of newsrooms underwent a re-evaluation of the use of mugshots in news coverage and by early 2020 decided to reduce usage to only truly newsworthy offenses.[40]

The unrestricted capability of data brokers to collect, aggregate, and transmit indefinite personal information without accountability to the subject makes independent consumer awareness and action nearly impossible.

Trimaldi's story is nevertheless representative of many online experiences. Data brokerage sites still sell or publish personal information, such as birthdays, e-mail addresses, and physical addresses, while charging a premium for removal. The number of such sites and the unregulated nature of their business makes it prohibitively expensive at best, or an impossible task at worst, for a person to control the personal information published about them. Additionally, mugshot aggregation sites still populate the internet, making money from advertisements–frequently for criminal background data brokerage companies–instead of pure extortion.

The unrestricted capability of data brokers to collect, aggregate, and transmit indefinite personal information without accountability to the subject makes independent consumer awareness and action nearly impossible. Prior to Vermont's recent establishment of a data broker registry, there had been no previous attempt to begin mapping the data broker industry. The 240 companies that have registered as of early 2020 are a small sampling of a rapidly growing industry about which consumers are unaware and disempowered. The Federal Trade Commission raises the concern of personal search data brokers leaving "domestic violence victims, law enforcement officers, prosecutors or public officials" vulnerable to harassment, stalking, retaliation, or other harm.[41] Further, these brokers often charge fees to correct or "de-list" information that individuals find compromising, embarrassing, or private.

Domestic violence victims are sometimes the targets of personal tracking devices. A survey conducted by the National Network to End Domestic Violence (NNEDV) at the Conference on Crimes

31. Sweeney, Latanya. "Privacy Technologies for Homeland Security." Privacy and Integrity Advisory Committee, Department of Homeland Security, 15 June 2005. Testimony. https://www.dhs.gov/xlibrary/assets/privacy/privacy_advcom_06-2005_testimony_sweeney.pdf.

32. Segal, David. "Mugged by a Mug Shot Online." *New York Times*, 5 Oct. 2013, https://www.nytimes.com/2013/10/06/business/mugged-by-a-mug-shot-online.html.

33. Ibid.

34. Ibid.

35. Ibid.

36. Ibid.

37. Ibid.

38. Ibid.

39. Ibid.

40. Garcia-Navarro, Lulu. "Some Newsrooms Are Rethinking their Approach to Publishing Mugshots." *Weekend Edition Sunday* on NPR, 16 Feb. 2020, https://www.npr.org/2020/02/16/806417359/some-newsrooms-are-rethinking-their-approach-to-publishing-mugshots.

41. *Data Brokers: A Call for Transparency and Accountability*. Federal Trade Commission, May 2014, https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf.

Against Women found that 13% of those surveyed had worked with a victim of "GPS tracking on a phone or other device."[42] Ten percent reported "abusers using online data to track or locate a victim" as a technology misuse with which they had first-hand experience.[43] A previous survey by NNEDV found that 36% of surveyed domestic violence victim service providers had encountered at least one incidence of offenders monitoring victims' activity by "gathering online data about the victim."[44]

DATA BREACHES

Data brokers and other organizations that collect and analyze personal data are often subject to data breaches. The scale of these breaches, and the secretive nature of the organizations who fall victim to them, make tracking and understanding data breaches difficult. The cybersecurity analysis firm Risk Based Security identified over 5,000 data breaches in the first nine months of 2019, six of which each compromised over 100 million records or more.[45] The most frequently breached sectors were medical services, retail, and public entities.[46] In 2019, data breaches increased by 33% over 2018, while the number of exposed records more than doubled from the previous year.[47]

The digitization of personal data has made protection from data breaches increasingly challenging. In 2012, over three and a half million tax records were stolen from the State of South Carolina by cyber-criminals.[48] Before the digital age, such a crime would have been unthinkable. The sheer amount of effort and resources required to replicate then move millions of paper pages is enormous, and the ability to do so without raising security notice is impracticable. The 2012 crime was committed remotely over a period of several days of downloading and was not recognized for weeks after the event.[49] Modern regulators must protect citizens not only from digital data collection, but also later compromise of collected personal information.

Major data breaches such as the 2017 Equifax breach of over 100 million personal records often make headlines, but consumers are left confused and disempowered. During Equifax's attempt to reach potential victims, official Equifax websites and social media profiles unknowingly directed victims to fake websites set up by hackers attempting to gather even more personal information.[50] Americans feel understandably helpless before the enormous scale of these breaches, the opaqueness of the organizations hoarding personal data and the lack of government enforced accountability for these organizations.

The 2012 compromise of over three and a half million tax records by the South Carolina government is an example of the lack of cybersecurity accountability for organizations that maintain large databases of personal information. Hackers executed an attack that relied on a multi-step plan, which could have been disrupted by several broad security policy changes, but the response focused on quick, simple, and incomplete solutions. Although simple solutions are sometimes effective in the short-term, they are easily circumvented by future attackers. Josephine Wolff, a professor of cybersecurity policy at the Fletcher School at Tufts University, explains that companies often do not address large systemic risks so that they can avoid liability. As a result, the opportunity to learn from and develop new best practices from prior data breaches is often missed.[51]

Public concern is also minimized by a belief that data breaches are accidental or are not caused by individuals or state actors with an interest in causing harm to those whose data is compromised. Verizon's 2020 Data Breach Investigations Report tells a different story. The company's analysis found that over 55% of analyzed breaches were conducted by organized crime, with financial attacks being the leading motive.[52] The ability to rapidly scale an attack against all exposed victims can often mean that even individuals with lower net worth can be targeted.

42. *Tech Abuse: Information from the Field*. National Network to End Domestic Violence, 14 Sept. 2018, https://www.techsafety.org/blog/2018/9/12/tech-abuse-information-from-the-field.

43. Ibid.

44. *A Glimpse from the Field: How Abusers Are Misusing Technology*. National Network to End Domestic Violence, 17 Feb. 2015, https://www.techsafety.org/blog/2015/2/17/a-glimpse-from-the-field-how-abusers-are-misusing-technology.

45. *Data Breach Quick View Report: 2019 Q3 Trends*, Risk Based Security. Nov. 2019, https://pages.riskbasedsecurity.com/hubfs/Reports/2019/Data%20Breach%20QuickView%20Report%202019%20Q3%20Trends.pdf.

46. Ibid.

47. Ibid.

48. Acohido, Byron. "SC Data Breach Just Latest in Hacker Onslaught." *USA Today*, 26 Oct. 2012, https://www.usatoday.com/story/tech/2012/10/26/south-carolina-data-breach-36-million-ssns-stolen/1661541/.

49. Ibid.

50. Astor, Maggie. "Someone Made a Fake Equifax Site. Then Equifax Linked to it." *New York Times*, 20 Sept. 2017, https://www.nytimes.com/2017/09/20/business/equifax-fake-website.html.

51. Wolff writes extensively about liability processes that myopically focused on a single, easily circumvented vulnerability or holding a single party responsible when the acts of several contributed to the breach.

52. Verizon *2020 Data Breach Investigations Report*. Verizon, 2020, https://enterprise.verizon.com/resources/reports/dbir/.

The Cybersecurity Information Sharing Act of 2015 is the first and only regulation so far that is designed to encourage sharing of best practices in data management and cybersecurity.[53] The bill provides companies legal protections for establishing cyber defenses and sharing cyber threat indicators with federal, state, and local governments.[54] This provision may provide better information sharing and promulgation of best practices, but it also indemnifies companies from liability for negligent cyber defense of personal data.

The slow evolution of cybersecurity insurance is an indication of the challenge of assessing damages of data breaches and holding negligent parties accountable. Technologist Ran Levi has identified the difficulties of establishing a cyber data insurance market, including the lack of sufficient historical precedent to estimate the range of costs of claims, wide variance in the monetary damage of attacks, and the lack of clear market value for damage assessments.[55] Congress has held hearings on the subject of cyber insurance markets but has not taken action.[56]

Ultimately, the problem of data breaches and the resulting damage to the privacy of citizens will not be solved until the injury from these breaches becomes a liability for those directly involved in establishing and executing security practices.

The business model of collecting and monetizing consumer data puts the interests of data brokers at odds with consumers. Personal data is unlike any other previous business asset because incentives are not just misaligned, they are directly opposed. When customers have previously trusted companies with items of personal value, the value is tied to some physical or irreplaceable trait. For instance, when a customer makes a deposit at a bank the bank has an incentive to protect it. That deposit is critical for the bank to invest and become profitable. When a company collects personal data, however, it can utilize the data to be profitable even if it is stolen. Most data breaches result in the criminals duplicating and downloading the data instead of destroying it. As a result, the only loss a company with bad security practices suffers is a very slight reduction in the value of data due to duplication costs. The consumer is faced with all the negative privacy externalities.

Perhaps there is no greater evidence of the lack of financial consequence for companies that suffer data breaches than the succession of events following the Equifax breach in 2017. Over the course of the cyber attack, hackers stole personal information from over 145 million Americans. The records contained a combination of credit card numbers, driver's license numbers, social security numbers, dates of birth, phone numbers, and email addresses at a minimum. A 2018 report by the Government Accountability Office found that the compromise occurred because of a host of poor cybersecurity practices.[57] Equifax utilized a server with out-of-date software, did not monitor its network-data inspection system, and stored the data in an unencrypted form.[58] Despite this undisputed negligent behavior, the FTC imposed no penalties against the company and Equifax stock had appreciated by nearly 10% in early 2020. The company's CEO at the time of the breach was permitted to resign and retained bonuses worth more than $90 million.

THE DATA ECONOMY BUSINESS MODEL

The advent of large, scalable data technologies has made it possible for companies to collect personal and behavioral data of people across the globe. A growing consensus is emerging that the economics of the data economy are fundamentally broken. Some of the most biting criticism of these business models come from experts in computer science and business. Speaking at the annual Design Innovate Communicate Entertain conference in 2020, the CEO of Epic Games, one of the leading video game publishers, described the current technological environment as "a massive scale devolvement of industries that are based on adversarial business models, businesses that profit from doing customers harm and doing their supporting ecosystems harm. Facebook and Google have been leaders in this trend. They give you a service for free, and they make you pay for it in the form of currency that's dearer than money . . . loss of privacy and loss of freedom."[59] Amnesty International reports that Facebook and Google's "surveillance-based business model forces people to make a Faustian bargain, whereby they are only able to enjoy their human rights online by submitting to a system predicated on human rights abuse."[60] In *The Age of Surveillance Capitalism*, Harvard Business School Professor Shoshana Zuboff compares

53. United States, Congress, Senate. The Cybersecurity Information Sharing Act of 2015. *Congress.gov,* https://www.congress.gov/bill/114th-congress/senate-bill/754/text#toc-idc6842ed051194cfda77e2d250867c1f7. 114th Congress, 1st Session, Senate Resolution 754, passed 27 Oct. 2015.

54. Ibid., section 106.

55."What's the Problem with Cyber Insurance?" *Malicious Life Podcast* from Cybereason, https://malicious.life/episode/episode-64/. Accessed 11 Jan. 2021.

56. United States, Congress, House, Committee on Homeland Security. *The Role of Cyber Insurance in Risk Management*. US Government Publishing Office, 22 Mar. 2016, https://www.govinfo.gov/content/pkg/CHRG-114hhrg22625/html/CHRG-114hhrg22625.htm. Text transcription of hearing.

57. *Actions Taken by Equifax and Federal Agencies in Response to the 2017 Breach*. Government Accountability Office, 30 Aug. 2018, https://www.gao.gov/products/GAO-18-559.

58. Fleishman, Glenn. "Equifax Data Breach, One Year Later: Obvious Errors and No Real Changes, New Report Says." *Fortune*, 7 Sept. 2018, https://fortune.com/2018/09/07/equifax-data-breach-one-year-anniversary/.

59. Park, Gene. "Facebook, Google 'Profit from Doing Customers Harm,' Says Epic Games CEO Tim Sweeney." *Wahsington Post*, 12 Feb. 2020, https://www.washingtonpost.com/video-games/2020/02/12/facebook-google-profit-doing-customers-harm-says-epic-games-ceo-tim-sweeney/.

60. *Surveillance Giants: How the Business Model of Google and Facebook Threatens Human Rights*. Amnesty International, 21 Nov. 2019, https://www.amnesty.org/download/Documents/POL3014042019ENGLISH.PDF.

claims made by companies engaged in the personal data market to early conquistadors, who would read proclamations to indigenous populations in a language they did not understand prior to claiming their lands.[61] The modern conquerors are the companies who present consumers with legalese and technical terminology while usurping their basic rights to personal information.

Consumer product companies are increasingly adding personal data collection and sale to their business model and monetizing customer data. Examples abound, from the 20% projected growth in Visa's sale of consumer data to banks in 2020[62] to iRobot using their robot vacuums to map customers' living spaces for sale to third parties.[63] The underlying business principles of this trend are straightforward. These companies possess troves of consumer data that they have acquired at little or no cost and can reproduce for unlimited resale.

The California Consumer Privacy Act and Vermont Act 171 mentioned above begin to address unaccountable monetization of personal data. Both narrowly define data brokers as companies who buy and sell individual's personal data without a direct business relationship with the individual whose information is sold. While these regulations are an important first step towards making companies disclose their personal data collection, their narrow definition misses the more troubling aspect of the growing personal data marketplace. Additionally, though the CCPA went into effect in January 2020, the Attorney General of California will not begin to enforce its provisions until July 1, 2020 at the earliest. Predicting what such a piece of legislation will look like in practice is fraught. As noted earlier, many companies with direct customer relationships also collect personal data without complete customer awareness.

A right to privacy requires informed consent from an individual, including regarding the content of collected information and its future use. Data brokers act without any consumer awareness, and commercial companies who surreptitiously collect personal information for future profit are similarly taking advantage of consumer ignorance.

Regulators have viewed data companies as equivalent to old consumer-driven business models, where businesses compete on the basis of customer satisfaction and future repeat sales. However, companies monetizing data have an entirely different competition and incentive structure. An ideal company in a consumer-facing economy focuses on delivering the highest consumer satisfaction at the lowest price. An ideal company in the data economy harvests as much personal data as possible, while offering the fewest services with the lowest consumer awareness possible. Data companies have no business incentive, absent regulatory restrictions, to limit the collection of personal data or to invest in the protection of personal consumer data they have collected.

The security outcome of this misalignment is that consequences of breaches fall not on organizations in a position to prevent breaches but on the victims whose information is collected and compromised. This creates further incentive to focus on simple solutions instead of holistic ones. A simple solution allows the company to move on without solving the underlying security shortcoming or expending the capital that such remedies would require. A lack of overriding federal policy and a patchwork of state regulations and restrictions are a major factor encouraging companies not to act. As Zuboff concludes, "this new market form declares that serving the genuine needs of people is less lucrative, and therefore less important, than selling predictions of their behavior."[64]

Data brokers have capitalized on the rapid pace of technological change. From tracking the real-time movements of a user's cellphone to scraping up arrest records across the country, these companies are collecting personal data on an unprecedented scale and often making it available to the highest bidder without the data subjects' awareness or knowledge.

The resulting data-collection environment denies consumers any true choice to protect their data. For example, the response of several companies to the registration inquiries of the Vermont Secretary of State indicated that there was no process in place for Americans to opt out of the collection, storage, and sale of their information. Even when the opportunity to control a person's data is provided, the process is long and unnecessarily arduous. The same Vermont registry has opt-out policies that require phone calls, e-mails, or online forms to be filled out. Virtually all of the nearly 250 companies responded negatively to Vermont's query of "whether the data broker permits a consumer to authorize a third party to perform the opt-out on the consumer's behalf."[65] This puts an onus on the consumer to first identify which companies have opt-out policies and then invest the time to contact each individually, by their directed means. None of this provides any guarantee that even if an individual were to successfully opt out of the registered companies, that new companies would not arise with new opt out procedures.

Government Surveillance

Traditionally the purview of government entities, surveillance has a long history as a contentious issue in the United States. The Fourth Amendment and federal and state legislation provide some limits on law enforcement's ability to target individuals

61. Zuboff, Shoshana. *The Age of Surveillance Capitalism*. 1st ed., PublicAffairs, 2019.

62. Visa projects revenue of $3.5 billion from such sales, which represents 14% of their total revenue in that period. "Visa Sees Data Sales Driving $3.5 Billion in Consulting Revenue." *Bloomberg News*, 11 Feb. 2020, https://www.paymentssource.com/articles/visa-sees-data-sales-driving-3-5-billion-in-consulting-revenue.

63. Wen, Melissa. "iRobot Shares Surge on Strong Sales of Roomba Vacuum Cleaners." *Reuters*, 26 July 2017, https://www.reuters.com/article/us-irobot-stocks-idUSKBN1AB2QW.

64. Zuboff, Shoshana. *The Age of Surveillance Capitalism*. 1st ed., PublicAffairs, 2019.

65. 9 V.S.A. § 2446. *Vermont State Legislature*, https://legislature.vermont.gov/statutes/section/09/062/02446. Accessed 11 Jan. 2021.

for electronic surveillance. Despite those protections, people in the U.S. are subject to increasing technological surveillance by government agencies and their private contractors.

Three judicial decisions over the last half century are central to surveillance law and technology in the United States: *Katz v. The United States*, *Smith v. Maryland*, and *United States v. Graham*. These cases specify Fourth Amendment protections which require law enforcement to obtain a search warrant in order to collect data through electronic surveillance.

- *Katz* was a 1967 case in which law enforcement investigators placed a physical device on a public phone used by a suspect to record conversations. The evidence was ruled to be inadmissible due to a lack of search warrant and a violation of the search and seizure protections of the Fourth Amendment.[66] This decision outlines the constitutional restrictions on government surveillance, limiting the use of a physical object to surveil a citizen and establishing the judicial standard of a "reasonable expectation of privacy."[67,68]

- *Smith* was a 1979 case in which law enforcement installed a "pen register" at a telephone company without a search warrant in order to log the phone numbers dialed by a suspect. The Supreme Court ruled that there was no reasonable expectation of privacy because the "petitioner voluntarily conveyed numerical information to the telephone company."[69] This decision hinged on the lack of a "reasonable expectation of privacy" within the petitioner's home due to transmittal of information that was voluntarily disclosed to the phone company.[70]

- *Graham*, a 2016 case, upheld the right of law enforcement to access metadata without a search warrant. A U.S. District Court in Maryland held that electronic metadata (in this instance, historical location data) was not protected by the Fourth Amendment if it was collected and retained by a third party.[71,72]

The Privacy Act of 1974 set the standard for federal government collection, maintenance, and transmittal of personal data. It regulates "Personally Identifiable Information" (PII) within federal "agencies."[73] It is generally not applicable to law enforcement and intelligence agency surveillance due to its focus on the transmission and storage, not collection or acquisition, of PII. Military intelligence, civilian intelligence, and law enforcement agencies are regulated only by small divisions internal to their organization. The Civil Liberties and Privacy Office of the Office of the Director of National Intelligence is an example of such oversight. The Implementing Recommendations of the 9/11 Commission Act of 2007 also created the stand-alone executive Privacy and Civil Liberties Oversight Board to provide oversight and advice for the "implementation of Executive Branch policies, procedures, regulations, and information-sharing practices relating to efforts to protect the nation from terrorism."[74] During the 13 years of its existence, the board has had a quorum for six years and has been fully staffed for only four. Its few actions and positions have been inconsequential and either ignored or disputed by the relevant agencies.

Technology has created new methods for private and public entities to observe and record personal activity, and granted more legal ambiguity for law enforcement to circumvent civil liberties protections. This situation became more prevalent following the terrorist attacks of September 11th, 2001. Many analysts, including Zuboff, conclude that, in the wake of the attacks, the public and political demand for security through certainty outweighed considerations of personal privacy and led to the practice of mass data collection.[75] Former Clinton Administration Chief Counselor for Privacy Peter Swire observed that the 1990's "brought a flurry of privacy protections across the world," but after the attacks of September 11th, 2001, "legislation and attention to privacy issues cooled as security took center stage."[76]

66. LaFave, Wayne R. *Search & Seizure: A Treatise on the Fourth Amendment*. 2nd ed., West Publishing Company, 1987.

67. This physical standard was recently upheld by the *United States v. Jones* decision, which eliminated evidence collected by placing a physical GPS tracker on a suspect's car. Medinger, Jason. "Post-*Jones*: How District Courts Are Answering the Myriad Questions Raised by the Supreme Court's Decision in *United States v. Jones*." *University of Baltimore Law Review*, vol. 42, no. 3, 2013.

68. The "reasonable expectation of privacy" legal standard is credited to US Supreme Court Justice John Marshall Harlan in his concurring opinion.

69. United States, Supreme Court. *Smith v. Maryland*. 20 June 1979. *Justicia*, https://supreme.justia.com/cases/federal/us/442/735/.

70. Rapisarda, Mark. "Privacy, Technology, and Surveillance: NSA Bulk Collection and the End of the *Smith v. Maryland* Era." *Gonzaga Law Review*, vol. 51, no. 1, 2015, pp. 121–583.

71. Derman, Jeremy. "Constitutional Law - Maryland District Court Finds Government's Acquisition of Historical Cell Site Data Immune from Fourth Amendment - *United States v. Graham*." *Suffolk University Law Review*, vol. 46, no. 1, 2013.

72. "*United States v. Graham*: Fourth Circuit Holds that Government Acquisition of Historical Cell-Site Location Information Is not a Search." *Harvard Law Review*, Vol. 130, no. 4, Feb. 2017, https://harvardlawreview.org/2017/02/united-states-v-graham/.

73. United States Code. 5 USC §552a – Records Maintained on Individuals. *Legal Information Institute*, Cornell Law School, https://www.law.cornell.edu/uscode/text/5/552a. Accessed 12 Jan. 2021.

74. "About." *US Privacy and Civil Liberties Oversight Board*, https://www.pclob.gov/about/. Accessed 12 Jan. 2021.

75. Zuboff, Shoshana. *The Age of Surveillance Capitalism*. 1st ed., PublicAffairs, 2019. pp. 113-114

76. Swire, Peter. "The Second Wave of Global Privacy Protection: Symposium Introduction." *Ohio State Law Journal*, vol. 74, no. 6, 2013, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2404261.

THIRD-PARTY CONTRACTORS

Intelligence and law enforcement agencies are increasingly relying on private sector third-party contractors as a means of circumventing regulation intended to control or limit government surveillance. "Third-party doctrine," established in cases such as *Smith v. Maryland*, maintains that law enforcement agencies may access collected data about a suspect's activity from private third-party entities without a warrant.[77]

One of the most famous facilitators of this practice is Palantir, a data-analysis company founded by Peter Thiel. Palantir has been credited as a critical member of the team that identified the location of Osama Bin Laden, along with the CIA, in 2012.[78] The CIA was an original seed funder of the company and Palantir has recently expanded to serve local law enforcement as well. As a result of Palantir's involvement, domestic law enforcement entities bear an increasing resemblance to intelligence agencies that are permitted to operate with few restrictions in international operations. Palantir software runs in many of the "fusion centers" furnished by the Department of Homeland security, and owned and operated by state and local law enforcement to conduct data analysis and collection.[79,80] In marketing materials, Palantir describes its software, which runs in these centers,[81] as integrating data points from "suspicious activity reports, Automated License Plate Reader (ALPR) data, and unstructured data such as document repositories and emails."[82] Regulatory compliance is based on "need to know" controls, without resolving whether collection on this scale by a company acting as a surveillance arm for law enforcement is legal or desired by the American public.[83]

In 2004, Congress denied an appeal from the National Security Agency to implement a global artificial intelligence system called "Total Information Awareness" (TIA). The basis for this denial was the need to comply with the Foreign Intelligence Surveillance Act (FISA), which establishes a judicial warrant requirement for initiating domestic surveillance. An investigative report in 2006 by the MIT Technology Review found that while TIA did not exist in name, the NSA had circumvented the congressional denial by executing a system of surveillance very similar to TIA's initial intent through partnerships with telecoms such as AT&T and other technology companies.[84]

Local law enforcement agencies in municipalities across the country have begun to utilize software, like that offered by Palantir, to be more predictive in crime prevention. Legal challenges have alleged that these algorithms can be racially biased, but in the absence of regulation many uses of these sorts of programs may be going unrecognized.[85] The use of artificial intelligence and algorithms increase the likelihood of malfeasance. Because the logic used by these programs and systems is usually unclear, it remains a distinct possibility that that they identify groups that are protected classes through a combination of unprotected variables, opening the potential for racial, gender, religious, or other illegal discrimination on that basis. Though algorithms prevent an understanding of the exact decision-making process, it is not hard to understand how easily accessible third-party data can lead to identification of protected information. For example, using a dataset of cell phone tracking information, religious affiliation can be inferred by weekly church, synagogue, or mosque attendance.

Arrangements with third-party companies came under scrutiny during the Trump Administration's proposal for a Muslim registry.[86] The capacity to conduct demographic inference, such as indirectly identifying the religion of an individual, is a selling point for the marketing power of these companies.[87] Over the past decade, a number of algorithms have claimed a capability

77. "*United States v. Graham*: Fourth Circuit Holds that Government Acquisition of Historical Cell-Site Location Information Is not a Search." *Harvard Law Review*, Vol. 130, no. 4, Feb. 2017, https://harvardlawreview.org/2017/02/united-states-v-graham/.

78. Greenberg, Andy. "How a 'Deviant' Philosopher Built Palantir, a CIA-Funded Data-Mining Juggernaut." *Forbes*, 14 Aug. 2013, https://www.forbes.com/sites/andygreenberg/2013/08/14/agent-of-intelligence-how-a-deviant-philosopher-built-palantir-a-cia-funded-data-mining-juggernaut/#521abbbd7785.

79. "Surveillance Tech in San Diego County, California." *Electronic Frontier Foundation*, https://www.eff.org/aos-san-diego-county-california. Last updated 17 Dec. 2019.

80. "Fusion Centers." *US Department of Homeland Security*, 19 Sept. 2019, https://www.dhs.gov/fusion-centers.

81. Haskins, Caroline. "Revealed: This Is Palantir's Top Secret User Manual for Cops." *Motherboard*, Vice, 12 July 2019, https://www.vice.com/en/article/9kx4z8/revealed-this-is-palantirs-top-secret-user-manual-for-cops.

82. "Law Enforcement." *Palantir*, https://www.palantir.com/solutions/law-enforcement/. Accessed 28 Jan. 2021.

83. "Palantir Gotham." *Palantir*, https://www.palantir.com/palantir-gotham/. Accessed 12 Jan. 2021.

84. Pontin, Mark Williams. "The Total Information Awareness Project Lives On." *MIT Technology Review*, 26 Apr., 2006, https://www.technologyreview.com/s/405707/the-total-information-awareness-project-lives-on/.

85. Collins, Dave. "Should Police Use Computers to Predict Crimes and Criminals?" *Associated Press*, 5 July 2018, https://apnews.com/article/14bb35110b644edc8798365ade767bd2.

86. Feldman, Brian. "Can the Government Get its Hands on Silicon Valley's Big Data?" *Intelligencer*, New York Magazine, 21 Dec. 2016, http://nymag.com/intelligencer/2016/12/can-the-government-get-its-hands-on-silicon-valleys-data.html.

87. *Data Brokers: A Call for Transparency and Accountability*. Federal Trade Commission, May 2014, https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf.

to determine the sexual orientation of users through content on Facebook.[88,89] The potential for a Muslim registry is one of many potentially dangerous ways the power of this technology could be utilized.

The increasing prevalence of cameras and microphones connected to private databases has brought into question whether past privacy defenses still hold. For example, *United States v. Jones* upheld a standard preventing law enforcement from placing physical transmitters without a warrant, but there is no legal precedent regarding sensors set up by private entities or consumers (e.g. artificial intelligence instruments like 'Alexa,' smart speakers, video doorbells, etc.). A murder case in Bentonville, Arkansas, is a bellwether of the sort of legal challenges that our judicial system will be tasked with answering soon, absent legislative guidance. Investigators discovered an Amazon Echo Dot (a smart home speaker) at the home of a murder suspect and subpoenaed voice recordings of the device from Amazon. If the smart speaker had been placed by law enforcement, any evidence from it would have been inadmissible. However, because the smart speaker was willingly placed by the suspect himself in his home, and Amazon retained sound recordings of the apartment, this case fell outside of the guidance provided by *Katz*. Ultimately, no legal precedent was established because the suspect consented to the search.[90]

PERSONAL DATA-MINING, SOCIAL MEDIA, AND ARTIFICIAL INTELLIGENCE

Facial recognition and biometric information databases are increasingly being compiled by law enforcement organizations. The Georgetown Law Center Privacy Project describes the concerns these programs present:

> "We know very little about these systems. We don't know how they impact privacy and civil liberties. We don't know how they address accuracy problems. And we don't know how any of these systems—local, state, or federal—affect racial and ethnic minorities."

Twenty states now provide access to drivers' license photos and mugshots to the FBI and/or local law enforcement for algorithmic search.[91] While police routinely share mugshots for staged lineups, the inclusion of facial data of regular law-abiding residents for algorithmic searches is a recent development.

Delegating decision making in the public sector to data sets or data driven processes introduces the opportunity for bias. In 2017, Immigration and Customs Enforcement (ICE) undertook an "Extreme Vetting Initiative." The program was to fund the internal creation of an artificial intelligence system capable of reviewing individuals' data scraped from the internet and provided by existing third-party contracts with data aggregators.[92] After public disclosure and outcry, the agency ultimately decided cost and privacy considerations made the project prohibitive. Instead, ICE outsourced the project to a private-sector third-party contractor to conduct similar behavioral vetting.[93] Meanwhile, Customs and Border Protection regularly reviews and mines the social media feeds and other internet activity of legal visitors within the country. Visa applications routinely request the social media handles of applicants. The Electronic Frontier Foundation has done extensive reporting on the close relationships that federal agencies enjoy with social media and other digital data companies.[94]

Digital data brokering practices can exacerbate discriminatory impacts on racial minorities. The National Fair Housing Alliance conducted a study using data from 2007 demonstrating that the data points for calculating personal credit scores created racially discriminatory outcomes.[95] A report by Pro Publica in 2016 revealed a private-sector developed algorithm used by some state law enforcement agencies in making bail or sentencing recommendations substantially overestimated the recidivism risk of African-American defendants.[96] These overestimates were based on police interactions (more common in communities of color), instead of criminal convictions, to predict the probability of future offenses.

88. Locke, Susanna F. "Gaydar Algorithm Outs Facebook Users." *Popular Science*, 21 Sept. 2019, https://www.popsci.com/scitech/article/2009-09/gaydar-algorithm-outs-facebook-users/.

89. Heaney, Katie. "Facebook Knew I Was Gay Before My Family Did." *Buzzfeed News*, 19 Mar. 2013, https://www.buzzfeednews.com/article/katieheaney/facebook-knew-i-was-gay-before-my-family-did.

90. Shackleton, Julia R. "Alexa, Amazon Assistant or Government Informant?" *University of Miami Business Law Review*, vol. 27, no. 2, 2019, https://repository.law.miami.edu/cgi/viewcontent.cgi?article=1345&context=umblr.

91. Only the state of Arizona has affirmatively denied the use of facial recognition in their law enforcement departments, after ending the practice in 2013.

92. Funk, McKenzie. "How ICE Picks its Targets in the Surveillance Age." *New York Times*, 2 Oct. 2019, https://www.nytimes.com/2019/10/02/magazine/ice-surveillance-deportation.html.

93. Harwell, Drew, and Nick Miroff. " ICE Just Abandoned its Dream of 'Extreme Vetting' Software that Could Predict Whether a Foreign Visitor Would Become a Terrorist." *Washington Post*, 17 May 2018, https://www.washingtonpost.com/news/the-switch/wp/2018/05/17/ice-just-abandoned-its-dream-of-extreme-vetting-software-that-could-predict-whether-a-foreign-visitor-would-become-a-terrorist/.

94. "NSA Spying." *Electronic Frontier Foundation*, https://www.eff.org/nsa-spying. Accessed 12 Jan. 2021.

95. Rice, Lisa, and Deidre Swesnik. "Discriminatory Effects of Credit Scoring on Communities of Color." *Suffolk University Law Review*, vol. 46, no. 3, 2013.

96. Angwin, Julia, et al. "Machine Bias." *Pro Publica*, 23 May 2016, https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing.

President Trump's 2017 Executive Order on "Enhancing Public Safety in the Interior of the United States" directed federal agencies to apply the protections of the Privacy Act only to U.S. citizens or legal residents.[97] The executive order has created uncertainty about the E.U.-U.S. Privacy Shield data agreement between the European Union and the United States, which allows American companies and European companies to transmit personal data across the Atlantic by voluntarily submitting to oversight. Additional concerns include whether the new order violates the privacy rights of undocumented residents.[98]

Machine learning and algorithmic decision-making in the public sector can become an existential threat to the rule of law in a democracy. The U.S. legal system is built around standards that allow an understanding of the judgment process, whether through argumentation or written opinions. This transparency is particularly important in the public sector.

PUBLIC HEALTH AND SAFETY VS. PRIVACY

The Coronavirus pandemic of 2020 has brought attention to what seems an inevitable tradeoff between public health and privacy. Chastened by the overreaches of the post-9/11 intelligence and technology sectors, the media and the general public have retained a surprising focus on maintaining and increasing privacy protections for individuals. The editorial boards of *The Washington Post* and *The New York Times* have published editorials demanding the preservation of personal privacy protections in measures to combat the virus through digital contact tracing.[99,100]

The public has been generally supportive of protective measures, but contact tracing and other provisions potentially constituting a violation of individual privacy have been a rare point of skepticism. A Washington Post/University of Maryland Poll found that 82% of Americans were supportive of current restrictions or supportive of greater restriction, but only 41% of Americans would be willing to use a smart-phone-based contract tracing app. The least trusted organizations for the handling of personal data were "tech companies like Apple and Google," followed by health insurance companies.[101] A similar Axios-Ipsos poll found that only half of Americans would participate in a "cell-phone-based contact tracing program."[102] That number decreased significantly if the program was overseen by any organization other than "the CDC and public health officials."[103]

The consistency of polling, despite the severity and acuity of the coronavirus pandemic, are the result of bad faith over personal data collection issues that has been fostered between government agencies, private corporations, and the general public over the past two decades.

Though more information will emerge over the coming months and years, early research indicates that public suspicions were warranted. North and South Dakota were some of the first state governments to develop cell-phone-based contact tracing apps. The app developer ProudCrowd offered to complete the development of the states' Care19 contact tracing app free of charge. After completion, the app was vetted by state officials and Apple, and included a privacy policy stating location data "will not be shared with anyone including government entities or third parties." An analysis by privacy company Jumbo, and follow-up reporting by *The Washington Post*, confirmed that some data from the app goes directly to the location-marketing company Foursquare. Apple's policy is to work with companies found to violate their privacy policies to get them in compliance, with no consideration for data that may already have been collected.[104] This failure highlights the dangers of rushing contact-tracing data products to market and the limits of privacy policies in the absence of regulation and penalties.

The civil rights of marginalized groups can also come under the greatest threat from contact tracing. South Korea traced an outbreak to a nightclub frequented by members of its LGBTQ+ community. The government's attempts to contact and isolate patrons of the bar risked outing a number of citizens in the socially conservative country. Between Friends, a Korean advocacy group for gay men, fielded more than 50 calls from gay men fearful they could be outed to their employers or families due to government

97. United States, Executive Office of the President [Donald J. Trump]. Executive Order: Enhancing Public Safety in the Interior of the United States. *The White House*, 25 Jan. 2017, www.whitehouse.gov/presidential-actions/executive-order-enhancing-public-safety-interior-united-states/.

98. Caporal, Jack. "Justice Department: Trump's Immigration Order Does Not Affect Privacy Shield." *Inside Cybersecurity*, 28 Feb. 2017, https://insidetrade.com/daily-news/justice-department-trumps-immigration-order-does-not-affect-privacy-shield.

99. Editorial Board. "Before We Use Digital Contact Tracing, We Must Weigh the Costs." *Washington Post*, 1 May 2020, https://www.washingtonpost.com/opinions/tech-firms-must-prove-that-digital-contact-tracing-is-worth-the-privacy-intrusion/2020/05/01/cbf19b8e-7dc7-11ea-9040-68981f488eed_story.html.

100. Editorial Board. "Privacy Cannot Be a Casualty of the Coronavirus." *New York Times*, 7 Apr. 2020, https://www.nytimes.com/2020/04/07/opinion/digital-privacy-coronavirus.html.

101. "Washington Post-University of Maryland National Poll, April 21-26, 2020." *Washington Post*, https://www.washingtonpost.com/context/washington-post-university-of-maryland-national-poll-april-21-26-2020/3583b4e9-66be-4ed6-a457-f6630a550ddf/?itid=lk_inline_manual_3. Updated 21 May 2020.

102. Talev, Margaret. "Axios-Ipsos Coronavirus Index Week 9: Americans Hate Contact Tracing." *Axios*, 12 May 2020, https://www.axios.com/axios-ipsos-coronavirus-week-9-contact-tracing-bd747eaa-8fa1-4822-89bc-4e214c44a44d.html.

103. Ibid.

104. Fowler, Geoffrey A. "One of the First Contact-Tracing Apps Violates its Own Privacy Policy." *Washington Post*, 21 May 2020, https://www.washingtonpost.com/technology/2020/05/21/care19-dakota-privacy-coronavirus/.

disclosures.[105] In the United States, the disproportionate concentration of coronavirus cases among racial and ethnic minority groups, and working class populations could cause contact-tracing programs to result in increased surveillance of groups who have strong historical reasons to distrust government surveillance. Human Rights Watch has expressed concern that "such tracking could open a dangerous new front in the surveillance and repression of marginalized groups."[106]

The potential privacy pitfalls of public health or public safety programs should not preclude their development or employment, but should result in a critical analysis by implementing policymakers. In the case of contact tracing apps, leading experts have raised questions about efficacy, privacy protections, and security, among other concerns.[107,108] These concerns, and further concerns about the duration and conclusion of programs, must be adequately addressed prior to the implementation of any such initiatives.

Weak Regulatory Environment

In 1973, Caspar W. Weinberger, then Secretary of Health, Education, and Welfare, transmitted a report titled "Records, Computers and the Rights of Citizens" to President Richard Nixon. The report detailed the growing threat of computerized record keeping within the government to the privacy of individuals. It outlined five principles as "safeguard requirements for automated personal data systems:"

- There must be no personal data record keeping system whose very existence is secret.
- There must be a way for an individual to find out what information about him is in a record and how it is used.
- There must be a way for an individual to prevent information about him that was obtained for one purpose from being used or made available for other purposes without his consent.
- There must be a way for an individual to correct or amend a record of identifiable information about him.
- Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take precautions to prevent misuse of the data.[109]

Twenty-five years later, in 1998, the Federal Trade Commission released its own Fair Information Practices as part of its "Privacy Online: A Report to Congress." That report similarly established five general principles:

- Notice/Awareness
- Choice/Consent
- Access/Participation
- Integrity/Security
- Enforcement/Redress[110]

Internationally, the Organization for Economic Cooperation and Development (OECD) promulgated similar guidelines in 1980.[111] The European Union also established a regulatory framework for Fair Information Practices in 1981.[112]

There is a clear line from the first discussion of Fair Information Practices in 1973 to the White House's 2012 report on "Consumer Data Privacy in a Networked World" and the FTC's 2012 report "Protecting Consumer Privacy in an Era of Rapid Change." The principal difference is that the initial establishment of Fair Information Practices in 1973 was followed by major legislative action, The Privacy Act of 1974. With both the Privacy Act and the Fair Credit Reporting Act, legislators identified the biggest threat to consumer privacy in the form of personal data–government agencies and consumer reporting agencies, respectively–and took measures to ensure Fair Information Practices were observed and enforced. The passage of time and the development of new technologies have not invalidated Fair Information Practices nor the rights they imply for individual citizens, but legislators have failed to maintain compliance pressure on relevant organizations as the primary threat has shifted from government to the private sector. Within the government, the structure of the Privacy Act of 1974 has grown outdated.

105. Yoon, Dasl, and Timothy W. Martin. "'What if My Family Found Out?': Korea's Coronavirus Tracking Unnerves Gay Community." *Wall Street Journal*, 12 May 2020, www.wsj.com/articles/south-koreas-coronavirus-efforts-spark-privacy-concerns-in-gay-community-11589306659?mod=hp_lead_pos10.

106. Toh, Amos, and Deborah Brown. "How Digital Contact Tracing for COVID-19 Could Worsen Inequality." *Human Rights Watch*, 4 June 2020, https://www.hrw.org/news/2020/06/05/how-digital-contact-tracing-covid-19-could-worsen-inequality.

107. Raskar, Ramesh, et al. "Apps Gone Rogue: Maintaining Personal Privacy in an Epidemic." *arXiv*, Cornell University, 19 Mar. 2020, https://arxiv.org/abs/2003.08567.

108. Editorial Board. "Show Evidence that Apps for COVID-19 Contact-Tracing Are Secure and Effective." *Nature*, 29 Apr. 2020, https://www.nature.com/articles/d41586-020-01264-1.

109. *Records, Computers, and the Rights of Citizens*. US Department of Health and Human Services, 1 July 1973, https://aspe.hhs.gov/report/records-computers-and-rights-citizens.

110. *Privacy Online: A Report to Congress.* Federal Trade Commission, June 1998, https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-report-congress/priv-23a.pdf.

111. "OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data." *Organization for Economic Co-operation and Development*, 2013, http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm.

112. "Data Protection." *Council of Europe*, https://www.coe.int/en/web/data-protection/background-modernisation. Accessed 12 Dec. 2021.

Beyond the early regulation provided by laws such as the Privacy Act and the Fair Credit Reporting Act, Congress has passed a patchwork of privacy protections for small groups. The Children's Online Privacy Protection Act protects only children under 13 years old. The Video Privacy Protection Act of 1988 protects "wrongful disclosure of video tape rentals" or similar audio-visual materials. The Health Insurance Portability and Accountability Act of 1996 protects only "protected health information" or individually identifiable health information. The Gramm-Leach-Bliley Act focuses exclusively on information directly tied to credit and financial information.[113]

Private companies have capitalized on the narrow definitions of protected data or individuals with well-financed legal challenges. In the absence of broad, value-based legislation, privacy rights are under serious threat.

Without federal action, states have been left to act. California has been one of the leading actors protecting individual privacy. These actions are supported by a state constitutional guarantee of privacy adopted by constitutional amendment in 1974. Additionally, the state legislature has acted to enshrine privacy protections for individuals through a steady stream of privacy regulation, most recently with the passage of the California Consumer Privacy Act. After passage, the act added a provision for a data broker registry, though it is still in the early stages of implementation.[114] Vermont Act 171 (Data Broker Regulation) was the first state-level legislation to explicitly target data brokers. It requires the registration of data brokers and establishes minimum security standards for such companies. [115] These laws have the possibility of becoming de facto national regulation, but the limited jurisdiction of state Attorneys General and the enormous funding of legal challenges by technology companies leaves their efficacy in question.

The few effective protections that have been passed are increasingly circumvented through loopholes, technological advances, and secrecy in the absence of government oversight. One such example is the recent movement by Google to gain access to health records. The company has struck multiple deals for information sharing of medical records under a provision within HIPAA that allows the data to be shared if it is used "only to help the covered entity carry out its health-care functions."[116] Broad and often outdated regulations are subject to legal wrangling and aggressive business practices. In the financial sector, companies are developing non-traditional data aggregations to determine credit scores to elude regulations within the FCRA.[117] Banks and financial technology companies are currently exploring the possibility of incorporating more personal data into credit scores and decisions. Experian, among others, is lobbying to allow this new approach to behavioral information collection.[118] In the absence of regulation, these practices have grown rapidly without consideration of their impact on privacy.[119]

PRIVACY POLICIES AND SELF-REGULATION

There are no federal requirements for online commercial entities to post or explain their privacy policies. At the state level, The California Online Privacy Protection Act of 2003 created a requirement for online companies to post privacy policies on the home page of their website and included several content requirements.[120] Due to the high cost for companies to identify California-based users prior to website interaction, the legislation became a de facto requirement for almost all American companies. Despite this legislation, a 2008 study by Carnegie Mellon professors Aleecia M. McDonald and Lorrie Faith Cranor found that a reasonable reading of all the privacy policies an individual encounters in a year would require 76 full workdays at a national opportunity cost of $781 billion.[121] The recently passed California

113. Hodges, Sarah. "Examining the Gramm-Leach-Bliley Act's Opt-Out Method for Protecting Consumer Data Privacy Rights on the Internet." *Information & Communications Technology Law*, vol. 22, no. 1, 2013, https://www.tandfonline.com/doi/abs/10.1080/13600834.2013.785177.

114. Kagan, Odia. "CCPA Amendment Adds Data Broker Registration." *Fox Rothschild*, 18 Sep. 2019, https://dataprivacy.foxrothschild.com/2019/09/articles/california-consumer-privacy-act/ccpa-amendment-adds-data-broker-registration/.

115. *Guidance on Vermont's Act 171 of 2018: Data Broker Regulation*. Vermont Office of the Attorney General, 11 Dec. 2018, https://ago.vermont.gov/wp-content/uploads/2018/12/2018-12-11-VT-Data-Broker-Regulation-Guidance.pdf.

116. Copeland, Rob, and Sarah E. Needleman. "Google's 'Project Nightingale' Triggers Federal Inquiry." *The Wall Street Journal*, 12 Nov. 2019, https://www.wsj.com/articles/behind-googles-project-nightingale-a-health-data-gold-mine-of-50-million-patients-11573571867?mod=article_inline.

117. "Non-traditional credit" is a wide-ranging term that can involve all sorts of personal data. Some examples are rent payment history, child support/alimony payments, utilities, and tuition. Dobson, Amy. "Non-Traditional Credit Options for Mortgage Applicants." *Forbes*, 14 Sept. 2018, https://www.forbes.com/sites/amydobson/2018/09/14/non-traditional-credit-options-for-mortgage-applicants/#44e4c20f24d3.

118. *State of Alternative Credit Data*. Experian, May 2019, www.experian.com/consumer-information/alternative-credit-data-report?intcmp=Insights.

119. *Agencies Should Provide Clarification on Lender's Use of Alternative Data*. Government Accountability Office, 25 June 2019, https://www.gao.gov/products/GAO-19-694T.

120. The privacy policy must: identify the categories of personally identifiable information the operator collects; identify the categories of third parties with whom the operator may share such personally identifiable information; describe the information review and change request process – if such a process exists, disclose whether third parties may collect consumer data directly from the website; disclose the response to "do-not-track" signals;" describe the process of notification of change; and identify the effective date of the privacy policy.

121. McDonald, Aleecia M., and Lorrie Faith Cranor. "The Cost of Reading Privacy Policies", *I/S: A Journal of Law and Policy for the Information Society*, 2009, https://lorrie.cranor.org/pubs/readingPolicyCost-authorDraft.pdf.

The ambiguity of privacy policies is a critical component of corporate efforts to circumvent regulation and consumer awareness.

Consumer Privacy Act of 2018 (CCPA) provides some further guidance. CCPA requires companies to include a description of a user's rights pursuant to the legislation, categories of data the company has collected about consumers in the preceding 12 months, and categories of consumer data the company has sold or transmitted for a business purpose in the preceding 12 months.

The enforcement policy behind these requirements is a convoluted legal construct. The Federal Trade Commission uses consent agreements to enforce these policies. The enforcement is on the basis of companies engaging in deceptive practices by not living up to the agreement they strike with consumers.

The CCPA's protections are a step in the right direction, but still do not resolve a long-standing issue with privacy policies: obfuscation. While regulation requires websites to disclose "categories" of information collected, no current legislation defines categories specifically. This creates the opportunity for corporations to define categories and obfuscate their definition to the company's benefit. For example, Google's newly revised CCPA privacy policy lists two large categories of information collected with several subsections.[122] The two categories neatly match the policy's ontology of discrete and behavioral information. Google further provides examples of what specific types of collection might contain. Some are straightforward, such as "terms you search for" and "videos you watch." Others are less clear. For example, "activity on third-party sites and apps that use our services" is sufficiently broad to encompass all manner of data collection. Google's categorization of collected data is ambiguous to the point of preventing an internet user from gaining a comprehensive understanding of the data that is being collected. Importantly, the list of examples is also not exhaustive of the company's collection methods. When providing examples of collection, the company prefaces them with statements implying ambiguity: "The activity information we collect may include," "Your location can be determined with varying degrees of accuracy by," and "We also collect the content you create, upload or receive from others. This includes things like…"

The ambiguity of privacy policies is a critical component of corporate efforts to circumvent regulation and consumer awareness. For example, Google's privacy policy states, "We do not sell your *personal information* to anyone."[123] The Electronic Frontier Foundation conducted an extensive evaluation of Google's treatment of personal data and found that statement incomplete at best and intentionally misleading at worst. Because no laws or regulation define "personal information" for private corporations, corporations like Google are free to provide their own definition. Google narrowly defines this category as name, e-mail address, or billing information. This allows them to obscure the fact that the company's Real Time Bidding (RTB) marketing platform sells a trove of other data, including granular location information, specific device identification numbers, and browsing history.[124]

Another important omission from Google's privacy policy is the duration for which the company maintains user data. The policy lists four different types of retention into which data may fall.[125] These categories are clear and well stated, but the last category (which grants Google ownership of data that has "legitimate business purposes") provides a legal exception for Google to hold data for indeterminate periods of time at their sole discretion. It effectively usurps any user right to "opt-out" in the future.

Compared to the rest of the data collection industry, Google's policy gives more detail than many competitors. It should be recognized that CCPA has caused companies to issue more comprehensive privacy policies and is a step in the right direction. The ability of corporate data brokers to hide behind ambiguity while determining the definitions that define contracts with their large and robustly funded legal departments must be addressed.

The legal departments of corporations also frequently utilize privacy policies to deny individuals the ability to bring lawsuits against companies for the mishandling or misuse of their information. This right, typically called a private right to action, is partially reinstated by the CCPA. That bill gives individuals the right to bring a lawsuit against a company if the individual's personal data was compromised as the result of a data breach. If data was not stolen, but willfully sold or shared with third parties almost all privacy policies still prevent individuals from filing lawsuit, even when such sharing is in direct contradiction of the practices outlined in the privacy policy.

The outcome of this is reflected in polling conducted by Pew. Half of Americans said that they had not felt "confident that [they] understood what would be done with [their] data" while interacting with companies in the prior month. Significant

122. The two large sections are "Things you create or provide to [Google]" and "Information [Google] collects as you use [Google's] services." These would fall into discrete and behavioral data categorizations. The subsections of information collected by Google are: "Your apps browsers and devices," "Your activity," and "Your location information." "We Want You to Understand the Types of Information We Collect as You Use Our Services." *Privacy & Terms*, Google, https://policies.google.com/privacy?hl=en-US#infocollect. Accessed 13 Jan. 2021.

123. "We Do Not Sell Your Personal Information to Anyone." *Safety Center*, Google, https://safety.google/privacy/ads-and-data/. Accessed 13 Jan. 2021.

124. Cypher, Bennett. "Google Says it Doesn't 'Sell' Your Data. Here's How the Company Shares, Monetizes, and Exploits it." *Electronic Frontier Foundation*, 19 Mar. 2020, https://www.eff.org/deeplinks/2020/03/google-says-it-doesnt-sell-your-data-heres-how-company-shares-monetizes-and.

125. (1) Deletion upon user discretion, (2) deletion or anonymization after a set period, (3) retention until the deletion of user's Google account, and (3) data 'kept longer' for 'legitimate business or legal purposes' at Google's sole discretion.

minorities also reported feeling impatient, discouraged, and confused while attempting to parse company privacy policies.[126]

Companies collecting indefinite data obfuscate their personal data collection practices through vague language, lengthy verbiage, and misdirection in their privacy policies. The "agreements" that purport to govern the relationship between companies' data collection practices and their consumers are almost entirely unregulated. They also barely meet the threshold of agreements due to a lack of an ongoing relationship with data subjects. Privacy policies that claim to regulate the conduct of companies instead reduce the rights of consumers to delineate the acceptable use of their personal data and to seek remedies when companies misuse it by tying consumers' hands and creating legal hurdles to litigation.

CONSENT

Consent as it relates to privacy and technology has two important attributes, "informed" consent and "default" consent settings. No legislation defines informed consent for digital information disclosure, and thus there is no regulatory definition of consent in the nebulous world of digital data brokering. Organizations collecting data have benefited from a conception of legal consent that has not kept pace with digital technology. Consumers are frequently unaware of a company's intent with respect to their data at the point of surrender.

A 2019 survey of technology experts conducted by Pew Research found that nearly half believed that use of technology will "mostly weaken core aspects of democracy in the next ten years" and one of the keys to this process is a power imbalance created by "citizens' lack of digital fluency."[127] The reality is even more bleak, as the rapid pace of data collection, artificial intelligence, and business needs preclude even the most sophisticated computer scientists from fully understanding the implications of sharing personal data in the present. In such an environment, it is necessary to ask if informed consent of disclosure is even possible, and, if so, what determines it.

This is a critical issue to American voters. In 2015, Pew Research found that 93% of Americans "believed it was important to have control of who can get information about you."[128] Numerous other polls have echoed this concern.[129]

The genetic testing company 23andMe has long marketed itself as focused upon using customer's genetic data to provide personalized ancestry reports and health insights. They also marketed their product as capable of detecting genetic predilections for illness, until the Food Drug Administration (FDA) shut them down.[130] That product was judged to be deceptive, but the FDA left unaddressed the company's similarly misleading business model. As customers paid to have their DNA analyzed, 23andMe was focused on accumulating large amounts of genetic data in order to sell it to research organizations and medical corporations. In the absence of clear guidance, consumers tend to assume that their genetic information is protected by privacy protections, such as HIPAA. In practice, genetic testing companies typically fall outside of those regulations and frequently resell consumer genetic information.[131] In 2013, then 23andMe board member, Patrick Chung, revealed to FastCompany "[t]he long game here is not to make money selling kits, although the kits are essential to get the base level data. Once you have the data, [23andMe] does actually become the Google of personalized health care."[132] In other words, 23andMe relied on the false pretense of an ancestral DNA testing kit to collect consumer information for use at a later date for the company's sole benefit.

Data collection corporations often present themselves as altruistic entities who are driving a better world for all. In practice, they harvest user's most sensitive data and put it to work to create and record financial valuations with little return for the individuals who have had their privacy violated. In the words of Zuboff, we have been "harnessed to a market process in which individuals are definitively cast as the means to other's market ends."[133]

This "bait and switch" strategy is increasingly prevalent within companies that have business models based on the collection and sale of personal data, and rely on indefinite terms. Companies

126. Auxier, Brooke, et al. "Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information." *Pew Research Center*, 15 Nov. 2019, https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/.

127. Anderson, Janna, and Lee Rainie. "Many Tech Experts Say Digital Disruption Will Hurt Democracy." *Pew Research Center*, 21 Feb. 2020, https://www.pewresearch.org/internet/2020/02/21/many-tech-experts-say-digital-disruption-will-hurt-democracy/.

128. Madden, Mary, and Lee Rainie. "Americans' Views About Data Collection and Security." *Pew Research Center*, 20 May 2015, https://www.pewresearch.org/internet/2015/05/20/americans-views-about-data-collection-and-security/.

129. Zuboff, Shoshana. *The Age of Surveillance Capitalism*. 1st ed., PublicAffairs, 2019, p. 61.

130. Gray, Tyler. "FDA to 23andMe Founder Anne Wojcicki: Stop Marketing $99 DNA Test or Face Penalties." *Fast Company*, 25 Nov. 2013, https://www.fastcompany.com/3022208/fda-tells-23andme-founder-anne-wojcicki-to-stop-marketing-99-genetic-test-or-face-penalties.

131. May, Ashley. "Took an Ancestry DNA Test? You Might Be a 'Genetic Informant' Unleashing Secrets About Your Relatives." *USA Today*, 27 Apr. 2018, https://www.usatoday.com/story/tech/nation-now/2018/04/27/ancestry-genealogy-dna-test-privacy-golden-state-killer/557263002/.

132. Murphy, Elizabeth. "Inside 23andMe Founder Anne Wojcicki's $99 DNA Revolution." *Fast Company*, 14 Oct. 2013, https://www.fastcompany.com/3018598/for-99-this-ceo-can-tell-you-what-might-kill-you-inside-23andme-founder-anne-wojcickis-dna-r.

133. Zuboff, Shoshana. *The Age of Surveillance Capitalism*. 1st ed., PublicAffairs, 2019, p. 54.

The consent of individuals in the current privacy landscape is complex and convoluted.

collect consumer data with one stated purpose, only to exploit it later in a manner they previously obfuscated or omitted altogether. Can a consumer consent to data sharing if they do not understand the way in which their data will be utilized?

Companies also rely on consumers' desire for expedience to collect customer data. Most companies have created a system that requires customers to "opt-out" of data collection, aggregation, and sharing. This extra step creates a default-to-inclusion scenario for user data but demands re-evaluation from a consent perspective. "Opt-out" was codified by Gramm-Leach-Bliley, but research indicates that a shift to an "opt-in" system will establish stronger customer consent and comprehension of privacy implications.[134]

Overstating personal data collection requirements for the operation of consumer purchases is another tactic that companies utilize to bully users into surrendering their data. This tactic often involves removing functionality in a device a consumer has purchased as "ransom" for data policy submission. Companies imply that they must have access to data in order to complete business operations, when in fact the data is extraneous or intended for purposes beyond the service of the customer.

The Age of Surveillance Capitalism provides a chilling example of what the combination of these practices can look like. In July 2017, iRobot released a new version of its autonomous vacuum cleaner, Roomba, that can create a digital map of the living space where it is used. In a conversation with Reuters, iRobot's CEO Colin Angle revealed that the robots would create a new revenue stream that will come from selling the floorplans of customers' homes to Google, Amazon, or Apple. The CEO further explained that all data is captured by the Roomba regardless of customer choice, but the transmission of data to the cloud is dependent upon customers "opting-in." If customers do not "opt-in" to iRobot's data collection and sharing agreement, the app allowing them to use their phone to start or pause a cleaning, schedule cleanings, and several other critical features are disabled. As Zuboff eloquently puts it, the proposal to the consumer for data collection purposes is "[b]end the knee or we will degrade your purchase."[135]

The concept of data minimization is a critical component of moving companies away from this manner of deceptive behavior. The European Union's General Data Protection Regulation (GDPR) defines data minimization as collecting data that is "adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed."[136] The concept of collecting only the necessary data to conduct essential business processes is much older than that piece of regulation. The Federal Trade Commission called out the principle of data minimization by name in its 2013 report, "The Internet of Things: Privacy and Security in a Connected World."

While data minimization is a strong concept, in practice it is very difficult to regulate or enforce. In addition to the data minimization concept, GDPR also requires companies to collect data "sufficient to fulfil [the company's] stated purpose."[137] The importance of the stated purpose or business purpose of data once again introduces ambiguity into corporate practices. Companies have generally learned that personal data is profitable. As a result, they are likely to always err on the side of collecting more data and fall back on legal ambiguity as a protection.

The consent of individuals in the current privacy landscape is complex and convoluted. Effective regulation must not only ensure that consumers are aware at the moment of collection, but also have rights to collective bargaining for their data use and the ability to change their mind about data disclosure and use at a future date.

NATIONAL SECURITY IMPLICATIONS

Increasingly, Americans are discovering that their personal data and information has been acquired by foreign governments or proxies of foreign governments, particularly Russia and China. Two of the largest data breaches in American history, the Office of Personnel Management Breach of 2014 and the Equifax breach of 2017, are now suspected to have been carried out by actors within the Chinese Government.[138,139] The Cambridge Analytica scandal brought attention to Russia's capability to micro-target American citizens from abroad and present them with propaganda.[140]

134. Hodges, Sarah. "Examining the Gramm-Leach-Bliley Act's Opt-Out Method for Protecting Consumer Data Privacy Rights on the Internet." *Information & Communications Technology Law*, vol. 22, no. 1, 2013, https://www.tandfonline.com/doi/abs/10.1080/13600834.2013.785177.

135. Zuboff, Shoshana. *The Age of Surveillance Capitalism*. 1st ed., PublicAffairs, 2019, pp. 235-236

136. "Principle (c): Data Minimisation." *Information Commisioner's Office*, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/data-minimisation/.

137. Ibid.

138. Koerner, Brendan I. "Inside the Cyberattack that Shocked the US Government." *Wired*, 23 Oct. 2016, https://www.wired.com/2016/10/inside-cyberattack-shocked-us-government/.

139. Brewster, Thomas. "Chinese Government Hackers Charged with Massive Equifax Hack." *Forbes*, 10 Feb. 2020, https://www.forbes.com/sites/thomasbrewster/2020/02/10/chinese-government-hackers-charged-with-massive-equifax-hack/#5d5cb96161d6.

140. Wong, Julia Carrie. "The Cambridge Analytica Scandal Changed the World – But it Didn't Change Facebook." *The Guardian*, 18 Mar. 2019, https://www.theguardian.com/technology/2019/mar/17/the-cambridge-analytica-scandal-changed-the-world-but-it-didnt-change-facebook.

The breakdown of physical borders in cyberspace has created an environment where Americans' privacy is not just compromised by fellow citizens.

The emergence of the Chinese-owned social media application TikTok demonstrates that regulators have not found a solution, as Congress investigates concerns that members of the Chinese Communist Party could ultimately be making decisions about how the personal information of American citizens is handled.[141]

The breakdown of physical borders in cyberspace has created an environment where Americans' privacy is not just compromised by fellow citizens. The national security implications of allowing companies to keep enormous troves of consumer data without direct oversight of collection and protection measures was made plainly apparent when the United States Department of Justice charged four Chinese military members with the hack of nearly 150 million Americans' personal data in 2017.[142] This was not the first time that foreign governments have been suspected of attempting to hack online resources to gain access to Americans' personal information. American authorities have long suspected that the compromise of over 20 million individuals' security clearance information was conducted by the Chinese government and arrested a Chinese national in connection with that hack in 2017.[143]

Clearly, the personal information of American citizens is desired by competitors and adversaries around the world. In order to better protect U.S. national security, we must increase knowledge and transparency of data flows within private companies to ensure foreign governments are not surreptitiously interfering with American citizens.

LACK OF FEDERAL OVERSIGHT

Privacy regulation of government entities is decentralized and ineffective. The principal oversight bodies for government surveillance are the Privacy and Civil Liberties Oversight Board (PCLOB or the Board) and the Office of the Director of National Intelligence. The PCLOB was officially created by the Implementing Recommendations of the 9/11 Commission Act of 2007 to provide oversight and advice. It is made up of a chairperson, four part-time board members, and a small support staff. Although it was established as an independent executive agency in 2007, it was not until 2012 that the Senate confirmed enough board members to form a quorum. The Board again lost its quorum in 2016 and in October 2018 regained it, with three members appointed, including the chairperson. In June 2019, following the Senate confirmation of two nominations, the Board had a full slate of members for the first time since 2016. The planned expansion of the full-time staff following the reestablishment of quorum will contain 25 total members by the end of the third quarter of 2019. The Board's 2020 Budget Request is $8.5 million.[144,145,146] The National Intelligence Community appropriated budget was $81.7 billion in 2019 for military and national intelligence.[147]

As a result of the PCLOBs small budget and internal turnover, the Board has filled an advisory role with no oversight authority. The most noteworthy accomplishment of the PCLOB to-date was a report in 2014 that found the National Security Agency's bulk collection of telephone metadata from telecom companies "lack[ed] a viable legal foundation," "implicate[d] constitutional concerns under the First and Fourth Amendments," "raise[d] serious threats to privacy and civil liberties as a policy matter," and provided "only limited value." The report concluded by suggesting that the government should end its bulk collection program. The Obama administration responded by stating "we simply disagree with the board's analysis on the legality of the program."[148] The program continued for the next five years, until being shuttered

141. Quinn, Melissa. "Tiktok Scrutiny Shows Heightened Government Focus on Private Data and National Security Ties." *Washington Examiner*, 28 Nov. 2019, https://www.washingtonexaminer.com/news/tiktok-scrutiny-shows-heightened-government-focus-on-private-data-and-national-security-ties.

142. Brewster, Thomas. "Chinese Government Hackers Charged with Massive Equifax Hack." *Forbes*, 10 Feb. 2020, https://www.forbes.com/sites/thomasbrewster/2020/02/10/chinese-government-hackers-charged-with-massive-equifax-hack/#5d5cb96161d6.

143. Moon, Mariella. "FBI Nabs Chinese National Linked to Massive OPM Hack." *Engadget*, 25 Aug. 2017, https://www.engadget.com/2017-08-25-fbi-nabs-chinese-national-opm-hack.html.

144. "About." *US Privacy and Civil Liberties Oversight Board*, https://www.pclob.gov/about/. Accessed 14 Jan. 2021.

145. *Strategic Plan 2019-2020*, U.S Privacy and Civil Liberties Oversight Board, January 2019, https://documents.pclob.gov/prod/Documents/StrategicPlans/10/StrategicPlan_2019-2022.pdf

146. *Fiscal Year 2020 Budget Justification,* US Privacy and Civil Liberties Oversight Board, Jan. 2019, https://documents.pclob.gov/prod/Documents/BudgetJustification/25/CBJ%20FY20%20PCLOB.pdf.

147. "US Intelligence Community Budget." *Office of the Director of National Intelligence*, 18 Mar. 2019, https://www.dni.gov/index.php/what-we-do/ic-budget.

148. Nakashima, Ellen. "Obama Disagrees with Watchdog Group's Conclusion that NSA Phone Program Is Illegal." *Washington Post*, 23 Jan. 2014, https://www.washingtonpost.com/world/national-security/obama-disagrees-with-watchdog-groups-conclusion-that-nsa-phone-program-is-illegal/2014/01/23/7a945564-8464-11e3-8099-9181471f7aaf_story.html.

in 2019 due to a lack of efficacy.[149] The Trump administration signaled a desire to reauthorize the program, which collected the metadata of millions of Americans' phone usage. A bi-partisan bill is currently before Congress that would preclude the program being renewed.[150]

The secretive courts established by the Foreign Intelligence Surveillance Act (FISA) have also recently come under scrutiny. A December 2019 investigation by the Department of Justice (DoJ) found that 100% of warrants reviewed within the course of the investigation cited facts that were not properly supported. It is important to note that this review was only of the warrant requests and did not include associated case files, but the scale and ubiquity of the failure to meet basic recording requirements is a disturbing signal.[151]

This particular report's findings, which focused on procedures that require the inclusion of factual evidence to support claims, are emblematic of the problem facing larger intelligence and law enforcement oversight. The processes and procedures are necessarily confidential, but adequate oversight and transparency measures have not been developed as needed. Clearly, the existing bureaucratic entities provide little effective oversight and no protection of privacy in the data collection practices of the intelligence and law enforcement agencies.

LACK OF PRIVATE SECTOR REGULATION

The private sector is principally regulated by the Federal Trade Commission. The Federal Trade Commission was established in 1914 to "protect consumers and promote competition."[152] It now consists of three bureaus–The Bureau of Competition, The Bureau of Consumer Protection, and The Bureau of Economic–and approximately 1,100 full-time employees.[153] In 2019, it employed 52 full time employees, with a budget of $9.9 million, in execution of its Privacy and Identity Protection activity.[154]

These enforcement bodies are miniscule and lack the cohesion and budget to adequately regulate the personal data market and surveillance by government and private actors. The FTC referred to its recent $5 billion civil penalty against Facebook as a "paradigm shift."[155] Previously, the largest penalty paid by a technology company was $22.5 million by Google. The penalty is indeed one of the largest ever levied by any government towards a private company for any violation, and the largest such fine for a violation of customers' privacy. The judge who approved the fine offered a more nuanced evaluation, stating the complaints against Facebook "call into question the adequacy of laws governing how technology companies that collect and monetize Americans' personal information must treat that information."[156] The fine was levied through a consent agreement that Facebook had previously signed with the FTC in 2011.

Consent agreements have been the primary enforcement mechanism the government has used to penalize corporate privacy violations. These agreements penalize companies for violating their privacy agreements with customers–which the companies themselves crafted in the form of a privacy policy–, they require no admission of guilt or negligence on behalf of the participant organization, and they are mandated to expire in 20 years or less.

The rapid pace of growth and development within the data market suggest that even an enormous penalty is not enough to change social media practices that undermine the right to privacy without actual laws and regulations that prescribe standards for the collection, storage, and sale of personal information. Government surveillance programs still lack any effective oversight.

The public sector lacks expertise at all levels of government to define privacy standards for digital personal data collection and dissemination, and to hold government agencies and private corporations accountable for enforcing them. The dismantling

149. Nakashima, Ellen. "NSA Has Halted a Counterterrorism Program Relying on Phone Records Amid Doubts About its Utility." *Washington Post*, 5 Mar. 2019, https://www.washingtonpost.com/world/national-security/nsa-has-halted-a-counterterrorism-program-relying-on-phone-records-amid-doubts-about-its-utility/2019/03/05/f2d2793e-3f80-11e9-922c-64d6b7840b82_story.html.

150. Nakashima, Ellen. "House Panel to Debate Bill that Would Prevent NSA from Reviving Dormant Surveillance Program." *Washington Post*, 24 Feb. 2020, https://www.washingtonpost.com/national-security/house-panel-to-debate-bill-that-would-prevent-nsa-from-reviving-dormant-surveillance-program/2020/02/24/9c22cc1e-574a-11ea-9000-f3cffee23036_story.html.

151.*Management Advisory Memorandum for the Director of the Federal Bureau of Investigation Regarding the Execution of Woods Procedures for Applications Filed with the Foreign Intelligence Surveillance Court Relating to U.S. Persons*. Office of the Inspector General, US Department of Justice, 31 Mar. 2020, https://oig.justice.gov/reports/management-advisory-memorandum-director-federal-bureau-investigation-regarding-execution.

152. "Our History." *Federal Trade Commission*, https://www.ftc.gov/about-ftc/our-history. Accessed 31 Jan. 2021.

153. *Fiscal Year 2019 Congressional Budget Justification*. Federal Trade Commission, 12 Feb. 2018, https://www.ftc.gov/system/files/documents/reports/fy-2019-congressional-budget-justification/ftc_congressional_budget_justification_fy_2019.pdf.

154. Ibid.

155. Fair, Lesley. "FTC's $5 Billion Facebook Settlement: Record-Breaking and History-Making." *Federal Trade Commission*, 24 July 2019, https://www.ftc.gov/news-events/blogs/business-blog/2019/07/ftcs-5-billion-facebook-settlement-record-breaking-history.

156. Swisher, Kara. "The Immunity of the Tech Giants." *New York Times*, 1 May 2020, https://www.nytimes.com/2020/05/01/opinion/tech-companies-coronavirus.html?action=click&module=Opinion&pgtype=Homepage.

of the Office of Technology Assessment in 1995 left a void for experts in technology and data to serve the public sector. Instead, policy makers are provided a skewed perspective by lobbyists of the technology industry. For example, Google has been among the top 20 corporate lobbying spenders every year since 2012 and the top 10 in two of the three years between 2017 and 2019.[157] The emergence of the California Consumer Privacy Act and discussions of broader federal data privacy laws have resulted in an increase in lobbying over the past five years. A *Wall Street Journal* analysis found that the collective lobbying spending of 12 large, publicly traded cybersecurity firms more than tripled from 2015 to 2019.[158]

NEW REGULATORY MODELS

The European Union has begun to respond to the challenges of private entities that collect consumers' information. The most sweeping regulation was the E.U.'s recent passage of the General Data Protection Regulation. GDPR has yet to levy any major fines, but it is capable of fining corporations up to 4% of global annual revenue for infractions. The new guidelines have not been without controversy. GDPR strengthens existing protections for Europeans' right to be "forgotten" digitally. This has created a conflict over whether past crimes and arrests may still be reported in news outlets.[159]

Further concerns about GDPR's success have recently arisen. An in-depth report by *Politico* reveals that 18 months into the regulatory body's existence, only a single €50 million fine has been imposed. Concerns about the regulator include a conflict of interest regarding its placement in Ireland–a country heavily dependent upon revenues from data driven technology companies–and increasing delays on judgements. An official spokesman for a German data protection authority stated, "[i]t is absolutely unsatisfactory to see that the biggest alleged data protection violations of the last 15 months with millions of individuals [concerned] are far away from being sanctioned."[160]

California became the first American state to pass sweeping data privacy legislation, with the California Consumer Privacy Act of 2018. The law bears many similarities to GDPR, but is still in its early implementation stages, making it difficult to evaluate. Though the legislation has driven many positive trends, many of its important protections have still not been codified. An intensive lobbying effort is currently occurring in Sacramento by both privacy advocates and data collection lobbyists.[161] Over the course of the next year, the bill could gain significantly stronger privacy protections, or be left gutted of any significant consumer protections.

Multi-lateral organizations have also arisen to address the movement of personal data internationally. The E.U.-U.S. Privacy Shield lacks regulatory power, but is a recognized set of guidelines for both the United States Chamber of Commerce and the European Commission, and has been ratified by the United States and European congresses. Corporate participation with the organization is voluntary and not a prerequisite to conduct international data transfers, though it significantly reduces administrative hurdles to do so.[162] The future of the agreement has been thrown into question, however, due to President Trump's guidance that American government agencies do not afford non-citizens the protections of the Privacy Act of 1974.[163]

Zuboff lays out a cycle in *The Age of Surveillance Capitalism*: incursion, habituation, adaptation, and redirection. This is a cycle in which companies begin data collection–fully aware of legal ambiguity or prohibition–, amass enormous amounts of information and acclimate users to the practice through habituation, leverage collected data for new collection streams of which the public and regulators are not yet aware, and finally redirect outrage and regulation to a scapegoat with little operational control or impact.[164] This "dispossession cycle" relies on government regulators being slow to react. The enormous capitalization, robust legal departments, and a-symmetrical division of information many technology companies enjoy allow them to act in the absence of regulation.

Proposed Solutions

The principles of transparency, personal agency, and accountability are the foundations upon which the right to privacy can be restored. The establishment of these three values is a key first step towards re-establishing a hierarchy in which companies are accountable to the government and the government is accountable to its citizens. Solutions should provide greater oversight of data collection by public and private entities, guarantee adequate controls of previously collected and

157. "Lobbying Data Summary." *OpenSecrets.org*, https://www.opensecrets.org/federal-lobbying/

158. Rundle, James. "Cybersecurity Lobbying Spending Mounts as Privacy, Security Laws Take Shape." *Wall Street Journal*, 4 May 2020, https://www.wsj.com/articles/cybersecurity-lobbying-spending-mounts-as-privacy-security-laws-take-shape-11588619239.

159. Satariano, Adam, and Emma Bubola. "One Brother Stabbed the Other. The Journalist Who Wrote About it Paid a Price." *New York Times*, 23 September 2019, https://www.nytimes.com/2019/09/23/technology/right-to-be-forgotten-law-europe.html.

160. Vinocur, Nicholas. "'We Have a Huge Problem': European Tech Regulator Despairs Over Lack of Enforcement." *Politico*, 27 Dec. 2019, https://www.politico.com/news/2019/12/27/europe-gdpr-technology-regulation-089605.

161. Lapowsky, Issie. "Inside the Closed-Door Campaigns to Rewrite California Privacy Law, Again." *Protocol*, 6 Feb. 2020, https://www.protocol.com/inside-california-privacy-law-redo.

162. "Privacy Shield Program Overview." *Privacy Shield Framework,* https://www.privacyshield.gov/Program-Overview. Accessed 14 Jan. 2021.

163. Muncaster, Phil. "Trump Order Sparks Privacy Shield Fears." *Info Security Magazine*, 27 Jan. 2017, https://www.infosecurity-magazine.com/news/trump-order-sparks-privacy-shield/.

164. Zuboff, Shoshana. *The Age of Surveillance Capitalism*. 1st ed., PublicAffairs, 2019, pp. 139-155.

To effectively regulate privacy rights and create a new information ecosystem in which consumers are empowered to make decisions about the collection and use of their data, some definitions and concepts must be updated.

compromised personal data, and create economic incentives for personal data minimization by government and private industry.

Two thirds of Americans say "current laws are not good enough in protecting people's privacy" and 61% have said "they would like to do more to protect their privacy."[165] The expression of this broad level of public concern can form an important bi-partisan political basis for implementing regulations that Americans can use to control their own personal information.

To effectively regulate privacy rights and create a new information ecosystem in which consumers are empowered to make decisions about the collection and use of their data, some definitions and concepts must be updated. Distinctions between privacy and security, and the resulting prioritization of values, must be developed through transparency and debate between citizens, their representatives, and the companies pioneering the new data economy. The following proposed solutions do not define these new evaluations but establish a framework of transparency that will allow Americans to arrive at their own conclusions and create new standards.

REQUIRE TRANSPARENCY

In 2012, then-FBI Director Robert Mueller stated that there are two types of companies, "those that have been hacked and those that will be."[166] Despite this prescient statement, regulators have continued to allow companies to collect and process data as though they can protect it. A mentality shift from surprise at data breaches to the expectation that they will occur will result in a fundamental change in the presumption of companies' rights to collect data and individual's rights to control these behaviors.

Acknowledging the likelihood of a data breach also imposes a requirement upon companies to minimize risk to consumers whose data they collect. To effectively regulate this corporate responsibility, Congress must pass legislation to create federal cybersecurity and data maintenance requirements through the National Institute of Standards and Technology (NIST). NIST has already established a voluntary cybersecurity framework for organizations. Congress should act to make the standards mandatory and leverage harsh fines for companies that suffer a breach without adhering to them. Further, standards of criminal negligence should be established for corporate executives whose cybersecurity policies are egregiously negligent.

SET NATIONAL PRIVACY POLICIES AND STANDARDS

The Fair Information Practices of 1973 were national guidelines for the collection, storage, and use of data. Much of our current privacy erosion could be stopped by incorporating them into legislation that governs the behavior of companies. Similarly, extending the responsibilities of The Privacy Act of 1974 to organizations beyond the government would significantly increase the individual right to privacy in America.

Absent this sort of sweeping legislation, however, lawmakers can take important steps toward protecting Americans by mandating privacy policies that state in clear and understandable terms:

- What data is being collected (an exhaustive list with specific examples)
- How it is being used
- When and how it might be sold
- How long it will be retained
- The rights of individuals to change or opt out of collection or sharing, following initial consent.

Regulations should require these five questions to be the first sections of any policy to allow consumers to quickly read and understand companies' practices without being bogged down by liability or other legal distinctions. Additionally, laws should require these policies to be prominently displayed and highlighted at the top of a company's website instead of buried where consumers are unlikely to find them and even less likely to read them.

RE-EVALUATE THE TRADEOFFS BETWEEN HARMS AND BENEFITS OF PUBLIC RECORD DISCLOSURES.

The world was different when most current government disclosure regulation was written. Information such as real estate listings and arrest records could be made available to the public because they were restricted by both geography and vested interest. In order to access the arrest records for the previous night in Flagler County, Florida a person would have to travel to the police station. That could be argued to be a genuine public good. It allowed local members of a community to be aware of current events in their area. Now, that same information is available to anyone who visits florida.arrests.org, along with mugshots and "tags" provided by anonymous internet users. Minor criminal convictions or other embarrassing information can now function as a modern scarlet letter.

Local, state, and federal governments must do an extensive review of all data personal data made available to the public and re-evaluate its public good against the privacy harms of wide internet availability.

165. Rainie, Lee. "Americans' Complicated Feelings About Social Media in an Era of Privacy Concerns." Pew Research Center, 27 Mar. 2018, https://www.pewresearch.org/fact-tank/2018/03/27/americans-complicated-feelings-about-social-media-in-an-era-of-privacy-concerns/.

166. Mueller, Robert S. "Combating Threats in the Cyber World: Outsmarting Terrorists, Hackers, and Spies." RSA Cyber Security Conference, March 1, 2012, San Francisco, CA, https://archives.fbi.gov/archives/news/speeches/combating-threats-in-the-cyber-world-outsmarting-terrorists-hackers-and-spies.

PROTECT AGENCY OF PERSONAL DATA SUBJECTS

The current corporate environment has allowed companies to presume consent for data collection from consumers, using an "opt-out" method. This form of data collection requires the consumer to act in order to remove their information from collection or consideration. In other words, it requires an act of affirmative dissent. This standard was established by the Gramm-Leach-Bliley Act for companies in the financial sector and other information collection companies have taken the same approach. GDPR regulation is one of the first to require consumers to "opt-in" to data collection. This requirement of active consent requires companies to fully engage customers on matters of privacy instead of concealing it.

Vermont and California have already created data broker registries through legislation in the past few years. Creation of a national registry will standardize this practice and ensure that Americans residing in all 50 states will have the right to know the companies that are secretly collecting their data. Just as centralizing a registry for data brokers will provide a single source for consumers to learn of the companies engaging in the practice of collecting and selling data, the federal government should create a single portal by which consumers can update and remove data profiles these companies maintain.

Governments must especially protect consumer data that is unchangeable (social security number, genome, birth date) and prevent companies from collecting or selling such information. Existing protections for protected classes of data, such as health and financial data, are actively being circumvented by data collection corporations. In January 2020, the *Wall Street Journal* reported that Google has gained access to millions of individual medical records. The report indicated that this acquisition was permitted by HIPAA because the law includes a provision for health organizations to share patient health records with other companies in service of business functions. Piecemeal legislation protecting classes of data will not solve this problem. Privacy reforms must establish the types of data that are acceptable for companies to gather, sell, and analyze, and create regulations that clearly prohibit any organization or corporation from selling or collecting protected categories of data in one comprehensive document.

GOVERNMENT ACCOUNTABILITY

In response to the current crisis of privacy, many have called for an end to behavioral data and personal data markets. The reality is the opportunity for such an approach has already passed. The world's largest corporations now utilize this business model and provide millions of jobs, while consumers have grown accustomed to services and conveniences offered at the price of personal data. The market for personal data is here to stay, but it should be heavily regulated.

The Privacy and Civil Liberties Board should be expanded and given broad oversight authority, reimagined as The Privacy and Data Commission. Using the U.S. Securities and Exchange Commission as a model, the new data commission would provide oversight and regulation for the collection of personal data in military departments and add authorities in both the civilian national intelligence sector and the private sector. Critically, this new agency would have regulatory control of personal data from initial collection through destruction. The intertwined nature of these organizations makes effective regulation impossible if segmented to just one sector. Additionally, The Privacy and Data Commission will provide market oversight instead of targeting individual companies. As a result, the Commission can create and advise policy to encourage regulatory compliance and best practices across the industry instead of catching only a few bad actors via consent agreements.

The Privacy and Data Commission should have authority over the existing privacy and civil liberties departments in federal law enforcement and intelligence agencies. The creation of the Office of the Director of National Intelligence resulted in a centralized organization to streamline intelligence efforts. The new Privacy and Data Commission will provide cohesive and coherent privacy and data policy across all sectors. Both GDPR and the Office of the Privacy Commissioner of Canada are good models for this new vision. California's Consumer Privacy Act is enforced by the California Attorney General but, like other American regulatory bodies, data privacy is just one of many competing priorities that they must juggle.

Data privacy in the corporate and private sectors creates complex challenges. No single solution will resolve these issues, just as federal regulation has been adjusted and re-evaluated in the financial sector since the passage of the Securities Exchange Act of 1934. That law still represented an important first step by establishing the U.S. Securities and Exchange Commission in recognition that the securities market was an emerging threat to consumer rights. The development of the personal data market over the past few decades necessitates a similar first step. The Commission must be funded and staffed at a comparable level to the SEC for its new responsibilities. While financial markets are larger than personal data markets at the moment, five of the top six most valuable companies in the world are engaged in data collection and monetization. Additionally, this new entity will have an unprecedented combination of oversight of public and private entities that will require scale to implement.

The creation of The Privacy and Data Commission will be an important step towards bringing balance to the market for personal data.

VALUE DATA BREACH LIABILITY AT MARKET VALUE

The largest hurdle preventing regulators from holding companies accountable for data breaches is the lack of a clear value for data compromises. The federal government must pass legislation to collect damages related to a data breach equal to the market value of that data as related by the most recent unamortized cost of acquiring that data, or as the value of the data as represented on a publicly traded company's corporate tax return.

This reform would pass the cost of the data breach onto the company that stored the information and allowed it to become compromised. The Equifax data breach of 2017 provides an example of how this would work. Equifax was limited to a judgment of at most $425 million to benefit those affected by the breach, but their own balance sheet valued the data the company maintained at $1.44 billion. The problem with data breaches is the value of the company's core asset, data, is not negatively affected because it is only duplicated not stolen. In this way, the federal government can create the appropriate incentives for companies to protect consumer data by ensuring that companies feel the full expense of their compromised asset.

Policy Recommendations

HOW TO REIMAGINE RIGHTS AND RESPONSIBILITIES:

- **Require Transparency and Security.** Enact federal legislation to require the subject's "conscious consent and opt-in" to any personal data that companies collect, mandate strict standards for maintaining data security, and provide remedies to data subjects for breaches of data security.

- **Establish National Privacy Policies and Standards.** Require all government and private sector organizations and entities to state in clear and understandable terms what personal data they collect, how it is used, when and how it is disseminated, how long it will be retained, and what rights individuals have to change or opt out of collection or sharing, following their initial conscious consent.

- **Protect Agency of Personal Data Subjects.** Prohibit indefinite data collection by companies with no relationship to targeted personal data subjects, establish a central data registry and a single process by which individuals can de-list information, and limit the collection and sale of specific forms of data, such as personal health and financial information.

- **Create a Government Accountability Agency for Personal Data Collection and Distribution.** Establish The Federal Privacy and Data Commission, based on the regulatory model of the Securities Exchange Commission, with broad authority to promulgate and enforce privacy standards for personal data collection by government and private sector organizations and entities.

Reimagining Rights & Responsibilities in the United States

Carr Center for Human Rights Policy
Harvard Kennedy School
79 JFK Street
Cambridge, MA 02138

This publication was published by the Carr Center for Human Rights Policy at the John F. Kennedy School of Government at Harvard University

79 JFK Street
Cambridge, MA 02138

617.495.5819
https://carrcenter.hks.harvard.edu