

PRIVACY IN AUTHORITARIAN TIMES: SURVEILLANCE CAPITALISM AND GOVERNMENT SURVEILLANCE

DANIEL J. SOLOVE

INTRODUCTION	53
I. AUTHORITARIANISM AND PRIVACY	58
<i>A. Shades of Authoritarianism</i>	59
1. Authoritarianism Is Not Necessarily Extra-Legal	59
2. Authoritarianism Involves a Large Ensemble	61
3. Marshaling Individual Collaboration and Vigilantism	62
<i>B. Why Privacy Is Essential to Resist Authoritarianism</i>	63
1. Personal Data Is Essential to Power and Control	64
2. The Harms of Government Surveillance and Authoritarian Privacy Invasions	67
<i>C. The Dangers of the Digital Age and AI</i>	74
1. Data and Digital Dossiers	74
2. Inferences	76
3. Enhanced Surveillance Capabilities	77
<i>D. Surveillance Capitalism Meets Government Surveillance</i>	79
II. REGULATING GOVERNMENT SURVEILLANCE	82
<i>A. Overturning the Third-Party Doctrine</i>	83
1. The Flaws and Dangers of the Third-Party Doctrine	83
2. <i>Carpenter</i> and Its Aftermath	84
3. Developing <i>Carpenter</i> 's Principles	85
<i>B. Revitalizing the Fourth Amendment</i>	88
1. Government Data Use and Retention	89
2. Beyond the Secrecy Paradigm: Protecting Privacy in Public	89
3. Restriction of Dragnet Searches	90
4. Restoring Fourth Amendment Principles	93
<i>C. Applying Other Constitutional Provisions to Government Surveillance</i>	94
<i>D. Statutory Restrictions on Government Surveillance</i>	95
1. Updating the Electronic Communications Privacy Act	95
2. Restrictions on Government Access to Data	97
3. Statutory Regulation of Government Use and Retention of Data	98
4. Principle-Based Regulation of Government Use of Surveillance Technologies	98
III. REGULATION OF SURVEILLANCE CAPITALISM	100
<i>A. Beyond the Individual Control Model</i>	102
1. The Failure of the Notice-and-Choice Approach	102

- 2. The Failure of Privacy Self-Management 103
- 3. An Example of the Problems with Privacy Laws: Health Data 106
- B. Data Minimization* 108
- C. Restricted Data Transfer to the Government* 110
- D. Protection of Confidentiality* 112
 - 1. Confidentiality of Relationships and Information Fiduciaries 112
 - 2. Protection of Confidentiality of Media Sources..... 114
- E. Rethinking Privacy in Public and Publicly Available Information*..... 115
- F. Regulation of Surveillance Technologies* 118
- G. How the Law Can Be Reformed*..... 119
 - 1. Legislation 119
 - 2. Judicial Actions 120
 - 3. State Constitutional Reforms..... 121
- IV. OTHER IMPORTANT PROTECTIONS 122
 - A. Protection of Decisional Privacy* 122
 - B. Civil Litigation and Discovery of Private Information*..... 123
 - C. Protection of Safety*..... 124
- CONCLUSION 125

PRIVACY IN AUTHORITARIAN TIMES: SURVEILLANCE CAPITALISM AND GOVERNMENT SURVEILLANCE

DANIEL J. SOLOVE*

Abstract: As the United States and much of the world face a resurgence of authoritarianism, the critical importance of privacy cannot be overstated. Privacy serves as a fundamental safeguard against the overreach of authoritarian governments. Authoritarian power is greatly enhanced in today's era of pervasive surveillance and relentless data collection. We are living in the age of "surveillance capitalism." There are vast digital dossiers about every person assembled by thousands of corporations and readily available for the government to access.

The federal government and some state governments are intensifying surveillance and data collection efforts, targeting immigrants, punishing those involved in seeking or providing abortion services, and cracking down on gender-affirming healthcare. Personal data is being weaponized against critics and others who resist these efforts.

In this Article, I contend that privacy protections must be significantly heightened to respond to growing threats of authoritarianism. Major regulatory interventions are necessary to prevent government surveillance from being used in inimical ways. But reforming Fourth Amendment jurisprudence and government surveillance alone will not protect against many authoritarian invasions of privacy, especially given the oligarchical character of the current strain of authoritarianism. To adequately regulate government surveillance, it is essential to also regulate surveillance capitalism. Government surveillance and surveillance capitalism are two sides of the same coin. It is impossible to protect privacy from authoritarianism without addressing consumer privacy.

This Article proposes regulatory measures that should be taken to address government surveillance and surveillance capitalism—on both sides of the coin—to guard against authoritarianism.

INTRODUCTION

As the United States and much of the world face a resurgence of authoritarianism reminiscent of the darkest chapters of the last century, the critical

* Bernard Professor of Intellectual Property and Technology Law, George Washington University Law School. Thanks to my research assistants Rafal Fryc, Vaishali Nambiar, and Luke Posniewski. Thanks to Hannah Bloch-Wehba, Kiel Brennan-Marquez, Andrew Guthrie Ferguson, Barry Friedman, Allyson Haynes Stuart, Aziz Huq, Orin Kerr, Matthew Tokson, Ari Waldman, and Rebecca Wexler for helpful feedback.

importance of privacy cannot be overstated.¹ Privacy serves as a fundamental safeguard against the overreach of authoritarian governments. Unfortunately, existing privacy laws are poorly equipped to shield individuals from government access to personal data, leaving us more exposed than ever in an era of pervasive surveillance.

Authoritarian governments seek to control people by invading their private lives. They envelop people in surveillance to ensure that people are obedient. They ferret out dissenting thought to be attacked—with threats, ostracism, blacklisting, pretextual law enforcement, and outright criminal penalties. They seek to control people's bodies and minds. They use personal data to manipulate, blackmail, apprehend, or punish people.

Authoritarian power is greatly enhanced in today's era of pervasive surveillance and relentless data collection.² We are living in the age of "surveillance capitalism," a term coined by Shoshana Zuboff to refer to the massive collection and use of personal data by companies.³ There are vast digital dossiers about every person assembled by thousands of corporations and readily available for the government to access.⁴

The Fourth Amendment offers little to no protection for much of our personal data in the digital age, largely due to the third-party doctrine. This flawed doctrine, crafted by the U.S. Supreme Court in the 1970s, asserts that individuals forfeit any reasonable expectation of privacy—and thus Fourth Amendment protection—when their personal data is held by third parties.⁵ The third-party doctrine is profoundly outdated and ill-suited to the modern era, where vast amounts of personal information are stored and managed by third-party entities.⁶

Beyond the lack of meaningful Fourth Amendment protection against modern digital surveillance technologies and government data gathering, Congress has failed to update existing laws and pass new ones to provide a meaningful regulatory framework.

¹ I am not attempting to advance a definition of authoritarianism or make claims about whether the U.S. has crossed a particular threshold for authoritarianism. This Article focuses on why the protection of privacy is essential to resist authoritarian power—to slow its growth, curtail its reach, and diminish its risks of metastasizing. My purpose is to explore why and how privacy law should be improved to address the threat of authoritarianism.

² I will refer to government data gathering and surveillance as simply "government surveillance" for shorthand, though data gathering is not quite the same as other forms of surveillance such as watching and listening.

³ SHOSHANA ZUBOFF, *THE AGE OF SURVEILLANCE CAPITALISM: THE FIGHT FOR A HUMAN FUTURE AT THE NEW FRONTIER OF POWER* 14 (2019).

⁴ Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. CAL. L. REV. 1083, 1084 (2002) [hereinafter Solove, *Digital Dossiers*].

⁵ See generally *Smith v. Maryland*, 442 U.S. 735 (1979) (holding that there is no reasonable expectation of privacy in information voluntarily shared with third parties).

⁶ Solove, *Digital Dossiers*, *supra* note 4, at 1084.

The federal government and some state governments are intensifying surveillance and data collection efforts, targeting immigrants, punishing those involved in seeking or providing abortion services, and cracking down on gender-affirming healthcare. Personal data is being weaponized against critics and others who resist these efforts. These campaigns may be bolstered by vigilante groups, using personal data to dox, threaten, and harm individuals they oppose—echoing historical instances where ordinary citizens actively aided totalitarian regimes in identifying and punishing dissenters or perceived “undesirables.”

AI is supercharging surveillance, amplifying its reach and effectiveness to unprecedented levels. With its ability to process vast amounts of data rapidly, AI can sift through countless streams of surveillance footage, identifying patterns and anomalies that would otherwise go unnoticed by human analysts.

When the government demands access to personal data or the use of corporate technologies, will companies resist? History suggests the answer is likely no. In the past, many companies have demonstrated a willingness to comply with such demands. During the last century, corporations provided the Nazis with the technology and information they sought, facilitating their regime’s sinister objectives.⁷

More recently, after 9/11, companies readily handed over vast amounts of data to the federal government, often in violation of their own privacy policies.⁸ Even businesses that are not initially inclined to cooperate frequently cave under the weight of government pressure, whether due to legal threats, financial incentives, or fear of retaliation. This pattern of compliance underscores a troubling dynamic: when governments seek access to private information, corporate resistance is often fleeting, leaving individuals’ privacy at risk and unchecked power in the hands of authorities.

For many decades, including in times when many might have considered the risk of authoritarianism to be remote, the law has struggled to reign in both surveillance capitalism and government surveillance. Government surveillance capabilities have vastly increased over the years despite concerns about growing police powers and a lack of accountability and democratic control. Surveillance capitalism has run rampant, with privacy law at most nipping gently at its heels but doing little to corral the vast expansion in the collection and use of personal data. Augmented and unaccountable government surveillance power is an underappreciated harm of surveillance capitalism—especially given the oligarchical nature of the growing authoritarianism in the U.S. Of course, even

⁷ See generally EDWIN BLACK, *IBM AND THE HOLOCAUST: THE STRATEGIC ALLIANCE BETWEEN NAZI GERMANY AND AMERICA’S MOST POWERFUL CORPORATION* (2012) (discussing the use of International Business Machines’ (IBM) technology in the Holocaust).

⁸ Julia Angwin et al., *AT&T Helped U.S. Spy on Internet on a Vast Scale*, N.Y. TIMES (Aug. 15, 2015), <https://www.nytimes.com/2015/08/16/us/politics/att-helped-nsa-spy-on-an-array-of-internet-traffic.html> [<https://perma.cc/X3WE-2K2M>].

in normal times, the law ought to protect privacy more effectively, but the current rise of authoritarianism dramatically heightens the stakes. Unfortunately, policymakers squandered the opportunity to erect a strong edifice of privacy protection, and the tremors of authoritarianism are now worsening. Although many measures would have been best established long ago, it is still not too late to undertake certain measures, and doing so is essential to withstanding the current wave of authoritarianism.

In this Article, I contend that privacy protections must be significantly heightened to respond to growing threats of authoritarianism. Major regulatory interventions are necessary to prevent government surveillance from being used in inimical ways. But reforming Fourth Amendment jurisprudence and government surveillance alone will not protect against many authoritarian invasions of privacy. To adequately regulate government surveillance, it is essential to also regulate surveillance capitalism. Government surveillance and surveillance capitalism are two sides of the same coin. It is impossible to protect privacy from authoritarianism without addressing consumer privacy.

A popular strand of thinking in the U.S.—one that has had a strong influence on U.S. privacy law—is a libertarian view of power under which government power should be strongly restrained and private sector power should be lightly regulated. Consistent with this view, U.S. privacy law has tended towards a market-based approach, regulating the corporate collection, use, and disclosure of personal data much more permissively than in the European Union.⁹ But in authoritarian regimes, especially oligarchical ones, corporate and government power are intertwined. To protect privacy, it is not possible to keep government power in check without addressing corporate power.

Unfortunately, as with the regulation of government surveillance, the regulation of surveillance capitalism has also been woefully inadequate. Despite the recent enactment of a blizzard of U.S. state consumer privacy laws, these laws are mostly quite weak and fail to address the harms and risks when companies become involved in government surveillance. Consumer privacy laws often provide a false sense of control, suggesting that individuals have meaningful agency over their personal data when, in reality, they do not. Though many privacy laws grant individuals the right to delete their data or opt out of certain uses, these rights are often narrowly defined and impractical for most people to exercise effectively. Most individuals lack the time, expertise, or resources to navigate the complex and time-consuming processes required to manage their digital footprint.¹⁰

⁹ ANU BRADFORD, *DIGITAL EMPIRES: THE GLOBAL BATTLE TO REGULATE TECHNOLOGY* 7–8 (2023).

¹⁰ Daniel J. Solove, *Privacy Self-Management and the Consent Dilemma*, 126 HARV. L. REV. 1880, 1880–81 (2013) [hereinafter Solove, *Privacy Self-Management*].

Even when individuals refrain from sharing sensitive information—such as health conditions, beliefs, ethnicity, immigration status, or other private matters—AI can infer such details by analyzing seemingly mundane data, like purchasing habits, location history, or online behavior.¹¹ This ability to deduce highly sensitive information from innocuous data renders many self-help measures futile.¹²

Consumer privacy laws fall short of tackling the core challenges of modern data collection and AI-driven inferences, leaving individuals exposed in a system that continues to prioritize the interests of governments and corporations over genuine privacy protections.

This Article proposes regulatory measures that should be taken to address government surveillance and surveillance capitalism—on both sides of the coin—to guard against authoritarianism. Although it is unlikely for the U.S. Supreme Court and Congress to do anything at this point in time, there are still many things that can be done by other governmental entities.

Federal lower court judges have some leeway to strengthen Fourth Amendment and other U.S. Constitutional protections as well as consumer privacy protections. State court judges can interpret their state constitutions in ways that diverge from U.S. Supreme Court interpretations. State legislators can enact measures to limit government surveillance by their own state officials and others as well as to reign in surveillance capitalism, minimize the data available to authoritarian regimes, regulate data brokers, incentivize the creation of less privacy-invasive surveillance technologies, and curtail the increasing government-industrial collusion. States can make a significant difference—sometimes even at a national level. If a few large and powerful states pass such laws, many companies will follow the strictest laws rather than adopt a state-by-state approach. There is no silver bullet, but these measures can make a meaningful difference and at least create pockets of protection and resistance.

This Article proceeds as follows. Part I discusses why authoritarianism is a growing concern, how authoritarian regimes use surveillance as a powerful tool to achieve their aims, why protecting privacy is essential to curtailing the harms of authoritarianism, how the digital age is supercharging the dangers of authoritarian uses of surveillance and personal data, and how surveillance capitalism and government surveillance work in tandem.¹³ Part II discusses measures to regulate government surveillance: from ways judges can interpret the Fourth Amendment and state constitutions, to other constitutional provisions that can

¹¹ Alicia Solow-Niederman, *Information Privacy and the Inference Economy*, 117 NW. U. L. REV. 357, 361–62 (2022).

¹² Daniel J. Solove, *Data Is What Data Does: Regulating Based on Harm and Risk Instead of Sensitive Data*, 118 NW. U. L. REV. 1081, 1099 (2024) [hereinafter Solove, *Data Is What Data Does*].

¹³ See *infra* notes 17–164.

provide protection, to statutory protections at the federal and state levels.¹⁴ Part III proposes ways that surveillance capitalism can be regulated to reign in government surveillance.¹⁵ Part IV discusses other important protections that play a key role in safeguarding privacy in an age of authoritarianism.¹⁶

I. AUTHORITARIANISM AND PRIVACY

Privacy is in deep tension with authoritarianism. To ratchet up their power and stifle resistance, authoritarian governments seek to diminish and eliminate privacy. Authoritarians invade privacy as a means of control, such as surveillance, blackmail, and disclosure of information to threaten, embarrass, or discredit critics or disfavored individuals. Authoritarianism is thus a grave threat to privacy.

On the reverse side, privacy is a potent tool to undermine authoritarianism. Privacy provides safe spaces to harbor dissent and free expression and thinking. Privacy enables people to engage in activities and make decisions about their lives that cut against the orthodoxy of the authoritarian state.

At least three dimensions of privacy are the most common targets of authoritarianism. First is what Neil Richards calls “intellectual privacy,” the “zone of protection that guards our ability to make up our minds freely.”¹⁷ This privacy undergirds freedom of thought and belief; it protects private reading, consumption of ideas, conversations, religious activities, associations, and more. Second is what Danielle Citron terms “intimate privacy,” “the extent to which others have access to, and information about, our bodies; minds (thoughts, desires, and fantasies); health; sex, sexual orientation, and gender; and close relationships.”¹⁸ Third is privacy related to our safety and social status—the information that can put us at risk of physical, psychological, reputational, or financial harm. This information could be as seemingly innocuous as a home address, as it can be used to track us down to commit violence against us or our families.

Section A discusses how and why authoritarianism invades privacy in many ways to enhance its grip on power.¹⁹ Section B details the harms that government surveillance and other authoritarian privacy invasions cause.²⁰ Section C explains how current technologies enhance the dangers of authori-

¹⁴ See *infra* notes 165–266.

¹⁵ See *infra* notes 267–388.

¹⁶ See *infra* notes 389–402.

¹⁷ NEIL RICHARDS, *INTELLECTUAL PRIVACY: RETHINKING CIVIL LIBERTIES IN THE DIGITAL AGE* 95 (2015).

¹⁸ DANIELLE KEATS CITRON, *THE FIGHT FOR PRIVACY: PROTECTING DIGNITY, IDENTITY, AND LOVE IN THE DIGITAL AGE*, at xii (2022) [hereinafter CITRON, *THE FIGHT FOR PRIVACY*].

¹⁹ See *infra* notes 23–40.

²⁰ See *infra* notes 41–107.

tarianism.²¹ Finally, Section D discusses the intersection of authoritarian government and surveillance capitalism.²²

A. Shades of Authoritarianism

In this Part, I discuss some of the dimensions of authoritarianism, the ways in which they are manifesting in the U.S. to at least some degree, the harmful ways that government surveillance is used by authoritarian regimes, and how surveillance contributes to the power of such regimes.

Although authoritarianism throughout history shares many common themes, each instantiation has its own distinctive qualities. The U.S. authoritarianism of today's times is no exception. Beyond risks of centralized federal control, there are other risks due to the deepening political divisions in this country. State governments are diverging rather dramatically, especially on issues such as gender-affirming and reproductive healthcare. The result is not a monolithic authoritarian power but a power struggle in a culture war. What makes authoritarianism in the United States complicated is that it is like a cancer that has spread throughout various dimensions of the country and throughout many governments and their branches. But there still are healthy areas that can resist.

1. Authoritarianism Is Not Necessarily Extra-Legal

Authoritarianism is often carried out under the cloak of the rule of law. Authoritarian governments need not arbitrarily start arresting and punishing people, because they can find ways to do so within the law. They can pass new laws or can enforce existing laws as a pretext for attacking critics or disfavored individuals. In a recent example, Florida Governor Ron DeSantis demanded that state universities provide information on students who sought gender-affirming care at campus clinics.²³ This was done under the governor's authority "to require information in writing from all executive or administrative state, county, or municipal officers upon any subject relating to the duties of their respective offices."²⁴ In a related technique, the attorneys general in Indiana, Missouri, Tennessee, and Texas obtained medical records from healthcare providers of transgender patients under the guise of civil investigations for "mis-

²¹ See *infra* notes 108–137.

²² See *infra* notes 138–164.

²³ Carter Mudgett, *Florida Universities Pivot Again to Supply DeSantis with Records of Gender Affirming Care*, SPINNAKER (Jan. 18, 2023), <https://unfspinnaker.com/99024/news/florida-universities-pivot-again-to-supply-desantis-with-records-of-gender-affirming-care/> [<https://perma.cc/5CUX-KDDS>].

²⁴ Letter from Chris Spencer, Dir., Fla. Governor's Off. of Pol'y & Budget, to Chairs of All State University Board of Trustees (Jan. 11, 2023), <https://drive.google.com/file/d/1jBu1XzRHAYtdSNSMIERpFrXN6EnrK7jd/view> [<https://perma.cc/U6YV-9F7B>].

use of Medicaid funds (Tennessee) or violations of consumer protection laws (Indiana and Missouri).”²⁵

Even a good law can be enforced in non-pretextual ways that are problematic—either through selective enforcement or excessive enforcement. Authoritarians weaponize law enforcement as a tool to achieve their aims, using this potent governmental power in ways that are unfair, in bad faith, and targeted toward their enemies or disfavored people.

The deep moral divide in the U.S. on issues of regulating reproductive healthcare and gender-affirming healthcare presents significant challenges for law enforcement. Typically, for many crimes, such as murder or robbery, there is a general consensus about the wrongfulness of the conduct being criminalized. The debate focuses on the techniques of enforcement or the degree of punishment. But when it comes to healthcare and decisions about one’s body, there is an unbridgeable divide between those who view such decisions as fundamental rights and others who seek to control or prohibit these decisions. In the U.S., because the right to abortion recognized in the U.S. Supreme Court’s 1973 decision in *Roe v. Wade*²⁶ was overturned, in 2022, in *Dobbs v. Jackson Women’s Health Organization*,²⁷ states are attempting to pass laws criminalizing abortion and assisting women in seeking abortions, as well as traveling out of state to seek abortions.²⁸ Enforcing these laws presents a much more fraught set of issues because the stakes are so high, and many view healthcare decisions to be foundational for a free and democratic society, akin to freedom of speech and belief. Laws infringing upon the right to privacy in the U.S. Constitution (despite the right’s not being explicitly mentioned) go far beyond a mere culture war.

Ultimately, authoritarianism often occurs in a contested manner; it takes hold in societies where there are stark differences in opinion. There are typically many people who believe in the authoritarian government’s vision. In most cases, the authoritarian government grows out of the soil of a society and involves one part of that society seeking to impose its will on other parts. What makes it authoritarian are the types of matters the state seeks to control, how

²⁵ STAFF OF S. COMM. ON FIN., HOW STATE ATTORNEYS GENERAL TARGET TRANSGENDER YOUTH AND ADULTS BY WEAPONIZING THE MEDICAID PROGRAM AND THEIR HEALTH OVERSIGHT AUTHORITY 1, 2 (2024), https://www.finance.senate.gov/imo/media/doc/senate_finance_committee_majority_staff_report_how_state_attorneys_general_target_transgender_youth_and_adults_by_weaponizing_the_medicaid_program_and_their_health_oversight_authority.pdf [<https://perma.cc/HP7K-2AKZ>].

²⁶ See generally *Roe v. Wade*, 410 U.S. 113 (1973) (holding that under the U.S. Constitution there is a right to an abortion), *overruled by* *Dobbs v. Jackson Women’s Health Org.*, 597 U.S. 215 (2022).

²⁷ *Dobbs*, 597 U.S. at 300–02.

²⁸ Anna Claire Vollers, *Helping a Minor Travel for an Abortion? Some States Have Made It a Crime*, IDAHO CAPITAL SUN (Aug. 26, 2024), <https://idahocapitalsun.com/2024/08/26/helping-a-minor-travel-for-an-abortion-some-states-have-made-it-a-crime/> [<https://perma.cc/7Z4S-JR2M>].

pervasively and ruthlessly the state seeks to control them, the means the state uses to exercise its power, and the extent to which the state tolerates dissent and deviance from its vision.

It would be much easier to address authoritarian power if it were clearly outside the bounds of the law or if there were a decent test to determine when certain law enforcement becomes soured by authoritarianism. Many efforts at law enforcement are good, even when performed by an authoritarian government. We still want an orderly society with protection against crimes such as murder, sexual assault, robbery, kidnapping, and others. Certain privacy protections can make enforcing laws more difficult, and this can impede desirable law enforcement.

2. Authoritarianism Involves a Large Ensemble

Authoritarianism often is not the product of one monolithic leader. In modern times, Anne Applebaum notes, “autocracies are run not by one bad guy but by sophisticated networks relying on kleptocratic financial structures, a complex of security services—military, paramilitary, police—and technological experts who provide surveillance, propaganda, and disinformation.”²⁹ Authoritarianism often involves a network of politicians, government officials, media entities, thought leaders, and armies of online trolls. This network is fueled by massive funding from wealthy individuals, organizations, and foreign entities. And it is deeply intertwined with many companies that supply the platforms, tools, and technologies to facilitate the authoritarian aims.

All the actors are not motivated in the same way. Many individuals are moved by anger, hate, and grievances. Many other individuals and media companies are interested in advancing various ideological goals. Some are indifferent or are moved by short-term self-interested gains. For the companies facilitating authoritarianism, many might be indifferent or even opposed to the aims of authoritarian leaders, but they see strategic advantages to playing a part. Some might see it as a business opportunity to sell technologies or data to the government. Others might view it as a Machiavellian strategy to cooperate and try to endear themselves to authoritarians in power.

In the end, authoritarianism today in the U.S. is not just one or a few powerful leaders all with a unified aim. Rather, it is large ensemble of actors with different motives who work together as an orchestra in a sinister symphony.

²⁹ ANNE APPLEBAUM, *AUTOCRACY, INC.: THE DICTATORS WHO WANT TO RUN THE WORLD* 1 (2024).

3. Marshaling Individual Collaboration and Vigilantism

Authoritarian regimes marshal not just government power but also the power of individuals to attack each other. Creating a divided populace and a world of distrust is a frequent technique of authoritarian regimes.

Authoritarians can strengthen attacks on disfavored individuals when they can enlist others in society to help ostracize and penalize these individuals. For example, during the McCarthy era attacks on people with suspected Communist sympathies in the U.S., the government's efforts were buttressed by social ruin for these individuals. The FBI leaked data about suspected Communists to companies and the media. Exposed individuals were fired from their jobs and blacklisted from employment.³⁰

Government officials can marshal the assistance of private citizens to identify and target critics and undesirables. In the past, ordinary citizens collaborated with authoritarian regimes to identify, expose, and punish dissenters or disfavored individuals, fueling a culture of fear and repression.

Today, this phenomenon is already occurring. Polarization in the U.S. is increasing,³¹ and online discourse is becoming more extreme and vitriolic. Harassment and threats of violence are rising.³² This activity is stoked by authoritarian politicians as well as allied individuals. Online vigilantes are exploiting personal data to dox, intimidate, or harm people they oppose. For example, right wing attackers have harassed and threatened meteorologists, academics, disinformation experts, election workers, and others.³³

Some state laws encourage private individuals to help police the personal behavior of others. For example, several states have enacted statutes to allow

³⁰ Seth F. Kreimer, *Sunlight, Secrets, and Scarlet Letters: The Tension Between Privacy and Disclosure in Constitutional Law*, 140 U. PA. L. REV. 1, 13–71 (1991) (discussing FBI activity during the red scare); ELLEN SCHRECKER, *THE AGE OF MCCARTHYISM: A BRIEF HISTORY WITH DOCUMENTS* 76–84 (1994) (discussing the effects of red scare data leaks).

³¹ See generally EZRA KLEIN, *WHY WE'RE POLARIZED* (2020) (discussing polarization in the United States); CASS R. SUNSTEIN, *#REPUBLIC: DIVIDED DEMOCRACY IN THE AGE OF SOCIAL MEDIA* (2018) (discussing social media and the increase in polarization in the United States).

³² See generally CITRON, *FIGHT FOR PRIVACY*, *supra* note 18 (discussing the state of online rhetoric and discourse); DANIELLE KEATS CITRON, *HATE CRIMES IN CYBERSPACE* (2014) (explaining the rise of hate crimes on the internet); MARY ANNE FRANKS, *FEARLESS SPEECH: BREAKING FREE FROM THE FIRST AMENDMENT* (2024) (discussing what kinds of speech should and should not be protected in the United States).

³³ Kate Selig, *Meteorologists Face Harassment and Death Threats Amid Hurricane Disinformation*, N.Y. TIMES (Oct. 14, 2024), <https://www.nytimes.com/2024/10/14/us/meteorologists-threats-conspiracy-theories-hurricanes.html> [<https://perma.cc/LPK6-LU73>]; Joshua A. Cuevas, *A New Reality? The Far Right's Use of Cyberharassment Against Academics*, AM. ASS'N UNIV. PROFESSORS (Jan. 1, 2018), <https://www.aaup.org/article/new-reality-far-rights-use-cyberharassment-against-academics> [<https://perma.cc/99F9-B9P5>]; Steven Lee Myers & Sheera Frenkel, *G.O.P. Targets Researchers Who Study Disinformation Ahead of 2024 Election*, N.Y. TIMES (June 19, 2023), <https://www.nytimes.com/2023/06/19/technology/gop-disinformation-researchers-2024-election.html> [<https://perma.cc/RBX4-VUXV>].

people to sue abortion providers and others involved in assisting women who obtain abortions.³⁴ A Texas law allows “[a]ny person, other than an officer or employee of a state or local governmental entity in this state” to initiate a civil action enforcing the law.³⁵ The statute allows suits against people who “aid or abet[]” abortions, “regardless of whether the person knew or should have known that the abortion would be performed or induced.”³⁶ As Aziz Huq and Rebecca Wexler note, the goal of these laws is to buttress criminal law enforcement with “private legal actions and private investigative efforts.”³⁷

Jon Michaels and David Noll observe that the Texas Law (S.B.8):

is merely one example of a broader trend among state legislatures to use private rights of action to penalize and suppress highly personal and often constitutionally protected activities—not only abortions but also LGBTQ+ rights and even the rights of teachers and students to discuss race, gender, and sexual orientation in the classroom.³⁸

They further argue that “state legislatures deputize private actors to wage and win the culture wars by targeting the likes of abortion providers, trans kids, and teachers who adopt inclusive curricula.”³⁹ These efforts can be highly privacy-invasive because they open up civil discovery powers to plaintiffs who can demand extensive personal data about their targets from various businesses and organizations.⁴⁰

B. Why Privacy Is Essential to Resist Authoritarianism

An essential reason why privacy matters—perhaps the most important one—is to guard against authoritarian power. In Europe, the strong commitment to protecting privacy stems in significant part from its tragic history with authoritarianism—the use of personal data by the Nazis to identify Jews and others as well as the oppressive surveillance of the Stasi.⁴¹ If the privacy pro-

³⁴ Aziz Z. Huq & Rebecca Wexler, *Digital Privacy for Reproductive Choice in the Post-Roe Era*, 98 N.Y.U. L. REV. 555, 558 (2023).

³⁵ TEX. HEALTH & SAFETY CODE ANN. § 171.208(a) (West 2021).

³⁶ *Id.*

³⁷ Huq & Wexler, *supra* note 34, at 559.

³⁸ Jon D. Michaels & David L. Noll, *Vigilante Federalism*, 108 CORNELL L. REV. 1187, 1190–91 (2023).

³⁹ *Id.* at 1192.

⁴⁰ See generally Allyson Haynes Stuart, *The Privacy Paradox in Discovery*, 26 VAND. J. ENT. & TECH. L. 615 (2024) (discussing how the discovery process can be used to uncover private information) [hereinafter Stuart, *Privacy Paradox*]; Allyson Haynes Stuart, *Privacy in Discovery After Dobbs*, 26 VA. J.L. & TECH. 3 (2023) (discussing the impact of the Supreme Court’s *Dobbs* decision on the discovery process and privacy) [hereinafter Stuart, *Privacy in Discovery After Dobbs*].

⁴¹ BRADFORD, *supra* note 9, at 112 (discussing Nazi oppression and East German surveillance); Hannah Bloch-Wehba, *Confronting Totalitarianism at Home: The Roots of European Privacy Protec-*

tections in our laws cannot stand up to authoritarianism, then they have flunked their most important test.⁴²

1. Personal Data Is Essential to Power and Control

Privacy is fundamentally about power.⁴³ As Timothy Snyder observes in *On Tyranny*, “We are free only insofar as we exercise control over what people know about us, and in what circumstances they come to know it.”⁴⁴ He further notes: “Whoever can pierce your privacy can humiliate you and disrupt your relationships at will.”⁴⁵ As Neil Richards argues, “Information is power, and information about other people can bring power over those other people.”⁴⁶

Efforts to frighten, discredit, or purge people with disfavored identities or beliefs often involve finding personal data about them—their health, activities, beliefs, location, and more. The government can use surveillance technology and data gathering to find out information about people engaging in research, expression, beliefs, or activities involving these disfavored viewpoints. Another technique is more subtle and bureaucratic, a practice Margaret Hu calls “big data blacklisting”—using data and algorithms to deny people benefits, put them on suspicious persons lists (the No Fly List or Terrorist Watch List), or otherwise deprive them of rights and liberties.⁴⁷

Florida has been especially aggressive in using the power of the government to attack and intimidate opposition and disfavored viewpoints or people. For example, Florida officials engaged in an inquest to investigate people who signed an abortion ballot petition. After being confronted by a law enforcement officer, one signatory said: “The experience left me shaken. What troubled me was he had a folder on me containing my personal information—about 10 pag-

tions, 40 BROOK. J. INT’L L. 749, 751–52 (2015) (discussing the effects of the Nazis on European privacy laws).

⁴² Andrew Ferguson proposes what he terms the “tyrant test” to evaluate whether measures to regulate government surveillance are effective: “presuming the technology will be abused by a metaphorical tyrant, legal and institutional power structures can be developed to limit the potential harms before use.” Andrew Guthrie Ferguson, *Surveillance and the Tyrant Test*, 110 GEO. L.J. 205, 214 (2021).

⁴³ See generally Daniel J. Solove, *Privacy and Power: Computer Databases and Metaphors for Information Privacy*, 53 STAN. L. REV. 1393 (2001) (discussing the importance of privacy in political power); DANIEL J. SOLOVE, ON PRIVACY AND TECHNOLOGY (2025) (explaining the importance of privacy); CARISSA VÉLIZ, PRIVACY IS POWER: WHY AND HOW YOU SHOULD TAKE BACK CONTROL OF YOUR DATA (2021) (discussing why privacy matters and what can be done to claw back our privacy from big tech and the government).

⁴⁴ TIMOTHY SNYDER, ON TYRANNY: TWENTY LESSONS FROM THE TWENTIETH CENTURY 88 (2017).

⁴⁵ *Id.*

⁴⁶ NEIL RICHARDS, WHY PRIVACY MATTERS 39 (2022).

⁴⁷ Margaret Hu, *Big Data Blacklisting*, 67 FLA. L. REV. 1735, 1737–44 (2015).

es.”⁴⁸ Additionally, Florida tried to revoke liquor licenses of restaurants, hotels, and businesses that allowed children to attend drag shows.⁴⁹ In 2022, DeSantis established an office to prosecute election fraud, despite scant evidence of such fraud. Many criminal cases have been thrown out by judges.⁵⁰ But the damage is done, and this is the goal; the strategy is to scare people and deter them from voting.

In late 2024, following statements by Donald Trump about purging the ranks of federal agencies, many federal employees feared that their personal data online would be scoured and scrutinized to identify their views.⁵¹ For example, a National Weather Service meteorologist deleted social media posts about climate change.⁵² At the Energy Department, scientists removed their names from projects where the science is likely to be disfavored by the Administration.⁵³ Beyond personal data in employee records and online social media, data about people’s beliefs about science, health, vaccines, climate change, and other topics can readily be plucked from web browsing histories, bookstores, and other sites and services.

The first Trump Administration gathered personal data in response to media stories. For example, in 2017, the Justice Department seized phone records of several journalists for a leak investigation.⁵⁴ The U.S. government also tracked journalists and immigration advocates, constructing a secret database with information about them.⁵⁵

For his second administration, Trump has declared that he will engage in the largest mass deportation in U.S. history.⁵⁶ Personal data and surveillance is

⁴⁸ Sam Levine, *Florida Officials Investigate Voters Who Signed Abortion Ballot Initiative*, THE GUARDIAN (Sep. 13, 2024), <https://www.theguardian.com/us-news/2024/sep/13/florida-abortion-petition-investigation> [https://perma.cc/Q9SP-Y75T].

⁴⁹ Patricia Mazzei, *How Ron DeSantis Maximized the Power of the Florida Governor’s Office*, N.Y. TIMES (May 24, 2023), <https://www.nytimes.com/2023/05/24/us/politics/ron-desantis-florida-governor-power.html> [https://perma.cc/C4UC-BQ25].

⁵⁰ *Id.*

⁵¹ Lisa Rein & Jeff Stein, *Federal Employees Scramble to Insulate Themselves from Trump’s Purge*, WASH. POST. (Dec. 8, 2024), <https://www.washingtonpost.com/politics/2024/12/08/federal-employees-trump-fear-purge/> [https://perma.cc/6HBE-PF29].

⁵² *Id.*

⁵³ *Id.*

⁵⁴ Charlie Savage & Katie Benner, *Trump Administration Secretly Seized Phone Records of Times Reporters*, N.Y. TIMES (June 11, 2021), <https://www.nytimes.com/2021/06/02/us/trump-administration-phone-records-times-reporters.html> [https://perma.cc/PCB8-Q3DZ].

⁵⁵ Tom Jones, Mari Payton & Bill Feather, *Source: Leaked Documents Show the U.S. Government Tracking Journalists and Immigration Advocates Through a Secret Database*, NBC7 SAN DIEGO, <https://www.nbcsandiego.com/news/local/source-leaked-documents-show-the-us-government-tracking-journalists-and-advocates-through-a-secret-database/3438/> [https://perma.cc/RZB4-L24N] (Jan. 10, 2020).

⁵⁶ Ted Hesson, *Trump Aims to Deport All Immigrants in the US Illegally*, REUTERS (Dec. 9, 2024), <https://www.reuters.com/world/us/trump-says-he-aims-deport-all-immigrants-us-illegally-2024-12-08/> [https://perma.cc/D7MA-7D5Y]; Kristen Welker & Alexander Marquez, *Trump Says There’s ‘No*

key to locating these individuals.⁵⁷ The personal data of over seventy-nine million Medicaid enrollees, including their addresses and ethnicities, has been handed over to Immigration and Customs Enforcement (ICE) to track down immigrants.⁵⁸ The Administration may revive an idea proposed by Trump during his first presidential campaign in 2014, when he suggested he may implement a national registry of Muslims if elected.⁵⁹ The registry would require immigrants from Muslim-majority countries to register in a database to make vetting and tracking easier for law enforcement. Trump once noted that a “database is okay, and watch list is okay, and surveillance is okay.”⁶⁰

Beginning in the early days of the second Trump Administration, the newly formed Department of Government Efficiency (DOGE) has engaged in massive data gathering. DOGE gained access to databases held by the Internal Revenue Service (IRS), Social Security Administration (SSA), Center for Medicaid and Medicare Services (CMS), Department of Veterans Affairs (VA), and the Consumer Financial Protection Bureau (CFPB).⁶¹ It obtained data on hundreds of millions of Americans, including names, addresses, Social Security Numbers, financial information, marital status, family relationships, and health information on tens of millions of Americans.⁶² DOGE has provided hardly any transparency about its activities and purposes; it has failed to state what data it has obtained, how the data will be used, or how long the data will be retained.

Beyond DOGE, the IRS hired Palantir, a data analytics company, to create a single searchable “mega-database” of taxpayer records, a move that some

Price Tag’ for His Mass Deportation Plan, NBC NEWS (Nov. 7, 2024), <https://www.nbcnews.com/politics/2024-election/trump-says-no-price-tag-mass-deportation-plan-rcna179178> [<https://perma.cc/DPB5-GTK3>].

⁵⁷ See generally PETRA MOLNAR, *THE WALLS HAVE EYES: SURVIVING MIGRATION IN THE AGE OF ARTIFICIAL INTELLIGENCE* (2024) (describing the extensive data gathering and surveillance apparatus to control immigration).

⁵⁸ Kimberly Kindy & Amanda Seitz, *Trump Administration Hands Over Medicaid Recipients’ Personal Data, Including Addresses, to ICE*, AP NEWS (July 17, 2025), <https://apnews.com/article/immigration-medicaid-trump-ice-ab9c2267ce596089410387bfc40eeb7> [<https://perma.cc/EH7K-RP4F>].

⁵⁹ Trip Gabriel, *Donald Trump Says He’d ‘Absolutely’ Require Muslims to Register*, N.Y. TIMES (Nov. 20, 2015), <https://archive.nytimes.com/www.nytimes.com/politics/first-draft/2015/11/20/donald-trump-says-hed-absolutely-require-muslims-to-register/> [<https://perma.cc/5C5K-QY7K>].

⁶⁰ Aaron Blake, *Trump Says We’ve Known His Muslim Ban and Database Plans ‘All Along.’ But We Still Don’t—Not Really.*, WASH. POST (Dec. 21, 2016), <https://www.washingtonpost.com/news/the-fix/wp/2016/11/17/the-evolution-of-donald-trump-and-the-muslim-database/> [<https://perma.cc/83YG-BNN4>].

⁶¹ Laurel Wamsley, *The Government Already Knows a Lot About You. DOGE Is Trying to Access All of It*, NPR (Mar. 11, 2025), <https://www.npr.org/2025/03/11/nx-s1-5305054/doge-elon-musk-security-data-information-privacy> [<https://perma.cc/H7A8-6A85>].

⁶² Allison Stanger et al., *Understanding DOGE and Your Data*, ASH CTR. FOR DEM. GOV. & INNOVATION (Mar. 31, 2025), <https://ash.harvard.edu/resources/understanding-doge-and-your-data/> [<https://perma.cc/GYT9-LQV9>].

Congresspeople have decried as a “surveillance nightmare.”⁶³ Several other agencies are moving to use Palantir for analytics on their data in order to more aggressively share and use data.⁶⁴

Various measures being passed in the states or proposed at the federal level will involve gathering personal data to enforce. States are attempting to criminalize helping women travel out of state to obtain an abortion.⁶⁵ Enforcing such laws will depend upon gathering data such as location data and online browsing and research.⁶⁶ In one instance, Senator Ron Wyden accused a company of tracking people’s visits to hundreds of Planned Parenthood clinics to provide data for an anti-abortion group to target ads to them.⁶⁷ In another instance, in 2022, Nebraska police obtained a warrant to search Facebook messages between a mother and daughter to investigate whether a stillbirth was the result of a miscarriage or an abortion.⁶⁸

For all these endeavors to root out or attack people with particular views, to stop people from seeking healthcare in another state or receiving medication in the mail, and to round up groups of people for deportation or imprisonment, personal data will likely be one of the most powerful tools in the authoritarian’s tool kit.

2. The Harms of Government Surveillance and Authoritarian Privacy Invasions

Government surveillance is harmful because it fuels authoritarian power and enables authoritarian techniques such as blackmail, round ups, manipulation, embarrassment and discrediting of critics, threats, investigations, inquests, and arrests.

⁶³ Letter from Ron Wyden, Elizabeth Warren & Jeffrey Merlkey, Senators & Alexandria Ocasio-Cortez, James McGovern & Sara Jacobs, Members of Congress to Alex Karp, CEO, Palantir (June 17, 2025), https://www.finance.senate.gov/imo/media/doc/wyden_aoc_palantir_letter_061725.pdf [<https://perma.cc/Z9SU-WNS7>].

⁶⁴ Sheera Frenkel & Aaron Krolik, *Trump Taps Palantir to Compile Data on Americans*, N.Y. TIMES (May 30, 2025), <https://www.nytimes.com/2025/05/30/technology/trump-palantir-data-americans.html> [<https://perma.cc/SZ9K-VY6P>].

⁶⁵ *Idaho Governor Signs ‘Abortion Trafficking’ Bill into Law*, AP NEWS (Apr. 6, 2023), <https://apnews.com/article/idaho-abortion-minors-criminalization-b8fb4b6feb9b520d63f75432a1219588> [<https://perma.cc/7EX5-MEY4>].

⁶⁶ See Jolynn Dellinger & Stephanie Pell, *Bodies of Evidence: The Criminalization of Abortion and Surveillance of Women in a Post-Dobbs World*, 19 DUKE J. CONST. L. & PUB. POL’Y 1, 73–87 (2024) (discussing examples of how personal data can be gathered to enforce anti-abortion laws).

⁶⁷ Alfred Ng, *A Company Tracked Visits to 600 Planned Parenthood Locations for Anti-Abortion Ads, Senator Says*, POLITICO (Feb. 13, 2024), <https://www.politico.com/news/2024/02/13/planned-parenthood-location-track-abortion-ads-00141172> [<https://perma.cc/BUH9-JZPY>].

⁶⁸ Martin Kaste, *Nebraska Cops Used Facebook Messages to Investigate an Illegal Abortion*, NPR (Aug. 12, 2022), <https://www.npr.org/2022/08/12/1117092169/nebraska-cops-used-facebook-messages-to-investigate-an-alleged-illegal-abortion> [<https://perma.cc/5XZW-HXCH>].

Punishment and Oppression. Government surveillance can be a prelude to the punishment of expression, association, and consumption of ideas. As Paul Schwartz observes:

Through the use of their data banks, the state and private organizations can transform themselves into omnipotent parents and the rest of society into helpless children. Indeed, totalitarian regimes in Eastern Europe relied on information gathering and data storage to weaken the individual capacity for critical reflection and to repress any social movements outside their control.⁶⁹

Chilling Effects. Beyond direct punishment, government surveillance chills certain disfavored intellectual activities.⁷⁰ People become discouraged and afraid to engage in these activities. As Julie Cohen argues, “[p]ervasive monitoring” can not only “chill the expression of eccentric individuality” but also “dampen” even the desire to be unique.⁷¹ As Jonathon Penney aptly observes, “chilling effects predominantly involve not just a deterrent effect, but a shaping effect—people speaking, acting, or doing, in a way that conforms to, or is in compliance with, a perceived social norm, not simply self-censoring to avoid a legal harm.”⁷²

Suppressing Viewpoints and Dissent. The FBI has a long history of monitoring dissidents, such as anti-war activists, the Black Panther Party, Communists, and others. During the McCarthy era and into the 1980s, the FBI sought information from libraries about individuals’ reading habits, attempting to link their intellectual interests to subversive activities or ideologies.⁷³ These practices demonstrate a troubling pattern of leveraging personal information to suppress dissent and stigmatize individuals engaged in political or social advocacy.

Attacking and Discrediting Critics. Authoritarians use personal data to attack critics or anyone who stands in their way. For example, during the first Trump Administration, Trump disclosed details of private text messages of FBI

⁶⁹ Paul M. Schwartz, *Privacy and Participation: Personal Information and Public Sector Regulation in the United States*, 80 IOWA L. REV. 553, 560 (1995).

⁷⁰ Daniel J. Solove, *The First Amendment as Criminal Procedure*, 82 N.Y.U. L. REV. 112, 154 (2007) (discussing the impact of government action); Neil M. Richards, *The Dangers of Surveillance*, 126 HARV. L. REV. 1934, 1964 (2013) (discussing the harms of surveillance on intellectual pursuits); Jonathon W. Penney, *Understanding Chilling Effects*, 106 MINN. L. REV. 1451, 1453 (2022) (corporate and state surveillance chill exercises of rights). See generally Frederick Schauer, *Fear, Risk, and the First Amendment: Unraveling the “Chilling Effect,”* 58 B.U. L. REV. 685 (1978) (discussing the chilling effect of potential consequences for speech); NEIL RICHARDS, *supra* note 17 (discussing the connection between free speech and privacy).

⁷¹ Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 STAN. L. REV. 1373, 1426 (2000).

⁷² Penney, *supra* note 70, at 1455.

⁷³ WHITFIELD DIFFIE & SUSAN LANDAU, *PRIVACY ON THE LINE: THE POLITICS OF WIRETAPPING AND ENCRYPTION* 146 (1999).

agents who were having an extramarital affair to attack them for not pursuing Hillary Clinton.⁷⁴

Curtailling Freedom of the Press. Authoritarian regimes often crack down on the media in various ways.⁷⁵ Through the use of privacy-invasive surveillance or investigative powers (such subpoenas or court orders), authoritarian governments can obtain information to reveal confidential sources or journalists can be forced to divulge their sources. Media communications can be surveilled. These techniques undermine the ability of the media to shine light on the government.⁷⁶

Thought Control. Many authoritarians do not only want people to obey; they also want people to like it. As Orwell aptly demonstrated in *Nineteen Eighty-Four*, the book ends with Winston loving Big Brother.⁷⁷ Authoritarianism might start with efforts to stifle publicly-expressed viewpoints, but the next step often is to dive deeper into private thought and belief.

Obedience and Conformity. Foucault warned that surveillance was constructing a Panoptic society, one where everyone is under the constant watchful eye.⁷⁸ The ruthless efficiency of the Panopticon is that people internalize discipline; they no longer need to be forced to obey. As Margot Kaminski and Shane Witnov aptly point out, surveillance “discourages individuals with unformed ideas from deviating from majority political views” and “encourages individuals to follow what they think others expect of them and conform to perceived norms instead of engaging in unhampered self-development.”⁷⁹

Individual and Societal Shaping and Manipulation. Personal data can be used to shape individuals as well as society. As Julie Cohen notes, privacy is essential for human flourishing and growth; the self is dynamic, not static.⁸⁰ Online platforms do not just reflect people’s thoughts, expression, and behavior. With powerful algorithms, the platforms shape and manipulate what people

⁷⁴ CITRON, FIGHT FOR PRIVACY, *supra* note 18, at 51–52.

⁷⁵ Matthew Dalton & Jack Gillum, *Authoritarians Threaten Journalists Around the Globe*, WALL ST. J. (Mar. 29, 2024), <https://www.wsj.com/world/authoritarians-threaten-journalists-around-the-globe-38cda1d7> [<https://perma.cc/HA7W-8MNC>].

⁷⁶ See generally Peter Swire, *Privacy and Democracy: Protecting Journalists and the Political Opposition from Abuse of Power* (discussing the importance of protecting privacy of journalists and political opposition to prevent authoritarianism), in *PRIVACY AND DEMOCRACY* (Sebastian Ziegler, ed.) (forthcoming).

⁷⁷ See generally GEORGE ORWELL, *NINETEEN EIGHTY-FOUR* (1949) (discussing the goals of authoritarian regimes through the book’s ending).

⁷⁸ DANIEL J. SOLOVE, ON PRIVACY AND TECHNOLOGY 66–67 (forthcoming 2025). See generally MICHEL FOUCAULT, *DISCIPLINE AND PUNISH: THE BIRTH OF THE PRISON* (Alan Sheridan trans., Vintage Books 2d ed. 1995) (1975) (discussing the effects of surveillance on society).

⁷⁹ Margot E. Kaminski & Shane Witnov, *The Conforming Effect: First Amendment Implications of Surveillance, Beyond Chilling Speech*, 49 U. RICH. L. REV. 465, 467 (2015).

⁸⁰ Julie E. Cohen, *What Privacy Is For*, 126 HARV. L. REV. 1904, 1909–11 (2013).

think and say.⁸¹ Cohen notes how the “harvesting of personal data has engendered new patterns of reputational anxiety, manipulation, and insecurity” that deepen social divisions, promote “conspiracy theories and junk science,” and amplify “toxic currents of bigotry, nationalism, and ideological extremism.”⁸² These are precisely the sentiments authoritarians want to stoke in individuals and foster broadly in society.

Identification and Rounding Up of Disfavored People. Authoritarian regimes have used technology and personal data to round up people for imprisonment and elimination. Pamela Samuelson writes: “One factor that enabled the Nazis to efficiently round up, transport, and seize assets of Jews (and others they viewed as ‘undesirables’) was the extensive repositories of personal data available not only from the public sector but also from private sector sources.”⁸³ As Josef Ansorge notes: “Before anybody can be disciplined and punished they need to be identified and sorted. Lists are made. Individuals have to be recognised, placed into a hierarchical relation, and aggregated into groups.”⁸⁴

It takes more than mere personal data to facilitate certain authoritarian efforts, such as rounding up people. Technology is also required. The Nazis benefited from private-sector technology to process personal data. IBM’s punch-card machines were used to aid the Nazis in locating and rounding up Jews during the Holocaust.⁸⁵

In the U.S., government information-gathering played a critical role in facilitating the roundup and internment of disfavored groups, including Japanese Americans during World War II. Following the bombing of Pearl Harbor on December 7, 1941, the FBI imprisoned thousands of Japanese American community leaders. These initial roundups were enabled by a Justice Department index of potentially “subversive” individuals of Japanese descent, a list that had been compiled since the late 1930s.⁸⁶ Then, in 1942, under the pretext of national security, approximately 120,000 people of Japanese descent—most of whom were American citizens or lawful residents—were seized and confined in internment camps. The Census Bureau played a significant role in this ef-

⁸¹ JULIE E. COHEN, BETWEEN TRUTH AND POWER: THE LEGAL CONSTRUCTIONS OF INFORMATIONAL CAPITALISM 76–77 (2019) (discussing the impact of data algorithms on people’s actions) [hereinafter COHEN, BETWEEN TRUTH AND POWER]; MIREILLE HILDEBRANDT, SMART TECHNOLOGIES AND THE END(S) OF LAW: NOVEL ENTANGLEMENTS OF LAW AND TECHNOLOGY 41–67 (2015) (explaining the impact of algorithms on user’s thoughts and actions).

⁸² COHEN, BETWEEN TRUTH AND POWER, *supra* note 81, at 76.

⁸³ Pamela Samuelson, *Privacy as Intellectual Property?*, 52 STAN. L. REV. 1125, 1143 (2000).

⁸⁴ JOSEF TEBOHO, IDENTIFY AND SORT: HOW DIGITAL POWER CHANGED WORLD POLITICS 1 (2016).

⁸⁵ BLACK, *supra* note 7, at 19–21.

⁸⁶ ERIC. K. YAMAMOTO ET AL., RACE, RIGHTS, AND REPARATIONS: LAW AND THE JAPANESE AMERICAN INTERNMENT 96 (2001).

fort, producing special tabulations of Japanese Americans to assist in the government's relocation plan.⁸⁷ This dark chapter illustrates how government data collection can be weaponized to target specific groups, leading to widespread violations of civil liberties.

Data Security Vulnerabilities and Violations. Because authoritarian regimes often lack accountability and have little concern for the individuals whose data has been gathered, precautions to reduce security risks are often ignored. For example, the chief data officer of the SSA, Charles Borges, has stated that DOGE uploaded the personal data of over three hundred million Americans to a vulnerable and private cloud server.⁸⁸ Prior to storing the data, there was a security assessment of the server which described it as “high-risk” and capable of “catastrophic impact.”⁸⁹ Massive aggregations of personal data create significant risks to data security because they are especially attractive to hackers and bad actors who covet big payloads.

Purging and Blacklisting “Undesirables” from Employment. In several instances in U.S. history, efforts were made to fire disfavored individuals from federal employment as well as private-sector employment. During various “Red Scares” in the twentieth century, people with Communist beliefs were not only expelled from employment in the federal government but also blacklisted from private-sector employment, especially the entertainment industry.⁹⁰ In 1953, President Eisenhower issued an Executive Order mandating that federal employees be investigated for “sexual perversion” and “mental illness.”⁹¹ This launched government surveillance and investigations of LGBTQ+ individuals, known as the “Lavender Scare.”⁹² More than 10,000 civil servants lost their jobs, with some employees dismissed solely for associating with individuals accused of being LGBTQ+. ⁹³

Eliminating Obscurity and Anonymity. Obscurity in public places is a key component of freedom. Joel Reidenberg argues that “constitutional democ-

⁸⁷ DIFFIE & LANDAU, *supra* note 73, at 138.

⁸⁸ Nicholas Nehamas, *DOGE Put Critical Social Security Data at Risk, Whistle-Blower Says*, N.Y. TIMES (Aug. 26, 2025), <https://www.nytimes.com/2025/08/26/us/politics/doge-social-security-data.html> [<https://perma.cc/A9BB-5QL9>].

⁸⁹ Julia Jester, *DOGE Put Social Security Numbers and Other Data on a Risky Server, Whistle-blower Alleges*, NBC NEWS (Aug. 26, 2025), <https://www.nbcnews.com/politics/doge/doge-put-social-security-numbers-data-risky-server-whistleblower-alleg-rcna227259> [<https://perma.cc/5WKR-R33B>].

⁹⁰ History.com Editors, *Red Scare*, <https://www.history.com/topics/cold-war/red-scare> [<https://perma.cc/JG22-WSXB>] (Oct. 16, 2025). For more background on the Red Scares, see Laura K. Donohue, *Anglo-American Privacy and Surveillance*, 96 J. CRIM. L. & CRIMINOLOGY 1059, 1073–77 (2006).

⁹¹ Exec. Order No. 10450, 18 Fed. Reg. 2489 (Apr. 27, 1953); Katelyn Ringrose, *A Look Back at the Role of Law and the Right to Privacy in LGBTQ+ History*, FUTURE OF PRIV. F. (Oct. 22, 2020), <https://fpf.org/blog/a-look-back-at-the-role-of-law-and-the-right-to-privacy-in-lgbtq-history/> [<https://perma.cc/AU3L-QE5X>].

⁹² Ringrose, *supra* note 91.

⁹³ *Id.*

racy depends on spheres of privacy in public to preserve public safety and fair governance.”⁹⁴ People generally expect obscurity and anonymity in their everyday activities.⁹⁵ Living under the constant watchful eye places us in an Orwellian world where Big Brother is always observing. Even if it does not directly chill activities such as reading or protesting, it can blunt what is said or done. It adds an element of fear; and it also enables far greater government control. Public surveillance makes people feel less free; it impedes their free expression of selfhood.⁹⁶ Facial recognition systems even more dramatically undermine obscurity. As Woodrow Hartzog and Evan Selinger write, “facial recognition is the perfect tool for oppression.”⁹⁷ Beyond everyday obscurity, the ability to communicate and consume ideas anonymously is an essential component of a free society.⁹⁸

Pretextual Law Enforcement. A powerful tool in the authoritarian’s playbook is to use pretextual law enforcement against people. In today’s world of extensive criminalization, a crime can nearly always be found.⁹⁹ According to the National Association of Criminal Defense Lawyers, there are more than “4,450 crimes scattered throughout the federal criminal code”¹⁰⁰ and even more state crimes. With all these crimes, it is relatively easy for authoritarian governments to find pretextual bases to prosecute disfavored individuals and critics.

Blackmail and Control. Authoritarian officials can use government surveillance to obtain discreditable or embarrassing personal data and then use it to blackmail and control people. This technique was frequently used by J. Edgar Hoover who amassed dossiers about countless politicians, presidents, and Supreme Court justices.¹⁰¹ Hoover’s files of dirt and skeletons may have

⁹⁴ Joel R. Reidenberg, *Privacy in Public*, 69 U. MIA. L. REV. 141, 143 (2014).

⁹⁵ Helen Nissenbaum, *Toward an Approach to Privacy in Public: Challenges of Information Technology*, 7 ETHICS & BEHAV. 207, 208 (1997); Daniel J. Solove & Woodrow Hartzog, *The Great Scrape: The Clash Between AI Scraping and Privacy*, 113 CALIF. L. REV. 1521 (2025). See generally Woodrow Hartzog, *The Public Information Fallacy*, 99 B.U. L. REV. 459 (2019) (discussing the inadequacy of having privacy not apply in the public sphere).

⁹⁶ Andrew E. Taslitz, *The Fourth Amendment in the Twenty-First Century: Technology, Privacy, and Human Emotions*, 65 LAW & CONTEMP. PROBS. 125, 171–72 (2002) (explaining how people act under public surveillance); Christopher Slobogin, *Public Privacy: Camera Surveillance of Public Places and the Right to Anonymity*, 72 MISS. L.J. 213, 264–67 (2002) (privacy is tied to self expression).

⁹⁷ Woodrow Hartzog & Evan Selinger, *Facial Recognition Is the Perfect Tool for Oppression*, MEDIUM (Aug. 2, 2018), <https://medium.com/@hartzog/facial-recognition-is-the-perfect-tool-for-oppression-bc2a08f0fe66> [<https://perma.cc/5R8P-HQWN>]; see also Lindsey Barrett, *Ban Facial Recognition Technologies for Children—and for Everyone Else*, 26 B.U. J. SCI. & TECH. L. 223 (2020) (discussing facial recognition technology).

⁹⁸ Julie E. Cohen, *A Right to Read Anonymously: A Closer Look at “Copyright Management” in Cyberspace*, 28 CONN. L. REV. 981, 1012 (1996) (discussing the value of anonymous reading).

⁹⁹ See generally HARVEY A. SILVERGLATE, *THREE FELONIES A DAY: HOW THE FEDS TARGET THE INNOCENT* (2011) (discussing the impact of surveillance on criminal prosecution).

¹⁰⁰ Nat’l Ass’n of Crim. Def. Laws., *Overcriminalization*, <https://www.nacdl.org/Landing/Overcriminalization> [<https://perma.cc/3CLU-YRTF>].

¹⁰¹ CURT GENTRY, J. EDGAR HOOVER: THE MAN AND THE SECRETS 118 (1991).

helped him stay in power as head of the FBI for decades. The FBI once threatened to release surveillance recordings of Martin Luther King, Jr.'s extramarital affair unless he committed suicide.¹⁰²

Perpetuating Inequality. Surveillance often has disproportionate effects on marginalized groups.¹⁰³ Authoritarian regimes may deliberately seek to increase negative views about certain groups and stoke the flames of hatred. Surveillance can serve as a tool toward this end; the more surveillance, the more likely criminal activity can be found that can then be used to confirm and increase people's bias against these groups. Beyond disproportionate law enforcement targeting, government surveillance oppresses marginalized groups.¹⁰⁴ As Alvaro Bedoya observes, surveillance often is used as "a tool to stop marginalized people from achieving power."¹⁰⁵

Dragnets. The Framers of the U.S. Constitution detested dragnets for a good reason; dragnets are a tool of tremendous authoritarian power. The most despised searches were conducted with *general warrants*, which authorized the British government to conduct sweeping searches for evidence of a crime without particularized suspicion.¹⁰⁶ As Patrick Henry declared: "They may, unless the general government be restrained by a bill of rights, or some similar restrictions, go into your cellars and rooms, and search, ransack, and measure, eve-

¹⁰² DAVID J. GARROW, *THE FBI AND MARTIN LUTHER KING, JR.: FROM "SOLO" TO MEMPHIS* 100–26 (1980).

¹⁰³ Barry Friedman, *Lawless Surveillance*, 97 N.Y.U. L. REV. 1143, 1157–58 (2022) (explaining that the effects of surveillance are stratified on racial and class grounds); Rashida Richardson, Jason M. Schultz & Kate Crawford, *Dirty Data, Bad Predictions: How Civil Rights Violations Impact Police Data, Predictive Policing Systems, and Justice*, 94 N.Y.U. L. REV. ONLINE 15, 18 (2019), https://nyulawreview.org/wp-content/uploads/2019/04/NYULawReview-94-Richardson_et al-FIN.pdf [<https://perma.cc/B452-W9VV>] (biased data leads to algorithms producing biased results); Laura M. Moy, *A Taxonomy of Police Technology's Racial Inequity Problems*, 2021 U. ILL. L. REV. 139, 144 (explaining how surveillance technology effects people of color); Sandra G. Mayson, *Bias In, Bias Out*, 128 YALE L.J. 2218, 2251 (2019) (explaining how racial disparity cannot be eliminated in the data); Chaz Arnett, *Black Lives Monitored*, 69 UCLA L. REV. 1384, 1388 (2023) (discussing excessive surveillance of Black Lives Matter protests); Mary Anne Franks, *Democratic Surveillance*, 30 HARV. J.L. & TECH. 425, 441 (2017) (explaining the historical effects of surveillance on the marginalized); Anita L. Allen, *Dismantling the "Black Opticon": Privacy, Race, Equity, and Online Data-Protection Reform*, YALE L.J.F. 907, 907 (2022), <https://yalelawjournal.org/essay/dismantling-the-black-opticon> [<https://perma.cc/6QNJ-Y95H>] (explaining the vulnerabilities of African Americans in surveillance). See generally SIMONE BROWNE, *DARK MATTERS: ON THE SURVEILLANCE OF BLACKNESS* (2015) (discussing surveillance in the context of experience of black people in the United States).

¹⁰⁴ See generally KHIARA M. BRIDGES, *THE POVERTY OF PRIVACY RIGHTS* (2017) (discussing the impact of government surveillance).

¹⁰⁵ Alvaro M. Bedoya, *Privacy as Civil Right*, 50 N.M. L. REV. 301, 306 (2020).

¹⁰⁶ See LEONARD W. LEVY, *ORIGINS OF THE BILL OF RIGHTS* 158 (1999) (explaining the hatred of general warrants); Tracey Maclin, *When the Cure for the Fourth Amendment Is Worse Than the Disease*, 68 S. CAL. L. REV. 1, 9 (1994) (discussing the framers' opinions on general warrants).

rything you eat, drink, and wear. They ought to be restrained within proper bounds.”¹⁰⁷

C. The Dangers of the Digital Age and AI

The power available to authoritarian officials is significantly greater today than in prior decades because there is much more data. The government can seek personal information contained in records maintained by third parties, as these records can reveal a vast array of intimate details about an individual’s life. From various sources, the government can piece together a comprehensive profile about a person—which I’ve referred to as a “digital dossier.”¹⁰⁸ By using AI and algorithms, inferences about people can be gleaned far beyond what is immediately apparent.

1. Data and Digital Dossiers

We are enveloped by pervasive surveillance and data gathering.¹⁰⁹ As Bruce Schneier aptly observes, “[d]ata is the exhaust of the information age.”¹¹⁰ It is impossible to live without generating extensive data about nearly everything one does. Data involving our intellectual and intimate activities is being collected every second and stored in gigantic databases by companies eager to exploit it for a profit. Personal data is bought and sold between companies in an underworld bazaar, a practice that has been going on for decades.¹¹¹

Health data can be found in traditional places, such as in healthcare provider records, health insurance records, and pharmacy records. But health data can also be found in many other places. People are using wearable health devices and fitness devices that monitor their health conditions and bodily functions as well as track their movement.¹¹² Many apps and websites collect data

¹⁰⁷ 3 THE DEBATES IN SEVERAL CONVENTIONS ON THE ADOPTION OF THE FEDERAL CONSTITUTION 448–49 (Jonathan Elliot ed., 1974).

¹⁰⁸ See generally Solove, *Digital Dossiers*, *supra* note 4.

¹⁰⁹ Christopher Slobogin, *Transaction Surveillance by the Government*, 75 MISS. L.J. 139, 139 (2005) (explaining how much information law enforcement can access). See generally BYRON TAU, MEANS OF CONTROL: HOW THE HIDDEN ALLIANCE OF TECH AND GOVERNMENT IS CREATING A NEW AMERICAN SURVEILLANCE STATE (2024) (discussing how the government circumvents prohibitions on surveillance).

¹¹⁰ BRUCE SCHNEIER, DATA AND GOLIATH: THE HIDDEN BATTLES TO COLLECT YOUR DATA AND CONTROL YOUR WORLD 17 (2015).

¹¹¹ DANIEL SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE 19 (2004) (discussing the market for personal data) [hereinafter SOLOVE, THE DIGITAL PERSON]; Christopher Slobogin, *Government Data Mining and the Fourth Amendment*, 75 U. CHI. L. REV. 317, 322 (2008) (discussing private data markets); Chris Jay Hoofnagle, *Big Brother’s Little Helpers: How ChoicePoint and Other Commercial Data Brokers Collect and Package Your Data for Law Enforcement*, 29 N.C. J. INT’L L. & COM. REGUL. 595, 600 (2004) (discussing a company that sells data); Donohue, *supra* note 90, at 1142 (detailing the private data market).

¹¹² CITRON, THE FIGHT FOR PRIVACY, *supra* note 18, at 1–6.

about menstruation and sexual activity.¹¹³ Many fertility and period apps collect data about birth control, menstrual cycle, pregnancy, and geolocation.¹¹⁴ A *Consumer Reports* study revealed that many period tracking apps had hardly any privacy protections.¹¹⁵

Financial data can reveal a person's financial habits, including payments made to specific businesses or professionals, such as subscription services, doctors, attorneys, or other vendors. Credit card company records can disclose where a person shops, dines, and which cultural or entertainment events they attend.

Travel data can expose a person's travel history, including destinations, itineraries, and accommodations. Lodging data can reveal where a person stayed, the pay-per-view content they accessed, and even patterns of travel and lodging preferences. Rental car companies may provide details of trips. Increasingly, cars are vectors of intensive surveillance. When a man exploded his Tesla truck in front of the Trump International Hotel, Tesla was able to provide law enforcement officials with extensive information, such as video from a Tesla charging station. One reporter wrote that Tesla has the "ability to track users at every point along a journey" and that car companies "can now insert themselves into every moment of a person's driving experience, while also providing private information to law enforcement."¹¹⁶

Media and entertainment records can reveal insights into a person's interests and beliefs. Cable companies and video streaming services can supply information about an individual's viewing history. Data from social media and online activity reveal a plethora of details about a person. Platforms like Facebook, Twitter, or Google maintain detailed logs of online interactions, locations visited, and interests based on searches, likes, and posts.

Personal data also exists in the vast warehouses of data brokers. Danielle Citron notes that there are "more than 4,000 data brokers . . . with dossiers on 98% of Americans."¹¹⁷ The largest data broker, Acxiom, has "more than 10,000 data attributes on over 2.5 billion people in more than sixty coun-

¹¹³ Kayte Spector-Bagdady & Michelle M. Mello, *Protecting the Privacy of Reproductive Health Information After the Fall of Roe v. Wade*, JAMA HEALTH F., June 2022, at 1, 2, <https://jamanetwork.com/journals/jama-health-forum/fullarticle/2794032> [<https://perma.cc/7TYD-ZQ2X>].

¹¹⁴ Vittoria Elliott, *Fertility and Period Apps Can Be Weaponized in a Post-Roe World*, WIRED (June 7, 2022), <https://www.wired.com/story/fertility-data-weaponized/> [<https://perma.cc/WY52-QYAR>].

¹¹⁵ Catherine Roberts, *These Period Tracker Apps Say They Put Privacy First. Here's What We Found*, CONSUMER REPS. (Aug. 30, 2022), <https://www.consumerreports.org/health/health-privacy/period-tracker-apps-privacy-a2278134145/> [<https://perma.cc/3S23-ANFF>].

¹¹⁶ Christopher White, *How the Cybertruck Blast Revealed the Extent of Tesla's Sprawling Surveillance Capacity*, KFOX 14 (Jan. 3, 2025), <https://kfoxtv.com/news/nation-world/tesla-cybertruck-explosion-trump-hotel-fbi-surveillance-elon-musk-company> [<https://perma.cc/2R42-JDHU>].

¹¹⁷ CITRON, FIGHT FOR PRIVACY, *supra* note 18, at 11.

tries.”¹¹⁸ The amount of data being collected about people has increased dramatically in the last decade.¹¹⁹ As one article in *Wired* noted: “Companies that traffic in personal, geolocation, advertising, or other data could become digital crime scenes for eager prosecutors armed with subpoenas.”¹²⁰ Data brokers are selling reproductive health data to the government.¹²¹

2. Inferences

AI can be used to make inferences about individuals based on personal data.¹²² By analyzing behavioral patterns, location history, online activity, and even subtle facial expressions captured on camera, AI can predict personal preferences, health conditions, political leanings, and even potential future actions. This capacity to infer detailed insights about individuals from fragmented data poses profound risks to privacy, autonomy, and freedom.

Inferring personal information can invade privacy by uncovering details individuals wish to keep private. One of the most notorious examples involved the retailer Target, which developed an algorithm to identify pregnant women based on their shopping habits. Target realized that identifying pregnancies early could encourage women to begin purchasing baby products from their stores. In one incident, a teenage girl’s father noticed an influx of baby-related advertisements sent to their home and complained about the mistake. He later discovered, however, that his daughter was, in fact, pregnant. The algorithm had made this inference by recognizing a pattern in her purchases, including unscented products, vitamins, and cotton balls, which are common among pregnant women.¹²³

Analyzing financial, communications, location, and other data, scattered across various industries and entities, allows the government to build an incredibly detailed profile of an individual’s life. Such data can be used to infer beliefs, activities, and behaviors.

These inferences are currently being made by many companies with sophisticated AI systems as well as by nearly 80 fusion centers in the U.S.¹²⁴ As Danielle Citron points out, fusion centers are shady institutions that are “largely hidden from view” and that take data from data brokers and conduct sophis-

¹¹⁸ *Id.* at 13.

¹¹⁹ *Id.* at 13–14.

¹²⁰ Alejandra Caraballo, *Tech Companies Are Not Ready for a Post-Roe Era*, WIRED (May 4, 2022), <https://www.wired.com/story/tech-companies-not-ready-post-roe-era/> [<https://perma.cc/6N8U-8F53>].

¹²¹ Huq & Wexler, *supra* note 34, at 582.

¹²² Hideyuki Matsumi, *Predictions and Privacy: Should There Be Rules About Using Personal Data to Forecast the Future?*, 48 CUMB. L. REV. 149, 152 (2017); Solow-Niederman, *supra* note 11; Solove, *Data Is What Data Does*, *supra* note 12, at 1099.

¹²³ Charles Duhigg, *How Companies Learn Your Secrets*, N.Y. TIMES MAG. (Feb. 16, 2012), <https://www.nytimes.com/2012/02/19/magazine/shopping-habits.html> [<https://perma.cc/8JAR-M2PH>].

¹²⁴ CITRON, FIGHT FOR PRIVACY, *supra* note 18, at 58–59.

ticated data analytics on it to assist the government in locating people suspected of criminal activity such as terrorism or drug trafficking.¹²⁵

3. Enhanced Surveillance Capabilities

Digital technologies have contributed to the transformation of the U.S. into a surveillance society.¹²⁶ Intrusive government surveillance has been growing for decades, and digital technologies have fueled the fire. Outside, people can be tracked by surveillance cameras, drones, automated license plate readers (ALPRs), sensors, GPS, location data, geofencing, and more.¹²⁷ Inside, people's activities are also often monitored by surveillance cameras, as well as via their smartphones, web surfing, home assistant devices, and other devices and appliances that gather data.¹²⁸

Cities are increasingly incorporating “smart” technology that constantly amasses personal data by surveilling citizens.¹²⁹ As Andrew Ferguson notes: “Imagine what the smart sensor-enabled city of the future can do. It can monitor where citizens walk, drive, live, play, eat, what medical services they need, what they buy, what they like, who they visit and associate with, and who they love.”¹³⁰

Modern digital technologies enable surveillance at a size, scale, and depth that is radically different from analog surveillance. Ferguson argues that digital technologies are “allowing for a broader, deeper, faster, cheaper, more accurate, automated, and aggregated process of overcollection of personal data.”¹³¹

¹²⁵ *Id.* at 59.

¹²⁶ I. Bennett Capers, *Crime, Surveillance, and Communities*, 40 FORDHAM URB. L.J. 959, 960 (2013) (“[W]e have become a surveillance state.”).

¹²⁷ CHRISTOPHER SLOBOGIN, VIRTUAL SEARCHES: REGULATING THE COVERT WORLD OF TECHNOLOGICAL POLICING 8 (2022) [hereinafter SLOBOGIN, VIRTUAL SEARCHES]; Maneka Sinha, *The Automated Fourth Amendment*, 73 EMORY L.J. 589, 609–10 (2024) (ALPRs); M. Ryan Calo, *The Drone as Privacy Catalyst*, 64 STAN. L. REV. ONLINE 29, 30 (2011), https://www.stanfordlawreview.org/wp-content/uploads/sites/3/2011/12/64-SLRO-29_1.pdf [<https://perma.cc/UY27-PKEK>] (drones); Note, *Geofence Warrants and the Fourth Amendment*, 134 HARV. L. REV. 2508, 2509 (2021) (geofencing); Slobogin, *supra* note 96 (surveillance cameras); Andrew Guthrie Ferguson, *Why Digital Policing Is Different*, 83 OHIO ST. L.J. 817, 837–42 (2022) (cameras, ALPR, data analytics, GPS) [hereinafter Ferguson, *Digital Policing*]; Chaz Arnett, *Race, Surveillance, Resistance*, 81 OHIO ST. L.J. 1103, 1104 (2020) (discussing the use of many surveillance technologies on Black Lives Matter protests).

¹²⁸ SLOBOGIN, VIRTUAL SEARCHES, *supra* note 127, at 8.

¹²⁹ BEN GREEN, THE SMART ENOUGH CITY: PUTTING TECHNOLOGY IN ITS PLACE TO RECLAIM OUR URBAN FUTURE 1–14 (2019) (discussing smart technologies in cities); Andrew Guthrie Ferguson, *Structural Sensor Surveillance*, 106 IOWA L. REV. 47, 49–50 (2020) (detailing certain smart technology in cities) [hereinafter Ferguson, *Structural Sensor Surveillance*].

¹³⁰ Ferguson, *Structural Sensor Surveillance*, *supra* note 129, at 50.

¹³¹ Ferguson, *Digital Policing*, *supra* note 127, at 843–44.

AI can greatly enhance surveillance capabilities.¹³² As Bruce Schneier notes, without AI, surveillance is restricted by the limited human capacity to review and analyze the surveillance data.¹³³ It is costly to have humans monitor surveillance cameras or review footage; and it is also costly for humans to sift through reams of personal data. AI can assist with these tasks by screening through surveillance footage (whether live or recorded). AI can pre-screen vast amounts of data and single out specific instances for humans to review. With facial recognition, AI supercharges surveillance, enabling people to be tracked more precisely wherever they go.¹³⁴

Many commentators have pointed out how automation is fundamentally altering the nature of surveillance, not only enhancing its intrusiveness and scope, but also creating distortions, fostering inequality, and producing other harms.¹³⁵ David Gray and Danielle Citron note that “advanced statistical analysis tools have enhanced the capacities of those who wield surveillance technology to know us, often in ways that we do not know ourselves.”¹³⁶

When combined with surveillance infrastructure, plus the vast digital dossiers about people, AI can transform everyday environments into glass cages of constant monitoring. As Professor Richard Re observes, we may be facing a future of “perfect surveillance.”¹³⁷

¹³² Daniel J. Solove, *Artificial Intelligence and Privacy*, 77 FLA. L. REV. 1 (2025) (explaining AI use in surveillance); Matthew Tokson, *Artificial Intelligence and the Anti-Authoritarian Fourth Amendment*, 27 U. PA. J. CONST. L. 1067, 1067 (2025).

¹³³ Bruce Schneier, *The Internet Enabled Mass Surveillance. A.I. Will Enable Mass Spying*, SLATE (Dec. 4, 2023), <https://slate.com/technology/2023/12/ai-mass-spying-internet-surveillance.html> [<https://perma.cc/3QAB-853N>].

¹³⁴ KASHMIR HILL, *YOUR FACE BELONGS TO US: A SECRETIVE STARTUP’S QUEST TO END PRIVACY AS WE KNOW IT*, at vii (2023) (explaining the impact of AI and facial recognition); Evan Selinger & Woodrow Hartzog, *The Inconsistency of Facial Surveillance*, 66 LOY. L. REV. 33, 43 (2019) (explaining the expansive effect of AI on surveillance).

¹³⁵ See generally Matthew Tokson, *Automation and the Fourth Amendment*, 96 IOWA L. REV. 581 (2011) (discussing the effect of automation on privacy and surveillance); VIRGINIA EUBANKS, *AUTOMATING INEQUALITY: HOW HIGH-TECH TOOLS PROFILE, POLICE, AND PUNISH THE POOR* (2018) (discussing the disparate impacts of high tech surveillance); Andrew Guthrie Ferguson, *Big Data and Predictive Reasonable Suspicion*, 163 U. PA. L. REV. 327 (2015) (explaining the effect vast data collection can have on seizures of people); Elizabeth E. Joh, *Automated Policing*, 15 OHIO ST. J. CRIM. L. 559 (2018) (explaining the effects of automation on policing); Elizabeth E. Joh, *The New Surveillance Discretion: Automated Suspicion, Big Data, and Policing*, 10 HARV. L. & POL’Y REV. 15 (2016) (discussing the advancements in data collection and technology and their effect on policing).

¹³⁶ David Gray & Danielle Citron, *The Right to Quantitative Privacy*, 98 MINN. L. REV. 62, 75 (2013).

¹³⁷ Richard M. Re, *Imagining Perfect Surveillance*, 64 UCLA L. REV. DISCOURSE 264, 266 (2016), <https://www.uclalawreview.org/imagining-perfect-surveillance/> [<https://perma.cc/J6SF-4K2Y>].

D. Surveillance Capitalism Meets Government Surveillance

Increasingly, government surveillance is not conducted by the government alone. Companies augment governmental power.¹³⁸ As Barry Friedman notes: “A good portion of the surveillance of the United States’ population by law enforcement is the result of public-private partnerships. The data that those who police us want can be purchased, subpoenaed, or simply given to the government on an ask.”¹³⁹

There are several ways that companies facilitate government surveillance. First, companies can be compelled to provide data to the government via subpoenas, court orders, warrants, or civil discovery. The private sector is a rich source of personal data for the government to mine. As Kiel Brennan-Marquez points out, private surveillance can operate as an “extension of law enforcement infrastructure.”¹⁴⁰ The private sector has established an elaborate network of surveillance cameras and other technologies that government law enforcement can readily plug into.¹⁴¹

The decision about whether to challenge a government demand for data belongs to the third parties, not to the individuals whose data is being sought. These individuals are often not even notified that the government is demanding their data. Many companies are unlikely to expend the time, money, or resources to contest such government data demands. Instead, they may choose to comply and simply hand over the requested data. Sometimes, companies readily provide people’s data to the government on a mere request. For example, after the 9/11 attacks, government officials asked for records from companies without a subpoena, warrant, or court order; many companies readily turned over the data.¹⁴²

Second, companies can willingly give or sell data to the government.¹⁴³ A report by the Center for Democracy and Technology concluded that “law enforcement and intelligence agencies are among the customers of some data brokers, spending millions of dollars to gain access to private sector databases which often contain very sensitive and very personal information on individu-

¹³⁸ Arnett, *supra* note 103, at 1407 (“[N]ew surveillance technologies developed and often run by private companies make it difficult to find a line between government and private action.”).

¹³⁹ Friedman, *supra* note 103, at 1150.

¹⁴⁰ Kiel Brennan-Marquez, *The Constitutional Limits of Private Surveillance*, 66 U. KAN. L. REV. 485, 489 (2018).

¹⁴¹ *See generally id.*

¹⁴² Daniela Deane, *Legal Niceties Aside . . . ; Federal Agents Without Subpoenas Asking Firms for Records*, WASH. POST (Nov. 6, 2001), <https://www.washingtonpost.com/archive/business/2001/11/07/legal-niceties-aside/42343371-7cf9-4c2a-9708-ef2653abb182/> [<https://perma.cc/S4T7-LHKL>].

¹⁴³ Alan Z. Rozenshtein, *Surveillance Intermediaries*, 70 STAN. L. REV. 99, 112 (2018) (discussing how private sector companies operate as “surveillance intermediaries,” to gather data to be used for government surveillance); Hoofnagle, *supra* note 111, at 598 (private entities collect data the government cannot).

als.”¹⁴⁴ Data brokers willingly sell personal data to numerous government agencies.¹⁴⁵ There are more than 4,000 data brokers.¹⁴⁶ Data brokers sell an enormous cornucopia of personal data, including lists of rape victims and alcoholics.¹⁴⁷ State governments eager to police wombs can learn about pregnancies from Experian, a data broker that sells lists of parents expecting children.¹⁴⁸ U.S. Immigration and Customs Enforcement (ICE) obtains from companies “call records, child welfare records, credit headers, employment records, geolocation information, health care records, housing records and social media posts.”¹⁴⁹ ICE uses private-sector geolocation tracking services that provide databases of automobile license plate scans and biometric information.¹⁵⁰

Third, companies can contract with the government to perform surveillance services.¹⁵¹ ICE uses a vendor to gather data about people’s phone, internet, and email use.¹⁵² Companies mine personal data from many sources to assist the government in monitoring individuals.¹⁵³ In one instance, the government sought a court order mandating that Apple develop a way to decrypt a suspect’s iPhone. When Apple resisted and was litigating the issue, the government was able to find another company willing to do the work for them to break into the phone.¹⁵⁴ In 2020, during the Black Lives Matter protests, the Minneapolis Police Department enlisted a company to gather information

¹⁴⁴ SHARON BRADFORD FRANKLIN, GREG NOJEIM, DHANARAJ THAKUR & CAREY SHENKMAN, CTR. FOR DEMOCRACY & TECH., *LEGAL LOOPHOLES AND DATA FOR DOLLARS 5* (2021), <https://cdt.org/wp-content/uploads/2021/12/2021-12-08-Legal-Loopholes-and-Data-for-Dollars-Report-final.pdf> [<https://perma.cc/N5J8-P74Y>].

¹⁴⁵ Emile Ayoub & Elizabeth Goitein, *Closing the Data Broker Loophole*, BRENNAN CTR. FOR JUST. (Feb. 13, 2024), <https://www.brennancenter.org/our-work/research-reports/closing-data-broker-loophole> [<https://perma.cc/S2L5-W7ZG>] (discussing private work arounds to the Fourth Amendment’s protections); Donohue, *supra* note 90, at 1144–56 (discussing the private data market).

¹⁴⁶ Zachary McAuliffe, *Data Brokers and Personal Data Deletion Services: What You Should Know*, CNET (Feb. 22, 2023), <https://www.cnet.com/tech/services-and-software/data-brokers-and-personal-data-deletion-services-what-you-should-know/> [<https://perma.cc/N2XB-TQSR>].

¹⁴⁷ Kashmir Hill, *Data Broker Was Selling Lists of Rape Victims, Alcoholics, and ‘Erectile Dysfunction Sufferers’*, FORBES (Dec. 19, 2013), <https://www.forbes.com/sites/kashmirhill/2013/12/19/data-broker-was-selling-lists-of-rape-alcoholism-and-erectile-dysfunction-sufferers/> [<https://perma.cc/D7UQ-3AY5>].

¹⁴⁸ Kaminski & Witnov, *supra* note 79, at 469.

¹⁴⁹ *American Dragnet: Data-Driven Deportation in the 21st Century*, GEO. L. CTR. ON PRIV. & TECH. (May 10, 2022), <https://americandragnet.org/> [<https://perma.cc/T32R-93N3>].

¹⁵⁰ *Id.*

¹⁵¹ Paul Ohm, *The Fourth Amendment in a World Without Privacy*, 81 MISS. L.J. 1309, 1338 (2012) (discussing how the government can “outsource surveillance to private third parties”).

¹⁵² *American Dragnet*, *supra* note 149.

¹⁵³ See generally HEIDI BOGHOSIAN, *SPYING ON DEMOCRACY: GOVERNMENT SURVEILLANCE, CORPORATE POWER, AND PUBLIC RESISTANCE* (2013) (discussing the interplay between private companies and government surveillance).

¹⁵⁴ DANIEL J. SOLOVE & WOODROW HARTZOG, *BREACHED! WHY DATA SECURITY LAW FAILS AND HOW TO IMPROVE IT* 102 (2022).

about protestors, including those engaging in nonviolent activity.¹⁵⁵ The company monitored people's social media activities to keep "comprehensive records of upcoming anti-police violence rallies."¹⁵⁶

Fourth, companies create new surveillance technologies that the government uses. For example, Clearview AI markets a facial recognition system used by many law enforcement agencies.¹⁵⁷ Boasting a 98.6% accuracy rate, the company developed its system by scraping billions of photos from the internet without people's knowledge or consent.¹⁵⁸ Law enforcement officials around the world use Palantir's powerful data analytics software.¹⁵⁹ The law generally allows the government to use whatever new technologies it desires, without any public discussion about the risks versus benefits.¹⁶⁰

As Elizabeth Joh observes, "[p]rivate surveillance technology companies wield an undue influence over public police today in ways that aren't widely acknowledged, but have enormous consequences for civil liberties and police oversight."¹⁶¹ These technological tools used by the government are often designed with scant controls or oversight mechanisms.¹⁶²

Government entities readily work in tandem with the private sector, buy its services and technologies, or can just readily demand the vast data hoarded by companies. Most of this activity occurs in the shadows with hardly any accountability or limitation—the ideal conditions for authoritarian practices to thrive. As Andrew Guthrie Ferguson aptly argues: "Predictive policing algorithms, automated license plate readers, video analytics, gunshot sensors, sting-ray devices, drones, robots, and other innovations have grown from an interesting idea to government adoption without significant regulation or public oversight."¹⁶³ Government surveillance and surveillance capitalism are too closely aligned to serve as rival sources of power; they often blend together, dramatically enhancing the power of the state.

¹⁵⁵ Sam Biddle, *Police Surveilled George Floyd Protests with Help from Twitter-Affiliated Startup DataMinr*, THE INTERCEPT (July 9, 2020), <https://theintercept.com/2020/07/09/twitter-dataminr-police-spy-surveillance-black-lives-matter-protests/> [<https://perma.cc/G2BT-CRZQ>].

¹⁵⁶ *Id.*

¹⁵⁷ See generally HILL, *supra* note 134 (discussing the use of Clearview AI).

¹⁵⁸ See *id.* at viii.

¹⁵⁹ SARAH BRAYNE, *Dragnet Surveillance: Our Incriminating Lives* (discussing how Palantir's software helps LAPD officers to analyze ALPR data), in PREDICT AND SURVEIL: DATA, DISCRETION 49–50 (2020).

¹⁶⁰ Daniel J. Solove, *Reconstructing Electronic Surveillance Law*, 72 GEO. WASH. L. REV. 1264, 1264 (2004) [hereinafter Solove, *Reconstructing Electronic Surveillance*].

¹⁶¹ Elizabeth E. Joh, *The Undue Influence of Surveillance Technology Companies on Policing*, 92 N.Y.U. L. REV. ONLINE 19, 20 (2017), https://www.nyulawreview.org/wp-content/uploads/2017/08/NYULawReviewOnline-92-Joh_0.pdf [<https://perma.cc/23UU-EBDR>].

¹⁶² WOODROW HARTZOG, *PRIVACY'S BLUEPRINT: THE BATTLE TO CONTROL THE DESIGN OF NEW TECHNOLOGIES* 34 (2018).

¹⁶³ Ferguson, *supra* note 42, at 211.

Additionally, authoritarianism in the U.S. is taking on an oligarchical dimension. In his farewell address, President Biden warned that “an oligarchy is taking shape in America of extreme wealth, power, and influence that literally threatens our entire democracy, our basic rights and freedoms, and a fair shot for everyone to get ahead.”¹⁶⁴ Authoritarian power can readily be exercised by companies, not just by government officials.

II. REGULATING GOVERNMENT SURVEILLANCE

The law regulating government surveillance in the U.S. is an authoritarian’s dream. In its Fourth Amendment jurisprudence, the U.S. Supreme Court currently views privacy as synonymous with complete secrecy, focusing on the protection of an individual’s hidden world. It prioritizes safeguarding intimate details that people deliberately conceal, likening privacy to shielding the metaphorical skeletons in the closet. Under this conception, information shared with third parties is deemed exposed, and thus, not private or protected by the Fourth Amendment. This outdated conception fails to align with the realities of the modern Information Age, however, where much of an individual’s personal information resides within the record systems of countless entities.

Based on the current state of the law, the government can obtain a treasure trove of personal data from a myriad of different companies with hardly any procedural protections, oversight, or limitation.¹⁶⁵ As Barry Friedman notes, “[v]irtually every commentator in the space has concluded that the Fourth Amendment is hapless when it comes to digital surveillance.”¹⁶⁶ Current law allows for vast suspicionless searches—the kind of dragnets that are common in authoritarian regimes. Hannah Bloch-Wehba points out that the law fails to mandate transparency and accountability for government surveillance.¹⁶⁷ The law in the U.S. allows nearly limitless government surveillance to occur in the dark, the perfect recipe for an authoritarian regime.

Section A of this Part argues that the third-party doctrine should be overturned.¹⁶⁸ Section B argues that the Supreme Court should adopt a more robust interpretation of the Fourth Amendment.¹⁶⁹ Section C discusses other possible

¹⁶⁴ President Joe Biden, Remarks by President Biden in a Farewell Address to the Nation (Jan. 15, 2025), <https://www.whitehouse.gov/briefing-room/speeches-remarks/2025/01/15/remarks-by-president-biden-in-a-farewell-address-to-the-nation/> [<https://perma.cc/F7M6-7RDJ>].

¹⁶⁵ Lindsey Barrett, *Carpenter’s Consumers*, 59 WASHBURN L.J. 53, 54 (2020).

¹⁶⁶ Friedman, *supra* note 103, at 1166. An exception is Orin Kerr, who defends the third-party doctrine. *See generally* Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561 (2009) (discussing the justifications for the third-party doctrine).

¹⁶⁷ Hannah Bloch-Wehba, *Visible Policing: Technology, Transparency, and Democratic Control*, 109 CALIF. L. REV. 917, 921–22 (2021).

¹⁶⁸ *See infra* notes 173–204.

¹⁶⁹ *See infra* notes 205–232.

Constitutional protections against government surveillance.¹⁷⁰ Finally, Section D examines the statutory protections against government surveillance and argues they should be enhanced.¹⁷¹

A. Overturning the Third-Party Doctrine

The primary safeguard against privacy infringement by law enforcement is the Fourth Amendment, which prohibits unreasonable searches and seizures and requires judicial authorization before such actions can occur.¹⁷² In the digital age, however, the third-party doctrine almost totally undermines Fourth Amendment protection. It must be overturned.

1. The Flaws and Dangers of the Third-Party Doctrine

Under the third-party doctrine, the U.S. Supreme Court has ruled that individuals have no reasonable expectation in privacy for information known or exposed to third parties. In 1976, in *United States v. Miller*, the U.S. Supreme Court held that there is no reasonable expectation of privacy in financial records maintained by one's bank because "the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities."¹⁷³ In 1979, in *Smith v. Maryland*, the U.S. Supreme Court concluded that there was no reasonable expectation of privacy when the government obtained a list of phone numbers a person dialed from the phone company because people "know that they must convey numerical information to the phone company" and cannot "harbor any general expectation that the numbers they dial will remain secret."¹⁷⁴

In the digital age, the implications of the third-party doctrine are enormous. With modern technology, so much of our data is in the hands of third parties that the Fourth Amendment barely applies to much of our lives.¹⁷⁵ Countless companies maintain records about us. We store documents and photos with cloud service providers. Credit card companies keep detailed records about our purchases. Our location information is available to telecommunications companies. Our Web surfing activity is in the hands of internet service

¹⁷⁰ See *infra* notes 233–239.

¹⁷¹ See *infra* notes 240–266.

¹⁷² U.S. CONST. amend. IV.

¹⁷³ *United States v. Miller*, 425 U.S. 435, 443 (1976).

¹⁷⁴ *Smith v. Maryland*, 442 U.S. 735, 743 (1979).

¹⁷⁵ Laura K. Donohue, *The Fourth Amendment in a Digital World*, 71 N.Y.U. ANN. SURV. AM. L. 553, 554 (2017) (explaining the changes of the fourth amendment's applications to the digital age); Ohm, *supra* note 151, at 1320–35 (discussing the impact of third parties holding data); Katherine J. Strandburg, *Home, Home on the Web and Other Fourth Amendment Implications of Technosocial Change*, 70 MD. L. REV. 614, 619–21 (2011). See generally Solove, *Digital Dossiers*, *supra* note 4 (discussing the true reach of the third-party doctrine given modern data collection).

providers. Merchants such as Amazon.com have records about our purchases of books and movies and other things.

In today's digital age, the government no longer needs to enter a person's home to learn about that person—the books that person is reading, the person's communications, hobbies, interests, intellectual exploration, and more can all be learned from third party records. With the third-party doctrine, the Fourth Amendment will become increasingly obsolete, as our personal data is often in the hands of third parties.¹⁷⁶

The U.S. Supreme Court's flawed interpretation of the Fourth Amendment need not bind state courts in interpreting state constitutions. All state constitutions have a provision similar or identical to the Fourth Amendment. Although state courts have often interpreted their constitutions consistently with the U.S. Supreme Court's interpretation of the U.S. Constitution, some states have diverged. For example, the New Jersey Supreme Court rejected the third-party doctrine.¹⁷⁷

2. *Carpenter* and Its Aftermath

In 2018, the U.S. Supreme Court finally took a step back from the third-party doctrine in *Carpenter v. United States*.¹⁷⁸ The FBI was investigating a string of robberies of Radio Shack. The FBI obtained cell phone records of the defendants pursuant to the Stored Communications Act (SCA), which requires “specific and articulable facts” to demonstrate that there are “reasonable grounds to believe” that the records are “relevant and material to an ongoing criminal investigation.”¹⁷⁹ This standard is far short of what the Fourth Amendment would require, which is a search warrant based upon probable cause.¹⁸⁰ The Court held that the Fourth Amendment applies when the government “accesses historical cell phone records that provide a comprehensive chronicle of the user's past movements.”¹⁸¹

¹⁷⁶ *United States v. Jones*, 565 U.S. 400, 417 (2012) (Sotomayor, J., concurring) (arguing that the third-party doctrine “is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks.”). See generally SOLOVE, *THE DIGITAL PERSON*, *supra* note 111 (discussing the effect of the third-party doctrine on the fourth amendment).

¹⁷⁷ *State v. Hunt*, 450 A.2d 952, 955–56 (N.J. 1982) (rejecting the third-party doctrine); Stephen E. Henderson, *Learning from All Fifty States: How to Apply the Fourth Amendment and Its State Analogues to Protect Third Party Information from Unreasonable Seizure*, 55 CATH. U. L. REV. 373, 395 (2006) (discussing how to use state constitutions to provide more robust protections).

¹⁷⁸ See generally *Carpenter v. United States*, 585 U.S. 296 (2018) (deviating from the third-party doctrine).

¹⁷⁹ 18 U.S.C. § 2703(d).

¹⁸⁰ U.S. CONST. amend. IV.

¹⁸¹ *Carpenter*, 585 U.S. at 296–300.

Rather than overrule *Smith* and *Miller*, the *Carpenter* Court just stated that these cases don't apply to cell-site location records: "We decline to extend *Smith* and *Miller* to cover these novel circumstances. Given the unique nature of cell phone location records, the fact that the information is held by a third party does not by itself overcome the user's claim to Fourth Amendment protection."¹⁸²

The Court noted that its decision was a "narrow one" and that it would not "disturb the application of *Smith* and *Miller* or call into question conventional surveillance techniques and tools, such as security cameras" or "address other business records that might incidentally reveal location information."¹⁸³

Although the majority opinion finally indicated a limit to the third-party doctrine, the opinion left far too many unanswered questions and no test for when surveillance triggers the Fourth Amendment under *Carpenter*.¹⁸⁴

More broadly, as Andrew Ferguson notes, Fourth Amendment jurisprudence "offers little clarity" on key issues about data gathering and surveillance, such as whether the police can obtain smart home data or whether the police can monitor who enters or exits a person's home throughout a year.¹⁸⁵ Notwithstanding how courts are trying to answer these questions, the very fact Fourth Amendment jurisprudence has not reached definitive answers is already a major failure.¹⁸⁶

3. Developing *Carpenter*'s Principles

After *Carpenter*, government officials and entities almost immediately found an end-run around the case by purchasing location data from data brokers.¹⁸⁷ A cottage industry has arisen where companies sell location tracking data exclusively to the government.¹⁸⁸ For example, the federal government purchased location data from Venntel, a data broker that gathered location data from smart phone apps to track undocumented immigrants.¹⁸⁹

The rationale for how the government could continue obtaining location data from companies after *Carpenter* is based on the "willing seller rule," which holds that the Fourth Amendment does not apply when the government

¹⁸² *Id.* at 309.

¹⁸³ *Id.* at 316.

¹⁸⁴ Barrett, *supra* note 165, at 59.

¹⁸⁵ Andrew Guthrie Ferguson, *Digital Rummaging*, 101 WASH. U. L. REV. 1473, 1475 (2024).

¹⁸⁶ Susan Freiwald & Stephen Wm. Smith, *The Carpenter Chronicle: A Near-Perfect Surveillance*, 132 HARV. L. REV. 205, 234 (2018) ("[T]here is no sound reason why the Supreme Court should slow-walk its decisions on critical legal issues posed by advancing technology.").

¹⁸⁷ Matthew Tokson, *Government Purchases of Private Data*, 59 WAKE FOREST L. REV. 269, 274 (2024).

¹⁸⁸ *Id.*

¹⁸⁹ Byron Tau & Michelle Hackman, *Federal Agencies Use Cellphone Location Data for Immigration Enforcement*, WALL ST. J. (Feb. 7, 2020), <https://www.wsj.com/articles/federal-agencies-use-cellphone-location-data-for-immigration-enforcement-11581078600> [<https://perma.cc/6B94-H6UC>].

buys data from a company.¹⁹⁰ Orin Kerr contends that *Carpenter* does not upset this rule. But following such a rule after *Carpenter* creates an end-run—instead of obtaining cell phone site location data via a court order, the government could just buy it. Thus, obtaining the data under the SCA with some degree of protection would violate the Fourth Amendment but obtaining it by purchasing it without any protection would be just fine. As Matthew Tokson argues, “there is nothing special about a commercial transaction that allows it to strip otherwise protected data of its constitutional protections.”¹⁹¹

Additionally, police are using other technologies to obtain location data, such as automated license plate readers (ALPRs).¹⁹² And, beyond location data, government officials continue to feast upon the copious quantities of other types of personal data held by third parties. Government officials obtain DNA information, engage in social media monitoring, and use facial recognition systems—all outside of the safeguards of the Fourth Amendment.¹⁹³

The government increasingly uses AI algorithms and Big Data as tools for predictive policing.¹⁹⁴ These systems suffer from bias and error.¹⁹⁵ Predictive policing can readily be used in ways that disrespect human agency; algorithmic predictions are fraught with problems that violate fundamental principles of due process and fairness.¹⁹⁶ These types of concerns led Professor Emily Berman to argue that “statistical evidence, irrespective of its accuracy in predicting the presence of criminal activity or the means by which it is generated, should not form the basis of individualized-suspicion determinations.”¹⁹⁷ The very way algorithmic predictions work is to focus not on the particular individuals whose behavior they are predicting but on patterns of past behavior of a large number of people.¹⁹⁸ It is doubtful that algorithmic predictions can ever be squared with core constitutional values.

Lower courts need not proceed tepidly in developing the law after *Carpenter*; which is a classic starter case from the U.S. Supreme Court. The Court

¹⁹⁰ Orin S. Kerr, *Buying Data and the Fourth Amendment*, HOOVER INST. 2 (Nov. 17, 2021) (Aegis Series Paper No. 2109), https://www.hoover.org/sites/default/files/research/docs/kerr_webready.pdf [https://perma.cc/G5DW-3UX2].

¹⁹¹ Tokson, *supra* note 187, at 275.

¹⁹² Bloch-Wehba, *supra* note 167, at 919.

¹⁹³ *Id.* at 921.

¹⁹⁴ ANDREW GUTHRIE FERGUSON, *THE RISE OF BIG DATA POLICING: SURVEILLANCE, RACE, AND THE FUTURE OF LAW ENFORCEMENT* 19 (2017).

¹⁹⁵ *Id.* at 191.

¹⁹⁶ See generally Hideyuki Matsumi & Daniel J. Solove, *The Prediction Society: AI and the Problems of Forecasting the Future*, 2025 U. ILL. L. REV. 1 (discussing the constitutional and legal concerns surrounding predictive policing).

¹⁹⁷ Emily Berman, *Individualized Suspicion in the Age of Big Data*, 105 IOWA L. REV. 463, 466–67 (2020).

¹⁹⁸ Katrina Geddes, *The Death of the Legal Subject*, 25 VAND. J. ENT. & TECH. L. 1, 26 (2023) (observing that algorithmic predictions treat “data subjects not as unique individuals, but as patterns of behavior”); Matsumi & Solove, *supra* note 196 (discussing the predictions in surveillance).

signaled a new direction, and it left many unanswered questions and undeveloped issues. Lower courts can be more aggressive in developing the law.¹⁹⁹

The *Carpenter* Court expressed concerns about the “depth, breadth, and comprehensive reach, and the inescapable and automatic nature of its collection.”²⁰⁰ In a case decided a few years before *Carpenter* involving the search of a cell phone incident to arrest, the Court held that searching the entire phone was too broad because the “sum of an individual’s private life can be reconstructed through a thousand photographs labeled with dates, locations, and descriptions.”²⁰¹ The Court recognized that extensive surveillance and the aggregation of many pieces of data can violate privacy, an understanding of privacy that some have termed “mosaic theory.”²⁰²

Thus, there is a basis in current Fourth Amendment jurisprudence for a broader scope to Fourth Amendment protection. The U.S. Supreme Court has shifted away from viewing privacy as involving complete secrecy to focusing instead on how much data reveals about individuals’ lives. The question is how far the Court is willing to go down this rabbit hole. Conceptually, the rabbit hole leads to a radical rethinking of privacy—and of much of the Court’s Fourth Amendment jurisprudence. Although the logic might take us to Wonderland, the Court’s timid feet have only inched so far. The question, then, is whether lower courts proceed according to logic or try to mimic the Court’s hesitation.

Orin Kerr contends that generally, Fourth Amendment doctrine focuses on what he calls “equilibrium adjustment”—to seek to maintain a status quo balance between law enforcement investigatory power and the ability of criminals to avoid detection.²⁰³ Assuming that this is generally what courts seek to do, it is a problematic approach. It is far from clear that the current balance deserves to be preserved. Nor is it possible to translate modern technologies into a uniform balance, as if new technologies, government exercises of power, and criminal activities can all be averaged together to produce some kind of neat

¹⁹⁹ Ultimately, federal courts have attempted to craft an approach to analyzing surveillance issues after *Carpenter*. Surveying the cases, Matthew Tokson concludes that there are three factors that courts examine: “(1) the revealing nature of the data collected; (2) the amount of data collected; and (3) whether the suspect voluntarily disclosed their information to others.” Matthew Tokson, *The Carpenter Test as a Transformation of Fourth Amendment Law*, 2023 U. ILL. L. REV. 507, 510.

²⁰⁰ *Carpenter v. United States*, 585 U.S. 296, 320 (2018).

²⁰¹ *Riley v. California*, 573 U.S. 373, 394 (2014).

²⁰² See generally Orin S. Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 MICH. L. REV. 311 (2012) (discussing the mosaic theory of searches and the fourth amendment); David Gray & Danielle Keats Citron, *A Shattered Looking Glass: The Pitfalls and Potential of the Mosaic Theory of Fourth Amendment Privacy*, 14 N.C. J.L. & TECH. 381 (2013) (describing the realities of the mosaic theory).

²⁰³ Orin S. Kerr, *An Equilibrium-Adjustment Theory of the Fourth Amendment*, 125 HARV. L. REV. 476, 480 (2011).

midway line in a game between cops and robbers. New technologies have dramatically changed the very game itself.

At least part of the equation is how we want to structure and control the government's power. The standard fare of warrants and probable cause are not sufficient in light of today's technology. Professor Christopher Slobogin argues for a "proportionality approach" that focuses on "setting levels of suspicion" based on "how much explanation for a given intrusion is necessary to convince an innocent person subjected to it that the police acted reasonably."²⁰⁴ To balance the risk of authoritarianism, other considerations should also be included. This equation depends upon several factors—the seriousness of the crime, the societal consensus about the crime, and the degree of authoritarianism of the government. When the crime is a serious one with considerable consensus (such as terrorism), and there is a low risk of an authoritarian government, there is a stronger normative case to give the government strong enforcement powers. But when the crime is one such as abortion, where it is viewed by many as a fundamental right, and there is an authoritarian government or high risk of one, do we really want the same equilibrium point? Do we want the government to have the same powers?

Ultimately, the question of how much power the government should have depends on more than what criminals might do. It depends upon the types of crimes being enforced, the nature of government enforcement powers at a particular time in history, and many other factors that transcend a simple rat race between criminals and cops. The Fourth Amendment was not created simply to deal with ordinary policing and criminal enforcement. It was forged to serve as a bulwark against an authoritarian government.

B. Revitalizing the Fourth Amendment

Overall, the Fourth Amendment must be freed from the myopic ways it is currently interpreted. As Laura Donohue puts it simply and most directly, "Fourth Amendment doctrine no longer reflects how the world works."²⁰⁵ Ideally, the Supreme Court would wake up and rethink its unfortunate Fourth Amendment jurisprudence, which it seems to have started to do in *Carpenter* but then lost the fortitude and vision to continue. Lower federal courts can step into the void and advance the ball more aggressively. And state courts can break with the U.S. Supreme Court for interpretations of their own constitutions. The ideas below are thus proposed with the hope that any or all of the above might occur.

²⁰⁴ CHRISTOPHER SLOBOGIN, *PRIVACY AT RISK: THE NEW GOVERNMENT SURVEILLANCE AND THE FOURTH AMENDMENT* 39 (2007).

²⁰⁵ Donohue, *supra* note 175, at 554.

1. Government Data Use and Retention

The Fourth Amendment is generally understood to focus on government collection of data. But as Orin Kerr correctly notes, in the digital age, government surveillance occurs not just at one stage but multiple stages, such as the analysis of data gathered from initial surveillance techniques.²⁰⁶ But once the government collects it, current Fourth Amendment jurisprudence says little about how the government can analyze, use, or retain the data.²⁰⁷ For example, under current Fourth Amendment jurisprudence, a person's DNA can readily be gathered and analyzed by the government with no protections or oversight. Because people cannot avoid leaving DNA traces behind, those traces can readily be collected, and they fall outside of the Fourth Amendment because they are considered to be "abandoned."²⁰⁸ The government can then analyze this data however it wants, with no restrictions, because the Fourth Amendment fails to address downstream data uses or analysis.

Instead, the Fourth Amendment could be interpreted more broadly to extend protection beyond the collection of data. The Fourth Amendment's text prohibits "unreasonable searches and seizures."²⁰⁹ Courts have a wide leeway to determine what constitutes "unreasonable" action.²¹⁰ An unreasonable seizure can certainly extend beyond the time of initial collection and encompass how data is retained and analyzed. Likewise, a search could be understood to encompass certain types of analysis after gathering.²¹¹ Such an interpretation would strengthen Fourth Amendment protection, so that such protection could extend far beyond what it involves now.

2. Beyond the Secrecy Paradigm: Protecting Privacy in Public

Current Fourth Amendment law draws from an antiquated notion of privacy that I term the "secrecy paradigm."²¹² Under this view, a matter is not

²⁰⁶ Orin S. Kerr, *Use Restrictions and the Future of Surveillance Law*, BROOKINGS (Apr. 19, 2011), <https://www.brookings.edu/articles/use-restrictions-and-the-future-of-surveillance-law/> [<https://perma.cc/PX5P-8W4F>].

²⁰⁷ Emily Berman, *When Database Queries Are Fourth Amendment Searches*, 102 MINN. L. REV. 577, 578 (2017) ("So long as its collection is lawful, the Fourth Amendment has nothing to say about how information is employed.").

²⁰⁸ See generally Elizabeth E. Joh, *Reclaiming "Abandoned" DNA: The Fourth Amendment and Genetic Privacy*, 100 NW. U. L. REV. 857 (2006) (discussing the consequences of leaving DNA behind).

²⁰⁹ U.S. CONST. amend. IV.

²¹⁰ See generally Daniel J. Solove, *Fourth Amendment Pragmatism*, 51 B.C. L. REV. 1511 (2010) (discussing the practical applications of what constitutes "reasonable").

²¹¹ See Berman, *supra* note 207, at 579–80 (arguing that "when a database query returns information that the government could otherwise collect only through a Fourth Amendment-regulated means, the Fourth Amendment should regulate that query").

²¹² Solove, *Digital Dossiers*, *supra* note 4, at 1128–36.

private if it is exposed to the public in any way. The Court's conception of privacy is one of total secrecy. If any information is exposed to the public or if law enforcement officials can view something from any public vantage point, then the Court has refused to recognize a reasonable expectation of privacy. For example, in 1989, in *Florida v. Riley*, the U.S. Supreme Court held that a person lacked a reasonable expectation of privacy in his greenhouse because the police could view inside by flying over it with a helicopter and looking in where a few roof tiles were missing.²¹³ In 1983, in *United States v. Knotts*, the U.S. Supreme Court held that when in public, individuals have "voluntarily conveyed" their activities "to anyone who wanted to look."²¹⁴ Although *Carpenter* recognizes a privacy interest in public movement captured in cell-site location data, the case remains fairly limited to this context and has not overturned the secrecy paradigm. In sum, as it is currently interpreted, the Fourth Amendment does not provide protection to public surveillance, whether in public streets, malls, stores, supermarkets, office lobbies, or other places.²¹⁵

Ubiquitous surveillance—inescapable, ever present, highly intrusive—is the digital iron cage that authoritarian regimes use to watch and control their citizens. It is hard to imagine the Fourth Amendment having much meaning or purpose if it has no applicability to such surveillance. Beyond the Fourth Amendment, there is scant statutory regulation of surveillance in public. This means no oversight, no accountability, no limitations, no protection of expressive activities, and no safeguards against abuse.

Applying the Fourth Amendment to public surveillance does not mean prohibiting the practice. As Bennett Capers notes, public surveillance has benefits such as to deter crime, apprehend criminals as well as "to monitor the police, reduce racial profiling, curb police brutality, and ultimately increase perceptions of legitimacy."²¹⁶ The Fourth Amendment, if interpreted more robustly than the desiccated way in which it is currently construed, could provide a set of principles and the foundation for a framework to regulate public surveillance and prevent abuses.

3. Restriction of Dragnet Searches

Dragnet searches are one of the most dangerous tools in the hands of authoritarian governments. Perhaps the primary animating principle behind the Fourth Amendment to the U.S. Constitution is the importance of limiting drag-

²¹³ *Florida v. Riley*, 488 U.S. 445, 451 (1989).

²¹⁴ *United States v. Knotts*, 460 U.S. 276, 281 (1983).

²¹⁵ Capers, *supra* note 126, at 965–69. See generally SOLOVE, NOTHING TO HIDE: THE FALSE TRADEOFF BETWEEN PRIVACY AND SECURITY (2011) (discussing the Fourth Amendment applications in public spaces).

²¹⁶ Capers, *supra* note 126, at 978.

net searches.²¹⁷ Although there are many debates about the original intent behind the Fourth Amendment, if there's one consensus point, it is that the Framers hated general warrants.²¹⁸ A general warrant was a tool used by the British government to search broadly for any information relevant to a particular offense. The Framers explicitly wrote into the Fourth Amendment a prohibition on general warrants with the second clause of the Amendment that states "no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."²¹⁹ The Framers viewed the general warrant as a tool of oppression, as the overreach of government authority, and as a tyrannical abuse of power. The Framers didn't just dislike general warrants; they loathed them.

It is difficult, given its provenance, to conceive of how the Fourth Amendment can be interpreted to allow for widespread dragnet searches in a multitude of forms, but somehow, this is where the Supreme Court has brought us to today. A plausible interpretation would be that dragnet searches are barred by the Fourth Amendment, but at the very least, such searches should be treated with great caution and extensive oversight and limitation.

For example, Professor Jane Bambauer proposes that "filtered dragnets" (ones that are narrowed to searches for particular crimes) could potentially be regulated to lessen their potential for authoritarian abuses.²²⁰ She contends that filtered dragnets would achieve an appropriate balance between privacy and law enforcement:

when (1) they are used to find an individual related to a crime (rather than to find a crime related to an individual), (2) when they report details from an otherwise private database only after meeting a high threshold of confidence (e.g., probable cause or higher), and (3) when they withhold details that are *ex ante* unlikely to be relevant to the current criminal investigation, the nature of that surveillance is different from other types of police work.²²¹

²¹⁷ See generally WILLIAM J. CUDDIHY, *THE FOURTH AMENDMENT: ORIGINS AND ORIGINAL MEANING*: 602–1791 (2009) (discussing the principles and developments that led to the Fourth Amendment).

²¹⁸ Christopher Slobogin, *Government Dragnets*, 73 *LAW & CONTEMP. PROBS.* 107, 107 (2010) ("American colonists abhorred the suspicionless house-to-house searches visited upon them by government officials armed with so-called 'general warrants' . . . [which were] a major cause of the Revolutionary War."). See generally Barry Friedman, *The Constitutionality of Indiscriminate Data Surveillance*, U. PA. L. REV. (forthcoming 2026) (discussing general warrants).

²¹⁹ U.S. CONST. amend IV.

²²⁰ Jane R. Bambauer, *Filtered Dragnets and the Anti-Authoritarian Fourth Amendment*, 97 S. CAL. L. REV. 571, 575 (2024).

²²¹ *Id.* at 574–75.

Although Bambauer's framework would make modern surveillance technologies more consistent with Fourth Amendment values, it is unlikely to stand up to authoritarian activities. Bambauer herself notes that:

[f]iltered dragnets will dramatically increase the detection of crime, and this will intensify existing pathologies in American criminal justice that have little to do with privacy. Namely, we have too many crimes, too much punishment, and too much police and prosecutorial discretion. These problems jointly produce the risk of authoritarian power.²²²

These pathologies, when mixed with authoritarianism, might be too potent to be limited by the framework Bambauer proposes, especially when there is such great division about what activities are criminalized and how zealously they ought to be prosecuted.

Ultimately, the ability to define what is criminalized and when to enforce the law gives the government tremendous power. Typically, the nature of the crime is not an issue in Fourth Amendment jurisprudence; if proper procedures are followed, such as obtaining a warrant supported by probable cause or whatever is required in a given situation, the Fourth Amendment will allow a search. Although today, we call the Fourth Amendment "criminal procedure," the Amendment's text doesn't actually say that it is limited merely to procedure.²²³ An "unreasonable" search need not be agnostic as to the type of crime or limited to a few procedural devices, such as warrants, probable cause, or reasonable suspicion. The type of crime, the dangers of particular forms of enforcement, and the nature of the government's power in a particular context could be factors in a more robust Fourth Amendment analysis.

In light of modern surveillance technology, Fourth Amendment jurisprudence is in need of a radical rethinking—with the problem of authoritarianism at the forefront. But even in authoritarian times, law enforcement is essential for a safe and well-functioning society. It is impractical and undesirable to ban government use of many modern surveillance technologies or completely restrict government access to personal data.²²⁴ An approach beyond all-or-nothing is needed.²²⁵

²²² *Id.* at 576.

²²³ Bambauer argues that Fourth Amendment should be interpreted to "cross the procedural/substantive divide." *Id.* at 578; see also Morgan Cloud, *Pragmatism, Positivism, and Principles in Fourth Amendment Theory*, 41 UCLA L. REV. 199, 200 (1993) (critiquing the "isolation" of the Fourth Amendment from other areas of law). See generally William J. Stuntz, *The Substantive Origins of Criminal Procedure*, 105 YALE L.J. 393 (1995) (discussing how the Fourth Amendment is not limited to criminal procedure).

²²⁴ See generally SLOBOGIN, *VIRTUAL SEARCHES*, *supra* note 127 (discussing the importance of modern data and surveillance to law enforcement).

²²⁵ Friedman, *supra* note 218, at 15.

4. Restoring Fourth Amendment Principles

When examined through the lens of standing up to an authoritarian government, current Fourth Amendment jurisprudence has drifted far from its original meaning and purpose. Modern Fourth Amendment jurisprudence is an incoherent jumble where arbitrary distinctions make the difference between protection and non-protection, where the Fourth Amendment's scope doesn't turn on how invasive, harmful, dangerous, or problematic various surveillance practices and technologies are. Instead, Fourth Amendment jurisprudence is a lawyer's parlor game of happenstance and luck, with core Fourth Amendment principles easily evaded by the tricks of new technologies.

The Fourth Amendment should be interpreted broadly to impose key values: "minimization, particularization, and control."²²⁶ First, information collection should be minimized. Broad investigations and the accumulation of vast amounts of personal data by government entities create significant risks for misuse and abuse, as previously discussed.

Second, data gathering efforts must be particularized in their focus rather than broad and sweeping. Preventing dragnet investigations is essential to ensuring that government investigatory powers are not misused against the general population.

Third, government information gathering and its subsequent use must be strictly controlled. There must be robust oversight to ensure that information collection remains minimized and particularized. Additionally, safeguards must be in place to prevent misuse of the data and to protect it from security breaches or unauthorized access.

Andrew Guthrie Ferguson laments that "the Fourth Amendment fails to address issues of error, racial bias, fairness, and transparency in policing generally, and facial recognition more specifically."²²⁷ The Fourth Amendment need not be interpreted in such a narrow way; courts can read its broad prohibition on "unreasonable searches and seizures" to encompass a myriad of problems with government surveillance.²²⁸ Keil Brennan-Marquez notes that the problems with government surveillance the Fourth Amendment was designed to protect against still exist when the government enlists the private sector to enhance its surveillance powers.²²⁹ Ultimately, Fourth Amendment protections should turn on whether there are problems involving government power, not

²²⁶ SOLOVE, THE DIGITAL PERSON, *supra* note 111, at 211; Daniel J. Solove, *Fourth Amendment Codification and Professor Kerr's Misguided Call for Judicial Deference*, 73 FORDHAM L. REV. 747, 775–77 (2005).

²²⁷ Andrew Guthrie Ferguson, *Facial Recognition and the Fourth Amendment*, 105 MINN. L. REV. 1105, 1109 (2021).

²²⁸ U.S. CONST. amend. IV.

²²⁹ Brennan-Marquez, *supra* note 140, at 485.

on inane distinctions and technicalities.²³⁰ In earlier work, I have proposed that the reasonable expectation of privacy test should not be used as the main approach to determine the scope of Fourth Amendment protection; a broader focus is needed.²³¹ As David Sklansky aptly argues: “Information is power, and keeping reasonable restraints on governmental power is an imperative for any liberal democracy—wholly aside from whether that power is accumulated or exercised in ways that impinge on privacy.”²³²

C. Applying Other Constitutional Provisions to Government Surveillance

The Fourth Amendment is not the only Constitutional provision that can limit government surveillance power. Barry Friedman proposes that many parts of the Constitution could be used to establish a “regulatory scaffolding” for government surveillance, such as the First Amendment, Second Amendment, Fifth Amendment, and substantive due process under the Fourteenth Amendment.²³³ Carmel Shachar and Carleen Zubrzycki point out that the constitutional right to information privacy can be a potential tool to provide protection.²³⁴ Although the right has generally not encompassed data collection, it has been held to involve the government’s use and disclosure of personal data.²³⁵

In earlier work, I proposed that the First Amendment provides protection from government data gathering on First Amendment activities—data relating to expression, association, political activities, religious beliefs, and the consumption of ideas.²³⁶ The First Amendment also should be considered as a source of criminal procedure, and it need not take on the baggage of crabbed Fourth Amendment interpretations, such as the third-party doctrine.²³⁷

Under current Fourth Amendment doctrine, the government has broad subpoena powers.²³⁸ It can use subpoenas to compel information from individ-

²³⁰ See generally Solove, *supra* note 210 (discussing the appropriate analysis for Fourth Amendment protection).

²³¹ *Id.* at 1511–13.

²³² David Alan Sklansky, *Too Much Information: How Not to Think About Privacy and the Fourth Amendment*, 102 CALIF. L. REV. 1069, 1121 (2014).

²³³ Friedman, *supra* note 103, at 1147, 1166–81.

²³⁴ See generally Carmel Shachar & Carleen Zubrzycki, *Informational Privacy After Dobbs*, 75 ALA. L. REV. 1 (2023) (discussing the value of the constitutional right to information privacy even in the wake of *Dobbs*).

²³⁵ DANIEL J. SOLOVE & PAUL M. SCHWARTZ, INFORMATION PRIVACY LAW 489–92 (8th ed. 2024). See generally *Whalen v. Roe*, 429 U.S. 589 (1977) (discussing a constitutional interest in avoiding disclosure of some personal data); *NASA v. Nelson*, 562 U.S. 134 (2011) (discussing the interests at stake in disclosing certain personal information during background checks).

²³⁶ Solove, *supra* note 210 (discussing the impact of the First Amendment on data collection).

²³⁷ Solove, *The First Amendment as Criminal Procedure*, *supra* note 70, at 114–15. In the context of public surveillance cameras, Slobogin argues that the First Amendment right to anonymous speech should buttress the Fourth Amendment and lead to protecting a right to anonymity in public free from the pervasive gaze of surveillance cameras. Slobogin, *supra* note 96, at 252–71.

²³⁸ Christopher Slobogin, *Subpoenas and Privacy*, 54 DEPAUL L. REV. 805, 805 (2005).

uals themselves, including sensitive documents and items such as diaries and other things. Ideally, there should be greater Fourth Amendment regulation of government subpoenas, but in the void, at least the First Amendment can be used to restrict subpoenas when they involve information about speech, belief, thought, association, and other related activities.²³⁹

The Constitution thus need not be read as a set of isolated fragments. Provisions of the Constitution work in tandem; they overlap and enhance each other. At its core, the Constitution is about establishing the governmental structure and rights of the people necessary to prevent tyranny. Fighting tyranny was the animating purpose of the American Revolution, a fact that must be at the heart of any interpretation of the Constitution.

D. Statutory Restrictions on Government Surveillance

In today's absence of reasonable Fourth Amendment protection against government surveillance, a patchwork of federal and state statutes imposes limited restrictions on government surveillance. Most of these statutory protections are significantly weaker than those of the Fourth Amendment, allowing access to information through subpoenas and court orders with minimal constraints and limited judicial oversight. Many categories of records remain entirely unprotected. The privacy statutes at the federal and state levels that regulate government surveillance must be significantly strengthened.

1. Updating the Electronic Communications Privacy Act

The Electronic Communications Privacy Act (ECPA) is the primary federal law that regulates how the government and private parties can monitor people's Internet use, wiretap their communications, peruse their email, gain access to their files, and much more.²⁴⁰ Unfortunately, the ECPA was written in 1986 in a manner very tightly connected to the technology at the time, creating massive complexity and confusion when the ECPA is applied to today's technologies.²⁴¹ As is the case with nearly all privacy laws, the U.S. Congress has failed to keep the ECPA up to date. Law enforcement has exploited the ECPA's weaknesses, ambiguities, and gaps.

The ECPA makes distinctions that are no longer meaningful today. For example, the ECPA provides much less protection to electronic data than to audio data. The ECPA is so focused on audio that it entirely fails to regulate

²³⁹ See generally Solove, *The First Amendment as Criminal Procedure*, *supra* note 70 (discussing how First Amendment protections can fill in the gaps in fourth amendment jurisprudence).

²⁴⁰ ECPA actually consists of three Acts: Wiretap Act, Electronic Communications Privacy Act, 18 U.S.C. §§ 2510–2522; Stored Communications Act, Electronic Communications Privacy Act, *Id.* §§ 2701–2711; and Pen Register Act, *Id.* §§ 3121–3127.

²⁴¹ Solove, *Reconstructing Electronic Surveillance*, *supra* note 160, at 1294–95.

silent video surveillance. The ECPA has the strongest protection when information is “intercepted” while in transmission but much more weakly protects data accessed when being stored.²⁴² The result is that a phone call is protected much more than an email.²⁴³ To make matters worse, the ECPA was drafted long before most people used cloud computing and webmail. According to an interpretation advanced by the U.S. government, once an email has been read, ECPA treats it as a file stored by a third party and obtainable with a mere subpoena.²⁴⁴

There should be more consistent protection for our communications and data. It shouldn’t matter whether we speak on the phone or send an email. It shouldn’t matter whether we keep our data stored on our home computer or on a third party’s computer.

The ECPA also makes a faulty distinction between content and envelope information. Envelope information consists of what people commonly put on the envelope—such as the mailing and return addresses. Envelope information is routing information. Content information consists of the contents of the communication—the letter inside the envelope. The ECPA protects content information much more stringently than envelope information, even though envelope information can be just as sensitive and important as content information. People might care more about protecting the information about whom they are communicating with than about protecting what they are saying.²⁴⁵ The distinction between content and envelope information doesn’t make sense with the internet, which “render[s] content/non-content distinctions functionally meaningless.”²⁴⁶

The ECPA also allows the government to obtain internet service provider (ISP) customer records with a court order that falls short of a warrant.²⁴⁷ Customer records can be quite sensitive, for they link people to their online activity.

Instead of building a law so tightly around technology that can change so rapidly, a wiser approach would be to craft a broader, more principles-based law. Instead of focusing on the form or location of the data, or how the data is obtained, the law should focus instead on the data we want to protect and our values. Although principles-based, the law need not be absolutist; it can and should still respond to practical considerations.

²⁴² *Id.* at 1281.

²⁴³ *Id.*

²⁴⁴ *Id.* at 1284.

²⁴⁵ *Id.* at 1286.

²⁴⁶ Steven M. Bellovin, Matt Blaze, Susan Landau & Stephanie K. Pell, *It's Too Complicated: How the Internet Opens Katz, Smith, and Electronic Surveillance Law*, 30 HARV. J.L. & TECH. 1, 5 (2016). See generally Matthew J. Tokson, *The Content/Envelope Distinction in Internet Law*, 50 WM. & MARY L. REV. 2105 (2009) (offering an additional critique of the content/envelope distinction).

²⁴⁷ To obtain the court order, the government need only provide “specific and articulable facts showing that there are reasonable grounds to believe that . . . the records or other information sought, are relevant and material to an ongoing criminal investigation.” 18 U.S.C. § 2703(d).

2. Restrictions on Government Access to Data

Government access to data maintained by the private sector must be regulated. The Fourth Amendment's staunch restrictions on dragnet searches become empty through what Barry Friedman and Danielle Citron call "indiscriminate data surveillance"—the government's obtaining and analyzing of massive stores of personal data.²⁴⁸

Most federal privacy laws lack strong restrictions on law enforcement access to consumer data.²⁴⁹ For example, under the Video Privacy Protection Act (VPPA) of 1988, law enforcement may obtain video records with just a "court order" that has less protections than a warrant.²⁵⁰ Under the Children's Online Privacy Protection Act (COPPA), the parental consent requirement does not apply to law enforcement access, meaning that records of children's online activities can be obtained by a mere subpoena.²⁵¹ Under the Gramm-Leach-Bliley Act, financial records may be obtained with a subpoena.²⁵² These are just a few examples.

Unlike warrants, subpoenas do not require probable cause and can be issued without a judge's approval.²⁵³ Subpoenas are barely reviewed, and scrutiny typically must be initiated by the target.²⁵⁴ As Professor William Stuntz contends, federal subpoena power is "akin to a blank check."²⁵⁵ Court orders issued under most statutes are only marginally more restrictive than subpoenas. They generally require a showing of mere "relevance" to an ongoing criminal investigation—a standard that is far less stringent and more ambiguous than the probable cause requirement for warrants.²⁵⁶

A federal law requiring a warrant for the government to access data maintained by companies would at least provide protections eviscerated by the third-party doctrine. Such a law would curtail the government's mass purchases of information from data brokers. Although it is unlikely that the federal government will pass such a law, the states could pass such laws. Although

²⁴⁸ Barry Friedman & Danielle Keats Citron, *Indiscriminate Data Surveillance*, 110 VA. L. REV. 1351, 1355 (2024). See generally Friedman, *supra* note 218 (discussing indiscriminate surveillance).

²⁴⁹ Erin Murphy, *The Politics of Privacy in the Criminal Justice System: Information Disclosure, the Fourth Amendment, and Statutory Law Enforcement Exemptions*, 111 MICH. L. REV. 485, 487 n.2 (2013) (noting that numerous federal privacy statutes contain "a provision exempting law enforcement from its general terms"); FERGUSON, *supra* note 194, at 17. See generally Solove, *Digital Dossiers*, *supra* note 4 (discussing the lack of strong privacy laws).

²⁵⁰ 18 U.S.C. § 2710(b)(2)(C).

²⁵¹ 15 U.S.C. § 6502(b)(2)(E).

²⁵² *Id.* § 6802(a), (b), (c)(5), and (e)(8).

²⁵³ See generally Solove, *Digital Dossiers*, *supra* note 4 (discussing the consequences of a subpoena standard for accessing information).

²⁵⁴ Slobogin, *supra* note 238, at 805–06.

²⁵⁵ William J. Stuntz, *O.J. Simpson, Bill Clinton, and the Transsubstantive Fourth Amendment*, 114 HARV. L. REV. 842, 864 (2001); Huq & Wexler, *supra* note 34, at 626.

²⁵⁶ Solove, *Digital Dossiers*, *supra* note 4, at 1150.

state laws restricting government access to personal data can't stop the federal government, they can prevent state governments from purchasing data from companies within their state.

3. Statutory Regulation of Government Use and Retention of Data

Privacy laws are tremendously weak on providing limitations and oversight of the government's use and retention of personal data. At the federal level, the Privacy Act of 1974 is charged with these goals.²⁵⁷ But the law is outdated, weak, and riddled with loopholes.²⁵⁸ For example, the Act often fails to reign in the use of personal data for new purposes, allowing a wide array of secondary uses under the "routine use" exception.²⁵⁹ This exception provides far too much leeway for the government to repurpose personal data.²⁶⁰

The Privacy Act also fails in effective enforcement. It can be difficult for people to find out enough information to determine whether their rights under the Act were violated. It is also quite difficult to sue for violations.²⁶¹ As Robert Gellman contends, "[i]ndividual enforcement does not offer any significant incentive for agencies to comply more carefully with the Privacy Act's provisions."²⁶² And, the Privacy Act applies only to federal agencies, leaving state and local governments outside its purview.

Only a few states have comparable laws to protect personal data maintained by state governmental entities.²⁶³ In addition to revamping and strengthening the federal Privacy Act, there must be laws in each state to regulate how government entities can not only gather personal data but also how they can use, retain, and disclose it.

4. Principle-Based Regulation of Government Use of Surveillance Technologies

Privacy laws should focus on broader principles so they can be readily adapted as technology evolves. As discussed above, privacy laws such as the ECPA are often built tightly around particular technologies, and these laws become obsolete too quickly. Effective laws focus on principles and goals rather than on the intricacies of particular technologies. Thus, "laws should focus

²⁵⁷ See generally 5 U.S.C. § 552a (governing individual privacy at the federal level).

²⁵⁸ See generally Robert Gellman, *Does Privacy Law Work?* (discussing the shortcomings of the Privacy Act of 1974), in *TECHNOLOGY AND PRIVACY: THE NEW LANDSCAPE* (Philip E. Agre & Marc Rotenberg eds., 1997).

²⁵⁹ 5 U.S.C. § 552a(b)(3).

²⁶⁰ See generally Gellman, *supra* note 258 (discussing the effects of the routine use exception).

²⁶¹ See generally *id.* (discussing the recourse available for violations of the Privacy Act).

²⁶² *Id.* at 201.

²⁶³ SOLOVE & SCHWARTZ, *supra* note 235, at 583.

less on how technology *works* and more on what technology *does*.”²⁶⁴ For instance, the U.S. Video Privacy Protection Act (VPPA) has a scope that applies not just to “video tapes”—the technology of 1988 when it was enacted—but also to “similar audio visual materials.”²⁶⁵ This forward-thinking language has enabled the VPPA to remain relevant as technology has evolved from video tapes to online streaming.

As a general goal, the law should ensure that all forms of government surveillance, no matter what the technology used, should be subject to reasonable oversight, accountability, and restraint. What is reasonable should be determined by focusing on power, not on technicalities or arbitrary distinctions.

Far too often, law enforcement collection and use of personal data and use of surveillance technologies is based on a *trust us* model. The law relies too much on the assumption that the government will not abuse its power, even though history teaches otherwise again and again. With scant transparency, accountability, oversight, or limitation, the law that regulates government surveillance mainly operates on a hope and a prayer that law enforcement officials will be good, restrained, thoughtful, and fair. Taking authoritarianism seriously means ending the law’s naïveté.

The default rule currently is that law enforcement officials can try whatever new technologies or investigative data gathering techniques they desire, with scant oversight or limitation. Courts will then examine whether these technologies and techniques are regulated by the Fourth Amendment, often concluding that they are not, due to antiquated Fourth Amendment jurisprudence. The U.S. Supreme Court provides barely any illumination or guidance, choosing to wait tepidly until some magical point in time when it feels comfortable that technology is settled (which it never is). This current approach to regulating government surveillance is deeply flawed. A better approach is to switch the default—to bar law enforcement from using new technologies or data gathering techniques unless authorized by law and governed by a comprehensive framework for oversight and accountability.²⁶⁶

²⁶⁴ See DANIEL J. SOLOVE, ON PRIVACY AND TECHNOLOGY 95 (2025).

²⁶⁵ 18 U.S.C. § 2710(a)(4).

²⁶⁶ See Kiel Brennan-Marquez & Stephen E. Henderson, *Fourth Amendment Anxiety*, 55 AM. CRIM. L. REV. 1, 33 (2018) (“[W]hen privacy and liberty norms are in flux, as they currently are given recent and rapid technological change, police *should* seek the assistance of legislatures in governing investigatory methods, and they *must* seek the approval of courts.”); Solove, *Reconstructing Electronic Surveillance*, *supra* note 160, at 1301 (“As technology continues to develop, the burden should be on law enforcement officials to convince Congress that a new device does not threaten individual privacy and that they should be authorized to use it with less than a warrant.”).

III. REGULATION OF SURVEILLANCE CAPITALISM

Improved regulation of government surveillance alone is insufficient to address the problem of authoritarianism and privacy. We live in a world, as Bernard Harcourt aptly observes, where “[d]igital technology is breaking down whatever semblance of boundaries existed—if they ever existed at all—between the state, the economy, and private existence.”²⁶⁷ Regulating government surveillance will be ineffective in today’s world where so much personal data is in the hands of companies and so many surveillance technologies and data analysis tools are being produced by the private sector.²⁶⁸

Even if the Fourth Amendment were to apply to the government’s buying of data from companies, and even if the third-party doctrine were to be overruled, the protection of privacy against authoritarianism would still fail. Authoritarian regimes can pass oppressive laws or enforce laws pretextually and then use Fourth Amendment warrants to obtain the data they need from companies. If states criminalize abortion, for example, then they can use warrants to investigate the crime. As Aziz Huq and Rebecca Wexler note, “[b]ecause so much patient activity occurs online, or alternatively generates a digital data trail, the antiabortion prosecutor (or, indeed, civil plaintiff under certain circumstances) is likely to begin their search not solely with eyewitness interviews or physical evidence but also by looking for the electronic traces of patient search.”²⁶⁹ Moreover, as Paul Ohm contends, “warrant and probable cause requirements are often quite toothless requirements that the government will be able to meet with ease.”²⁷⁰

Andrew Ferguson proposes what he terms the “tyrant test” to evaluate whether measures to regulate government surveillance are effective: “presuming the technology will be abused by a metaphorical tyrant, legal and institutional power structures can be developed to limit the potential harms before use.”²⁷¹ He is right—stopping authoritarianism is the most important goal for regulation of government surveillance.

But the job cannot be done without profound changes to the way the law regulates surveillance capitalism. Authoritarianism today is not just about government power; it involves a fusion of government and corporate power.²⁷² Consumer privacy, then, must be protected not only to ameliorate consumer

²⁶⁷ BERNARD HARCOURT, *EXPOSED: DESIRE AND DISOBEDIENCE IN THE DIGITAL AGE* 25–26 (2015).

²⁶⁸ Arnett, *supra* note 103, at 1418 (the “ability to regulate private companies will also play a tremendous role in responding to the surveillance of the BLM movement”).

²⁶⁹ Huq & Wexler, *supra* note 34, at 576.

²⁷⁰ Ohm, *supra* note 151, at 1347.

²⁷¹ Ferguson, *supra* note 42, at 214.

²⁷² Richards, *supra* note 70, at 1935 (“[A]ny solution [to government surveillance] must grapple with the complex relationships between government and corporate watchers.”).

harms but also to limit authoritarian power. Weak consumer privacy law is a boon for authoritarianism.

Unfortunately, in the U.S., the regulation of surveillance capitalism is a complicated patchwork of federal and state privacy laws, which leaves tremendous gaps and soft spots.²⁷³ Certain types of information are covered but not other types. Laws protect data if collected by certain types of entities but fail to protect the same data if other entities collect it.

The patchwork is just the tip of the iceberg. The problems with U.S. privacy law extend much deeper to foundational principles. The current data ecosystem creates massive incentives for companies to engage in what I will call “data maximization”—to gather as much data as they can and use it in as many ways as they can. As Danielle Citron notes, with much of the modern digital economy today, the “[o]vercollection [of personal data] is the business model.”²⁷⁴ Citron contends: “No matter what we do, we can’t shield ourselves from the ad-tech industrial complex.”²⁷⁵ All this data is ripe for an authoritarian regime to gather. There is not enough accountability for the harms of collecting, using, storing, or transferring personal data; nor is there sufficient accountability for the harms of developing surveillance technologies. As Paul Ohm argues, “[r]eversing or narrowing the third-party doctrine will help stem official arbitrariness, but it will not do enough to reverse the unprecedented increase in police power that the surveillance society has created.”²⁷⁶ The problem, as Ohm aptly diagnoses, along with Raymond Ku and others, is power.²⁷⁷ And today, government power and corporate power are deeply intertwined.

To truly protect against authoritarianism, privacy laws must make fundamental changes in the data economy. Right now, the law mainly lets businesses go on as they normally have been operating. The law just adds some speed bumps, headaches, and paperwork, plus penalties for violations that amount to paper cuts.²⁷⁸ Privacy law is far from a game changer, and it barely reduces the corporate appetite for data.

In this Part, I propose that the most impactful changes to the regulation of surveillance capitalism involve strong data minimization requirements; potent

²⁷³ See generally ARI EZRA WALDMAN, *ADVANCED INTRODUCTION TO U.S. PRIVACY LAW* (2023) (discussing the shortcomings of the current privacy law framework in the United States).

²⁷⁴ CITRON, *THE FIGHT FOR PRIVACY*, *supra* note 18, at 6.

²⁷⁵ *Id.* at 10.

²⁷⁶ Ohm, *supra* note 151, at 1332.

²⁷⁷ *Id.* at 1334; Raymond Shih Ray Ku, *The Founders’ Privacy: The Fourth Amendment and the Power of Technological Surveillance*, 86 MINN. L. REV. 1325, 1326–27 (2002) (arguing that the Fourth Amendment protects “power not privacy” and that current Fourth Amendment doctrine leaves far too much to the discretion of law enforcement officials).

²⁷⁸ See generally ARI EZRA WALDMAN, *INDUSTRY UNBOUND: THE INSIDE STORY OF PRIVACY, DATA, AND CORPORATE POWER* (2021) (discussing how privacy law does not do enough to place meaningful limits on the collection of information).

duties on entities that collect, use, and disclose personal data; restricting data flow; broader protection of confidentiality; recognizing privacy in public; and requiring privacy by design in surveillance technologies. Section A explains why current privacy laws are inadequate to stand up to authoritarian demands for personal data.²⁷⁹ Section B discusses the importance of data minimization.²⁸⁰ Section C argues for restricting transfers of data from private entities to the government.²⁸¹ Section D discusses the importance of confidentiality in privacy law.²⁸² Section E contends that privacy laws should better protect publicly available information.²⁸³ Section F argues that states should enact more robust privacy laws.²⁸⁴ Finally, Section G discusses how consumer privacy laws can play an important role in regulating government surveillance.²⁸⁵

A. Beyond the Individual Control Model

Existing approaches in many U.S. consumer privacy laws are woefully inadequate to address the problem of controlling the flow of personal data from companies to the government.

1. The Failure of the Notice-and-Choice Approach

Many U.S. privacy laws follow an approach known as notice and choice. Companies can essentially do whatever they want as long as they bury a statement about it in a privacy notice. In some circumstances, privacy laws demand that people have a right to opt out, but hardly anyone does so because they do not read the privacy notice and do not understand the risks.²⁸⁶ The notice-and-choice approach is essentially self-regulation with weak and blunt regulatory teeth to give it the façade of legitimacy.

The notice-and-choice approach has been pummeled by the vast majority of commenters as being an utter failure at protecting privacy.²⁸⁷ This approach does

²⁷⁹ See *infra* notes 286–318.

²⁸⁰ See *infra* notes 319–326.

²⁸¹ See *infra* notes 327–337.

²⁸² See *infra* notes 338–353.

²⁸³ See *infra* notes 354–372.

²⁸⁴ See *infra* notes 373–376.

²⁸⁵ See *infra* notes 377–388.

²⁸⁶ Daniel J. Solove, *The Limitations of Privacy Rights*, 98 NOTRE DAME L. REV. 975, 985 (2023) [hereinafter Solove, *Limitations of Privacy Rights*].

²⁸⁷ See Barrett, *supra* note 165, at 74 (critiquing notice-and-choice as “incapable of fostering informed and meaningful decision-making”); Daniel J. Solove & Woodrow Hartzog, *Kafka in the Age of AI and the Futility of Privacy as Control*, 104 B.U. L. REV. 1021, 1035 (2024) (explaining the shortcoming of allowing people to manage their own privacy) [hereinafter Solove & Hartzog, *Kafka in the Age of AI*]; Charlotte A. Tschider, *Meaningful Choice: A History of Consent and Alternatives to the Consent Myth*, 22 N.C. J.L. & TECH. 617, 622 (2021) (discussing the problems with notice-and-choice).

hardly anything to limit the collection or use of personal data. Companies can just strategically list purposes of use that are broad enough to allow them to collect and use massive quantities of personal data however they please. When new uses emerge, they can just adjust their purposes to encompass these uses.

Despite the widespread recognition of the bankruptcy of the notice-and-choice approach, nearly all the state consumer privacy laws being passed since 2018 are based on this approach.²⁸⁸ As a result, they fail to reign in the collection and use of personal data or the transfer of it to government officials. Privacy notices are no match for governments thirsty for data. Indeed, many privacy notices contain language that states that companies can share personal data with law enforcement authorities or when needed in litigation.²⁸⁹ Even if privacy notices promised that companies would not provide personal data to the government, companies can't stop the government from compelling the data via a subpoena or other legal process much weaker than a warrant. Under the logic of the third-party doctrine, the promises of a privacy notice not to share data are irrelevant.²⁹⁰ Even binding contractual provisions that state that data can't be disclosed to others are unable to stand in the way of government demands for data. The only way for the government not to obtain the data is for the data not to exist.

2. The Failure of Privacy Self-Management

Most privacy laws rely on an approach that I have termed “privacy self-management.”²⁹¹ This approach attempts to give people control over their personal data, but such control is not possible in today's age of vast data collection and complex technologies such as AI.²⁹²

a. The Limitations of Privacy Rights

Privacy laws rely heavily on individual privacy rights, where people can access, correct, or delete their data that companies hold or where people can opt out of or opt into certain uses.

²⁸⁸ Solove & Hartzog, *Kafka in the Age of AI*, *supra* note 287, at 1029.

²⁸⁹ See, e.g., Medtronic Privacy Notice, MEDTRONIC (Oct. 2024), <https://www.medtronic.com/en-us/privacy-notice.html> [https://perma.cc/9DZK-74P2] (stating that personal data may be disclosed when the company is “[r]equired to disclose and/or share your personal data with regulatory, public, or governmental authorities to comply with any law, regulation, court order, legal, or government request”).

²⁹⁰ See generally DANIEL J. SOLOVE, NOTHING TO HIDE: THE FALSE TRADEOFF BETWEEN PRIVACY AND SECURITY (2011) (explaining the third-party doctrines impact on the government's ability to access data).

²⁹¹ *Privacy Self-Management*, *supra* note 10, at 1880.

²⁹² Dennis D. Hirsch, *From Individual Control to Social Protection: New Paradigms for Privacy Law in the Age of Predictive Analytics*, 79 MD. L. REV. 439, 462 (2020). See generally Solove & Hartzog, *Kafka in the Age of AI*, *supra* note 287 (discussing the impact of AI on privacy rights).

Unfortunately, individual privacy rights are ineffective. People rarely know about them or use them. People can't figure out all the companies that have data about them and have the time to request deletion of that data.²⁹³ Although data removal service companies have arisen to submit deletion requests on behalf of individuals,²⁹⁴ these services cost money and only a fraction of consumers use them.

Data collection is ongoing, and so deletion requests must routinely be made. As Molly Cinnamon observes: "Attempting to scrub one's Internet presence is a Hydra-like problem: although some sites allow users to request removal of their data, these hundreds, if not thousands, of data broker sites continuously repopulate their offerings by re-pulling their sources."²⁹⁵

Moreover, many laws do not require the data to be deleted until the data is no longer necessary for the purpose for which it was collected, or under other statutory exceptions. It is unreasonable to assume that people will keep checking in with a company to ask: "Have you finished yet?"

California's Delete Act attempts to regulate data brokers by giving individuals a more unified right to delete.²⁹⁶ A data broker is "a business that knowingly collects and sells to third parties the personal information of a consumer with whom the business does not have a direct relationship."²⁹⁷ The Act mandates that data brokers register with the state and provide a way for individuals to make a single delete request for all data brokers.²⁹⁸ Although this law addresses the problem of the scale and complexity of making delete requests to numerous companies, it has several limitations. The law only applies to data brokers, so the government could obtain the data from other companies. Data brokers are only one segment of the vast network of companies that gather and maintain personal data. The law excludes consumer reporting agencies that are regulated by the federal Fair Credit Reporting Act (FCRA).²⁹⁹ But consumer reporting agencies are enormous collectors of personal data, and the FCRA lacks a right to delete.

Ultimately, empirical evidence shows that a very small percentage of individuals use privacy rights of any sort.³⁰⁰ People should not have to spend time trying to figure out how to delete all their data trails like paranoid hermits.

²⁹³ Solove, *The Limitations of Privacy Rights*, *supra* note 286, at 985.

²⁹⁴ Molly Cinnamon, *You Have the Right to Be Deleted: First Amendment Challenges to Data Broker Deletion Laws*, 9 GEO. L. TECH. REV. 492, 503 (2025).

²⁹⁵ *Id.* at 495.

²⁹⁶ California Delete Act, SB-362, CAL. CIV. CODE § 1798.99.86 (West 2025).

²⁹⁷ *Id.* § 1798.99.80(c).

²⁹⁸ *Id.* § 1798.99.86(d)(1).

²⁹⁹ *Id.* § 1798.99.80 (c)(1); 15 U.S.C. § 1681 et seq.

³⁰⁰ Ella Corren, *Gaining or Losing Control: An Empirical Study on the Real Use of Data Control Rights and Policy Implications*, 109 IOWA L. REV. 2017, 2023 (2024) ("[F]or an overwhelming major-

b. *The Failure of Consent*

Consent also fails to work.³⁰¹ Opt-out consent is farcical, as the notion that one who fails to opt out somehow consents is absurd. Hardly anyone reads privacy notices.³⁰² Even with express consent (opt in), people readily consent to the collection and use of their personal data without reading the fine print of privacy notices.³⁰³

State consumer privacy laws rely heavily on consent, attempting to single out certain categories of personal data that are deemed to be “sensitive” and require opt in consent rather than opt out consent. Beyond the problem that people can readily be induced to consent to practices that they don’t fully understand, protecting only sensitive data fails to account for the power of inference. With modern data analysis, it is possible to infer sensitive information from even the most mundane personal data.³⁰⁴

Any solution to this problem can’t rely on simplistic distinctions between sensitive and non-sensitive data.³⁰⁵ I have proposed that despite being a well-meaning provision in privacy laws, the sensitive data delineation is ultimately unworkable. Privacy law should focus on risk and harm. Inferences about pregnancy, gender-affirming healthcare, immigration status, and other matters can be made from countless types of data. Trying in advance to identify sensitive data and single it out for heightened protection is bound to fail.

In the EU, the General Data Protection Regulation (GDPR) has a more robust requirement of consent, requiring express consent (opt in).³⁰⁶ But opt in consent still relies heavily on individuals being able to understand the risks of permitting the collection, use, and disclosure of their data. Individuals are not able to assess the risks of consenting; the downstream consequences of consenting are too hard to prognosticate in the present. Without expertise in data

ity of firms—roughly eighty percent—no more than 1 in 1,000 consumers a year (0.1 percent) have used their rights to know, to delete, or to opt-out.”).

³⁰¹ Neil Richards & Woodrow Hartzog, *The Pathologies of Digital Consent*, 96 WASH. U. L. REV. 1461, 1463 (2019) (discussing the failure of notice and choice); Helen Nissenbaum, *A Contextual Approach to Privacy Online*, 140 DAEDALUS 32, 34 (2011) (explaining that notice and choice ultimately has failed). See generally Daniel J. Solove, *Murky Consent: An Approach to the Fictions of Consent in Privacy Law*, 104 B.U. L. REV. 593 (2024) (discussing the failure of consent to adequately protect privacy) [hereinafter Solove, *Murky Consent*]; Richard Warner & Robert Sloan, *Beyond Notice and Choice: Privacy, Norms, and Consent*, 14 J. HIGH TECH. L. 370 (2014) (explaining why notice and choice is inadequate); Ella Corren, *The Consent Burden in Consumer and Digital Markets*, 36 HARV. J.L. & TECH. 551 (2023) (discussing consent in the context of consumer and digital transactions); Tschider, *supra* note 287 (explaining that consent does not always provide a meaningful choice in the privacy context).

³⁰² Solove, *Murky Consent*, *supra* note 301, at 607.

³⁰³ *Id.*

³⁰⁴ Solove, *Data Is What Data Does*, *supra* note 12, at 1099.

³⁰⁵ Anya E.R. Prince, *Reproductive Health Surveillance*, 64 B.C. L. REV. 1077, 1136–37 (2023).

³⁰⁶ Council Regulation 2016/679, 2016 O.J. (L 119) 1, 37 [hereinafter GDPR].

analytics, people can't comprehend all the inferences that could be made based on the data they share. Without legal training, most people don't understand the ease with which government officials can gain access to their data. Even with legal training, people lack enough information about whether companies will fight government demands for their data or, if they do contest these demands, how effectively they will do so.

3. An Example of the Problems with Privacy Laws: Health Data

Health data provides a strong example of the problems with existing privacy laws. After the Supreme Court's 2022 decision in *Dobbs v. Jackson Women's Health Organization*, there were many concerns about state governments obtaining health data about people seeking abortions. Changes were made to HIPAA and state laws were passed. These moves certainly advanced the goals of protecting health data, but these efforts still fall short because of problems in the overall system and approach to privacy laws. To understand why, one must understand the way that privacy laws operate as a patchwork and the underlying flawed privacy self-management model that most privacy laws have.

Under the Health Insurance Portability and Accountability Act (HIPAA) regulations, law enforcement officials can obtain medical records with a mere subpoena.³⁰⁷ Additionally, HIPAA allows health data to be disclosed "in response to a law enforcement official's request for such information for the purpose of identifying or locating a suspect, fugitive, material witness, or missing person."³⁰⁸

In April 2024, in response to *Dobbs* and the overturning of the Constitutional right to abortion, the Department of Health and Human Services issued the HIPAA Privacy Rule to Support Reproductive Health Care Privacy.³⁰⁹ The rule prohibits the use or disclosure of "protected health information" (PHI) under HIPAA by a healthcare provider, plan or clearinghouse (or by a business associate) to conduct investigations into "seeking, obtaining, providing or facilitating reproductive health care, where such healthcare is lawful under the circumstances in which it is provided."³¹⁰ The rule further prohibits the "identification of any person for the purpose of conducting such investigation."³¹¹ These investigations can be for violations of criminal law or for civil lawsuits. Essentially, HIPAA ordinarily has a *may-disclose* rule for disclosures of PHI,

³⁰⁷ 45 C.F.R. § 164.512(f)(1)(ii) (2001).

³⁰⁸ *Id.* § 164.512(f)(2).

³⁰⁹ HIPAA Privacy Rule to Support Reproductive Health Care Privacy, 89 Fed. Reg. at 32976 [hereinafter Rule to Support Reproductive Health Care Privacy].

³¹⁰ *Id.*

³¹¹ HIPAA PRIVACY RULE FINAL RULE TO SUPPORT REPRODUCTIVE HEALTH CARE PRIVACY: FACT SHEET, <https://www.hhs.gov/hipaa/for-professionals/special-topics/reproductive-health/final-rule-fact-sheet/index.html> [https://perma.cc/45XP-UBT2].

but the reproductive healthcare rule changes this to a *must-not disclose* rule. This rule was subsequently invalidated.³¹²

Even had this rule stood, its limitations were significant. The rule only applied to reproductive healthcare, but health data can be of interest to the government for many other purposes, such as gender-affirming care and vaccines. The rule only applied to PHI under HIPAA, which covers only health data originating from health plans, health care clearinghouses, and health care providers.³¹³ Health apps and websites can have extensive amount of health data that is not covered by HIPAA.³¹⁴ For example, DNA services like 23andMe are not covered by HIPAA. Nor are devices such as fitness watches or online groups where people discuss health conditions. Health data can readily be obtained from other sources, such as online browsing and stores. Data brokers can supply location tracking data. Data can also be obtained from rental car companies, ride sharing companies (Uber or Lyft), or car insurance companies that have discount driving monitoring and tracking programs.³¹⁵

Some states are attempting to address HIPAA's limitations by passing laws to fill in the gaps. HIPAA does not preempt states in providing broader and stronger protections to health data. After *Dobbs*, a few states passed health privacy laws in an attempt to protect reproductive and gender-affirming healthcare data. The strongest of these laws is the Washington My Health My Data Act (MHMDA).³¹⁶ The law provides consumers with a right to know about health data that companies possess as well as the third parties with whom the data has been shared. People have a right to delete the data. The MHMDA is notable for its very potent deletion right that lacks many of the exceptions found in other privacy laws. Additionally, it attempts to define health data broadly to account for inferences, though it does not broadly protect all data that could give rise to inferences about health, as this could technically be any personal data.³¹⁷

To its credit, the MHMDA requires very strict consent for the selling of personal data, so this could curtail the sale of such data to the government. But if a company has a person's health data, the government (or private litigant) can compel its disclosure with a subpoena, court order, or warrant. The main

³¹² See generally *Purl v. U.S. Dep't of Health & Hum. Servs.*, 787 F. Supp. 3d 284 (N.D. Tex. 2025) (invalidating the HIPAA rule); Stephen Murphy, *HIPAA Reproductive Health Rule Overturned*, NETWORK FOR PUB. HEALTH L. (July 8, 2025), <https://www.networkforphl.org/news-insights/hipaa-reproductive-health-rule-overturned/> [https://perma.cc/B8E4-HLD7].

³¹³ 45 C.F.R. § 160.102 (2001).

³¹⁴ Prince, *Reproductive Health*, *supra* note 305, at 1123–28.

³¹⁵ Wilson Kehoe Winingham Staff, *Legal Risks of Using Car Insurance Tracking Devices* (Apr. 1, 2024), <https://www.wkw.com/car-insurance-trackers/> [https://perma.cc/WL56-QDQL].

³¹⁶ See generally WASH. REV. CODE § 19.373.010 (2024) (providing a robust health data privacy framework).

³¹⁷ See generally *id.* (defining health data broadly).

protection against this is the MHMDA's right to delete. The MHMDA and other state health privacy laws, though, typically work on a privacy self-management model, placing the onus on individuals to exercise rights under the law. The data remains unless individuals request its deletion. People might not know that their health data is being collected. People might also not want to delete their data because they are actively using an app or service, and it might become too late to delete the data after it is demanded in an investigation.

Another big limitation of the MHMDA is that it excludes data regulated by many federal laws, such as the Gramm-Leach-Bliley Act (GLBA), the Family Educational Rights and Privacy Act (FERPA), and the Fair Credit Reporting Act (FCRA).³¹⁸ Some of this data could involve health or be used to make inferences about health. The MHMDA is also limited to health data and thus will not provide protection against other types of government inquests beyond health.

Ultimately, the MHMDA is a strong law, but far from enough. Without broad regulation of the entire data ecosystem, laws can only erect fragmented and incomplete protections against government access to personal data. Laws like the MHMDA close some doors to government access, but many other doors remain open.

B. Data Minimization

The best way to protect against authoritarian government officials' obtaining and using personal data is for companies not to have it. If the data doesn't exist or can't be accessed, then it can't be abused.³¹⁹ The most effective and powerful thing that privacy law can do is to push companies to minimize the collection, use, and disclosure of personal data—a privacy principle known as “data minimization.”³²⁰ Data minimization encompasses curtailing the data that is collected, using data only for necessary purposes and avoiding using data for unrelated secondary purposes, and not retaining data for longer than necessary to achieve the purposes of collection.

Unfortunately, privacy law mostly fails quite miserably at data minimization. Many laws often state data minimization as a principle—to collect personal data that is reasonably necessary for specified purposes—but this principle rings hollow in practice. Market incentives still strongly encourage data maximization, and the law does little to change these incentives and only weakly pushes back. The incentives are incredibly powerful to collect copious quantities of personal data and to use it as widely and aggressively as possible.

³¹⁸ *Id.*

³¹⁹ See generally SOLOVE & HARTZOG, *supra* note 154 (discussing the failure of data protection in the current legal landscape).

³²⁰ Helena Engfeldt & Elisabeth Dehareng, *Data Minimization: An Increasingly Global Concept*, IAPP (May 7, 2024), <https://iapp.org/news/a/data-minimization-an-increasingly-global-concept> [<https://perma.cc/J7KC-B3VK>].

For example, the recent boom in AI has led to a tremendous thirst for personal data, with companies scraping up massive quantities of personal data from the internet or purchasing it from other companies.³²¹ If companies forgo collecting personal data, the cost could be failing to keep up with the AI rat race, falling hopelessly behind, and eventually going bankrupt. If companies do not monetize personal data, they might fail to earn enough money to satisfy their investors. On the flip side, success can propel the founders of companies to become billionaires and give them unparalleled access to the levers of government power. With such enormous stakes, companies will not be deterred by vague laws that mostly rely on self-restraint.

State privacy laws have generally used what I call “self-defined data minimization”—requiring that data be necessary for whatever purposes of collection a company specifies. As long as the collection, use, disclosure, or retention of the data is relevant to the stated purposes, it is generally permissible. This approach is not particularly limiting, as companies can readily define their purposes to encompass a broad array of uses. Self-defined data minimization is little more than notice-and-choice adorned by a data minimization principle that is more decorative than potent.

Maryland recently passed a consumer privacy law with a different approach—what I call “use-based data minimization”—requiring that data be necessary for the services a consumer has requested.³²² Personal data must be limited to what is “reasonably necessary and proportionate” to “provide or maintain a specific product or service requested by the consumer to whom the data pertains.”³²³ Consumers cannot be made to consent around this requirement. In other words, even if consumers consent to more widescale data collection, this limit still applies. This prevents consent from being used as an end-run around data minimization.

Under Maryland’s law, data minimization is even tighter for sensitive data. Controllers cannot process sensitive data unless it is “strictly necessary” to “provide or maintain a specific product or service requested by the consumer.”³²⁴ The sale of sensitive data is prohibited regardless of whether people consent.

In comparison to self-defined data minimization, use-based data minimization provides less flexibility for companies to broadly define their purposes to allow for largescale data collection and a wide range of uses. With use-based data minimization, regulators have more power to force companies to curtail data collection, use, disclosure, and retention.

³²¹ Solove & Hartzog, *supra* note 95, at 1521 (explaining the recent trends of data collection in light of AI).

³²² MD. CODE ANN., Maryland Online Data Privacy Act, §§ 14-4601 to -4614 (LexisNexis 2024).

³²³ *Id.* § 14-4607(B).

³²⁴ *Id.* § 14-4607(A).

Data minimization is like dieting—to be done right, there must be a life-style change. Companies must find ways to do business without gorging on data. Far too often, privacy laws fail to account for this reality. The laws operate as if merely telling companies to slim down a bit will somehow work. But what is really needed is a more radical paradigm shift, which is not happening. Being slightly leaner on the amount of data a company hoards fails to address the magnitude of the problem. Ultimately, to be effective, privacy law must stand up to the market incentives and operate as a stronger force. Weakly whispering “restraint” is not going to stop a pride of hungry lions.

Overall, companies are collecting far too much personal data, storing it for far too long, selling and sharing it far too widely, and using it for far too many purposes. The problem is that the basic model for many modern technologies is to monetize through data collection and use, often for advertising and increasingly for training AI systems.³²⁵ Nearly all online activity is monitored, from the way people navigate sites to the posts they like to the videos they watch. For example, a 2024 FTC report on large social media platforms concluded that the “amount of data collected by large tech companies is simply staggering.”³²⁶

People on the internet are like rats in a glass cage in a lab. Their every movement and twitch is monitored. We should not be surprised by all this; in fact, it is naïve to hope that companies will be restrained when the incentives to gather and keep data are overpowering.

C. Restricted Data Transfer to the Government

To protect against authoritarian uses of personal data, laws must restrict the sale of personal data to the government and provide strict controls on government access. In the previous Part, I discussed how laws should regulate when and how the government can buy or access personal data maintained by companies. A flip side to this protection is to regulate when and how companies can sell or provide personal data to the government. Regulation is most effective when it is on both sides of the coin.

In 2024, the Consumer Financial Protection Bureau (CFPB) proposed a rule to classify data brokers as consumer reporting agencies subject to the Fair Credit Reporting Act (FCRA).³²⁷ Such a step would help to some degree, as it would bring a regulatory framework to the data broker industry. Under the FCRA, however, the government can still readily obtain information from con-

³²⁵ ZUBOFF, *supra* note 3, at 132.

³²⁶ FEDERAL TRADE COMMISSION, A LOOK BEHIND THE SCREENS: EXAMINING THE DATA PRACTICES OF SOCIAL MEDIA AND VIDEO STREAMING SERVICES, at i (Sep. 2024).

³²⁷ Jon Brodtkin, *US Plan to Protect Consumers from Data Brokers Faces Dim Future Under Trump*, ARS TECHNICA (Dec 3, 2024), <https://arstechnica.com/tech-policy/2024/12/us-plan-to-protect-consumers-from-data-brokers-faces-dim-future-under-trump/> [<https://perma.cc/VD25-MT38>].

sumer reporting agencies.³²⁸ And although data brokers are a significant source of personal data to the government, they are just one group of companies from which the government can obtain personal data. Ultimately, this rule will likely not be promulgated by the Trump Administration.

Several states have laws attempting to regulate data brokers, such as California, Vermont, Texas, and Oregon.³²⁹ Unfortunately, these data broker laws are not broad or powerful enough. These laws should not only cover data brokers but all companies where the government can procure personal data.³³⁰ The law should generally restrict the sale of all types of personal data to government entities unless particular exceptions apply. The default rule should be no sale.

Data broker laws are also weakened by relying too heavily on privacy self-management. Many laws mainly require data brokers to register with the state, but little else. Given weak enforcement and anemic penalties, many data brokers aren't even bothering to register.³³¹ The most powerful of these laws, California's Delete Act, attempts to enhance the state's data broker regulation by also giving consumers a right to delete.³³² But this still puts the onus on individuals to clean up their data. Most individuals will fail to delete their data or opt out. People often don't think about the risks, understand the data ecosystem, or know about how their data is being peddled in a clandestine bazaar.

Other state consumer privacy laws seek to protect certain types of personal data that are deemed to be "sensitive" with heightened protections, such as requiring opt in rather than opt out for the selling or sharing of data.³³³ But in today's world of Big Data, sensitive data can readily be inferred from non-sensitive data. It is impossible to readily single out particular categories of data.³³⁴ Moreover, opt in requirements are based upon the flawed consent model in privacy; people rarely understand the risks or can make an informed decision at the time they are asked to consent.³³⁵

Currently, when the government issues a subpoena or court order to a company demanding a customer's data, it is mostly within the company's dis-

³²⁸ 15 U.S.C. § 1681(f).

³²⁹ Cinnamon, *supra* note 294, at 495–96.

³³⁰ Under the California Delete Act, data brokers are businesses that sell personal data about individuals they don't have a direct relationship with. CAL. CIV. CODE § 1798.99.80(c) (West 2025).

³³¹ Suzanne Smalley, *Delete-Your-Data Laws Have a Perennial Problem: Data Brokers Who Fail to Register*, THE RECORD (Oct. 17, 2023), <https://therecord.media/state-data-broker-registries-california-vermont> [<https://perma.cc/59H6-UFZD>].

³³² Delete Act, CAL. CIV. CODE §§ 1798.100–199.100 (West 2025).

³³³ Bryan Cave Leighton Paisner LLP, 'Sensitive Personal Information'—*Understanding and Complying with the New Rules in the United States* (Feb. 16, 2023), <https://www.bclplaw.com/en-US/events-insights-news/sensitive-personal-information-understanding-and-complying-with-the-new-rules-in-the-united-states.html> [<https://perma.cc/A4BS-PR7K>].

³³⁴ Solove, *Data Is What Data Does*, *supra* note 12, at 1127.

³³⁵ See generally Solove, *Murky Consent*, *supra* note 301 (explaining the drawbacks of a consent based privacy system).

cretion whether to challenge the demand or even notify the customer.³³⁶ Privacy laws should require companies to notify individuals and challenge government demands for personal data, and these laws should extend far beyond reproductive healthcare.³³⁷

D. Protection of Confidentiality

1. Confidentiality of Relationships and Information Fiduciaries

We need a robust protection of confidentiality in relationships, something that U.S. privacy law has failed to do with sufficient breadth and rigor. Except for a few professional relationships, such as doctor-patient and lawyer-client, many relationships are unprotected. When a person shares a secret with family members and friends, the general rule in U.S. law is that the person runs the risk of betrayal. In contrast, the law in the United Kingdom is far more protective of confidentiality and protects these relationships.³³⁸ In many real and literary dystopias, authoritarian societies create a world where people do not trust their friends and family. Such dystopias can be avoided by safeguarding confidentiality in personal relationships.³³⁹ U.S. law can strengthen protection of these relationships by recognizing them as encompassed within the breach of confidentiality tort, as well as by evidentiary privileges. For example, in most states, privileges protect spouses, but not parents and children, which means that parents and children can be forced to divulge information about each other.³⁴⁰ This would mean that the government can compel a parent to divulge information about a child's abortion or gender-affirming care. States should recognize parent-child privileges and not force parents and children to provide evidence against each other.

Huq and Wexler propose that "federal and state legislatures should enact statutory evidentiary privileges that not only protect abortion-relevant data from voluntary disclosure but also make that data immune from law enforcement and judicial compulsory legal process alike."³⁴¹ Although a state privilege would only apply to courts in that state, it "would still be valuable because it could bar courts in those states from enforcing cross-jurisdictional subpoenas, warrants, or other court orders that originate in [abortion] restrictionist states."³⁴² I agree

³³⁶ Huq & Wexler, *supra* note 34, at 626.

³³⁷ *Id.* at 628 (recommending that companies voluntarily notify individuals and challenge government demands for data). I go further and contend that the law should mandate these things.

³³⁸ Neil M. Richards & Daniel J. Solove, *Privacy's Other Path: Recovering the Law of Confidentiality*, 96 GEO. L.J. 123, 158–59 (2007).

³³⁹ *Id.*

³⁴⁰ SOLOVE & SCHWARTZ, *supra* note 235, at 420.

³⁴¹ Huq & Wexler, *supra* note 34, at 635–36.

³⁴² *Id.* at 641.

with this proposal, but I would extend it beyond abortion to all other matters that could be targeted by authoritarian governments.

Additionally, an information fiduciary approach to privacy law would greatly help safeguard personal data.³⁴³ This approach seeks to extend fiduciary law principles to companies that collect and manage personal data. A fiduciary relationship is built on trust or confidence placed by one party in the integrity and loyalty of another. The law forbids fiduciaries from exploiting the relationship for personal gain or to the detriment of the other.³⁴⁴ Companies handling personal data should be seen as fiduciaries. Redefining these relationships in fiduciary terms could drive a major shift in legal obligations, requiring businesses to treat personal data with greater care and respect. This shift would reshape the foundation of the information economy, fostering stronger protections for individuals' privacy.³⁴⁵

Fiduciary relationships would impose special duties on companies that maintain personal data. For example, Neil Richards and Woodrow Hartzog contend that companies should owe the individuals whose data they collect a duty of loyalty—to put the individuals' interests above their own.³⁴⁶ Another key fiduciary duty is a duty of confidentiality. As I have argued, along with Neil Richards, this duty should be imposed on organizations that collect and maintain personal data.³⁴⁷ Such a duty could be used to close a gap with data broker laws, that focus on companies that lack direct relationships with individuals. A duty of confidentiality would apply to companies with relationships to individuals, and it would bar them from selling personal data to the government. The duty could be used to force companies to challenge government

³⁴³ Daniel J. Solove, *Information Fiduciaries and Privacy*, TEACHPRIVACY (Nov. 26, 2024), <https://teachprivacy.com/information-fiduciaries-and-privacy/> [<https://perma.cc/7947-TNU6>].

³⁴⁴ See, e.g., *Mobile Oil Corp. v. Rubinfeld*, 339 N.Y.S.2d 623, 632 (Civ. Ct. 1972) (finding that where a fiduciary relationship exists, “relief is granted in all cases in which influence has been acquired and abused, in which confidence has been reposed and betrayed”), *rev’d on other grounds*, 48 A.D.2d 428 (N.Y. 1975).

³⁴⁵ SOLOVE, *THE DIGITAL PERSON*, *supra* note 111, at 101–04. See generally Jack M. Balkin, *Information Fiduciaries and the First Amendment*, 49 U.C. DAVIS L. REV. 1183 (2016) (explaining fiduciary relationships in privacy law and the First Amendment); Alicia Solow-Niederman, *Beyond the Privacy Torts: Reinventing a Common Law Approach for Data Breaches*, 127 YALE L.J.F. 614 (2018), <https://yalelawjournal.org/forum/beyond-the-privacy-torts> [<https://perma.cc/LP8J-3FRV>] (discussing the possible common law solutions for breaches of trust in privacy law); Lauren Henry Scholz, *Fiduciary Boilerplate: Locating Fiduciary Relationships in Information Age Consumer Transactions*, 46 J. CORP. L. 143 (2020) (explaining the duty of loyalty that firms should owe to their customers); Lindsey Barrett, *Confiding in Con Men: U.S. Privacy Law, the GDPR, and Information Fiduciaries*, 42 SEATTLE U. L. REV. 1057 (2019) (discussing fiduciary relationships in the privacy context).

³⁴⁶ See generally Neil Richards & Woodrow Hartzog, *A Duty of Loyalty for Privacy Law*, 99 WASH. U. L. REV. 961 (2021) (discussing how companies should owe a duty of loyalty to those whose data they collect).

³⁴⁷ See generally Richards & Solove, *supra* note 338 (arguing that there should be a duty of confidentiality imposed on companies that store data).

demands for personal data.³⁴⁸ In combination, the fiduciary duties could be used to mandate that companies consider and mitigate the risks and harms that might befall their customers from government access to data.

2. Protection of Confidentiality of Media Sources

Certain dimensions of press freedom are intertwined with privacy—in particular, the confidentiality of sources and communications. The media is on the front lines of defending against authoritarianism, and journalists depend upon being able to obtain information from sources. Protection of the confidentiality of sources is essential to ensuring the candid flow of information that exposes the abuses of authoritarian regimes.

In the waning days of 2024, the U.S. Congress attempted to pass the Press Act, a bill that “protects from disclosure any information identifying a source, as well as any records, contents of a communication, documents, or information obtained or created by journalists in the course of their work.”³⁴⁹ The effort, unfortunately, failed.

If Congress cannot succeed in enacting protections, then states should step in and enact their own protections. Private litigants and even government officials can bring dubious lawsuits to attack critics. For example, Elon Musk’s social media platform X sued a group of disinformation researchers.³⁵⁰ Musk also sued watchdog group Media Matters for its reporting that X was pairing Nazi content with the ads of high-profile advertisers.³⁵¹ Donald Trump has also brought many defamation lawsuits, a strategy he uses to “straighten out the press.”³⁵² These lawsuits could be used to pry information about sources from the media.

³⁴⁸ Kiel Brennan-Marquez argues that “where private actors operate as information fiduciaries, law enforcement should not have carte blanche to demand their cooperation; nor should private actors that serve as information fiduciaries be free—without bound—to assist law enforcement voluntarily.” Kiel Brennan-Marquez, *Fourth Amendment Fiduciaries*, 84 FORDHAM L. REV. 611, 659 (2015).

³⁴⁹ Protect Reporters from Exploitative State Spying Act (PRESS Act): *CRS Summary*, S.2074—118th Cong. (2023), LIBR. OF CONG., <https://www.congress.gov/bill/118th-congress/senate-bill/2074#> [<https://perma.cc/27CB-BEB5>].

³⁵⁰ ACLU, *Federal Judge Dismisses Elon Musk’s X Lawsuit Against Nonprofit Researchers* (Mar. 25, 2025), <https://www.aclu.org/press-releases/federal-judge-dismisses-elon-musks-x-lawsuit-against-nonprofit-researchers> [<https://perma.cc/W869-L6AS>].

³⁵¹ Rebecca Buckwalter-Poza, *Elon Musk’s Supreme Court Endgame in Defamation Lawsuit*, SLATE (Mar. 25, 2024), <https://slate.com/news-and-politics/2024/03/elon-musk-media-matters-supreme-court.html> [<https://perma.cc/65S8-8CEV>].

³⁵² Alexander Panetta *‘We Have to Straighten Out the Press’: Trump’s Plan to Sue Media Critics into Submission*, CBC NEWS (Dec. 20, 2024), <https://www.cbc.ca/news/world/trump-suing-media-analysis-1.7415493> [<https://perma.cc/29C9-326Z>]; see Michael M. Grynbaum & Alan Feuer, *ABC to Pay \$15 Million to Settle a Defamation Suit Brought by Trump*, N.Y. TIMES (Dec. 14, 2024), <https://www.nytimes.com/2024/12/14/business/media/trump-abc-settlement.html> [<https://perma.cc/6FX6-2Y3H>] (discussing defamation suit brought by President Trump); Jack Queen & Helen Coster, *Trump’s Lawyers Bring Broad Approach to Court Battles with Media*, REUTERS (Dec. 20, 2024),

Additionally, because these lawsuits are costly and time-consuming, all states should pass anti-Strategic Lawsuit Against Public Participation (SLAPP) legislation to protect against frivolous suits designed merely to drench the media in costs. As of early 2026, thirty-eight states have anti-SLAPP laws.³⁵³

E. Rethinking Privacy in Public and Publicly Available Information

A major problem with U.S. privacy law is its embrace of a faulty conception of privacy that I term the “secrecy paradigm”—a view that anything exposed to the public, or data available to the public, or even information shared with others lacks any privacy interest because it is not totally secret.³⁵⁴ This flawed understanding of privacy creates two common and severe limitations of privacy law—a failure to protect privacy in public or publicly-available data.

The secrecy paradigm fails to appreciate the profound importance of obscurity. As Woodrow Hartzog and Frederic Stutzman astutely note, obscurity is an essential aspect of privacy.³⁵⁵ Most people do not live like hermits; they engage in their life’s activities in places where other people congregate. People expect that their activities are private because they are obscure—others won’t be paying attention or watching or listening. Modern surveillance technologies, however, are increasingly eroding this sense of obscurity. Conversations can be easily recorded, and movements meticulously tracked. As individuals use digital technologies, they leave behind a trail of personal data that previously was forgotten or never collected.

Although some countries have explicitly embraced becoming surveillance societies, such as the United Kingdom, which has decorated its cities and towns with 7.5 million CCTV cameras,³⁵⁶ the U.S. has more quietly assembled an enormous surveillance camera system of its own.³⁵⁷ The average U.S. city has about 1 surveillance camera for every 100 people.³⁵⁸ Atlanta is “the second most surveilled city in the world, beaten only by cities in China.”³⁵⁹ Via the

<https://www.reuters.com/world/us/trumps-lawyers-bring-broad-approach-court-battles-with-media-2024-12-20/> [<https://perma.cc/2V2N-XDW2>] (discussing President Trump’s suits against the media).

³⁵³ *Anti-SLAPP Legal Guide*, REPS. COMM. FOR FREEDOM OF THE PRESS, <https://www.rcfp.org/anti-slapp-legal-guide/> [<https://perma.cc/8EPC-FVNU>].

³⁵⁴ DANIEL J. SOLOVE, UNDERSTANDING PRIVACY 14 (2008).

³⁵⁵ See generally Woodrow Hartzog & Frederic Stutzman, *The Case for Online Obscurity*, 101 CALIF. L. REV. 1 (2013) (discussing the need for obscurity for privacy in the internet age).

³⁵⁶ CLEARWAY, *How Many CCTV Cameras in the UK? CCTV Usage in the UK*, <https://www.clearway.co.uk/news/cctv-usage-in-the-uk/> [<https://perma.cc/2ZPJ-ESGN>] (“The British Security Industry Authority (BSIA) reported that there are roughly 7.5 million cameras in the UK which is around one camera, for every eleven people.”).

³⁵⁷ Paul Bischoff, *CCTV Surveillance in the Most Populated Cities in the United States*, COMPARITECH (Jan. 8, 2024), <https://www.comparitech.com/blog/vpn-privacy/us-surveillance-camera-statistics/> [<https://perma.cc/BPE6-2BMX>].

³⁵⁸ *Id.*

³⁵⁹ *Id.*

“Connect Atlanta initiative,” the police can review the recorded footage of more than 19,000 private-sector surveillance cameras upon request and can have direct access to the video feed of more than 17,000 cameras.³⁶⁰

The “US has almost the same ratio of cameras to citizens installed” as in China.³⁶¹ But whereas in China the cameras are focused on public spaces, Anu Bradford notes that U.S. cameras “are commonly deployed in private sector commercial spaces such as hotels, restaurants, and offices.”³⁶² The U.S. system of cameras is essentially a public-private partnership, where the private-sector is conducting the surveillance and sharing the spoils with law enforcement. Although the per se existence of so many surveillance cameras is problematic, the more troubling problem is that there is virtually no regulation on the use of these cameras. This stems from the faulty notions of the secrecy paradigm. The result is that there are no controls on how much data can be gathered, how long it can be kept, how it can be used, or when the data can be turned over to the government. There is no oversight, accountability, or limitation.

Beyond cameras, other technologies gather data and track individuals wherever they go. As Kate Crawford notes, companies are installing sensors to detect wi-fi signals from smart phones to track people.³⁶³ To the data broker industry—and often to many other companies—“even the act of walking down the street is a legitimate data set to be captured, catalogued and exploited.”³⁶⁴ The general view of surveillance and data companies is that anything in public is free. An oft-made analogy is that data is the “new oil,”³⁶⁵ but any data that is collected in public or publicly available is more akin to air. Oil cannot readily be extracted without constraints and legal controls, whereas air is essentially free for the taking.

AI-powered facial recognition technology has become a widespread application, challenging the anonymity people once enjoyed in their daily lives. Although individuals may often blend into a crowd, facial recognition can now identify them with ease and link them to detailed personal profiles. With surveillance cameras proliferating, individuals can be tracked almost anywhere

³⁶⁰ *Id.*

³⁶¹ BRADFORD, *supra* note 9, at 101.

³⁶² *Id.*

³⁶³ Kate Crawford, *When Big Data Marketing Becomes Stalking*, SCI. AM. (Jan. 28, 2014), <https://www.scientificamerican.com/article/when-big-data-marketing-becomes-stalking/> [<https://perma.cc/3TVK-L2M6>].

³⁶⁴ *Id.*

³⁶⁵ Kiran Bhageshpur, *Data Is the New Oil—And That’s A Good Thing*, FORBES (Nov. 15, 2019), <https://www.forbes.com/councils/forbestechcouncil/2019/11/15/data-is-the-new-oil-and-thats-a-good-thing/> [<https://perma.cc/T6JK-6GL3>] (discussing the value of data); *The World’s Most Valuable Resource Is no Longer Oil, but Data*, THE ECONOMIST (May 6, 2017), <https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data> [<https://perma.cc/BB6S-LRCZ>] (explaining how data has overtaken oil as the most valuable resource).

they go. These systems are typically trained using billions of photos scraped from the internet without consent.³⁶⁶

The general failure of privacy law to recognize privacy in public allows for anyone to install surveillance cameras without any oversight about what may be done with the data or how long it may be retained. There are hardly any rules for government access. The surveillance and the data it generates are mostly in a lawless zone. There should be a strong regulatory framework to provide orderly rules and controls for surveillance in public, whether done by the government, companies, or individuals.

Beyond insufficient protection of privacy in public places, many privacy laws (especially ones in the U.S.) exempt publicly available information.³⁶⁷ Even the California Delete Act, which seeks to reign in data brokers, makes an exception for publicly available information.³⁶⁸ This exception creates a gaping loophole in privacy laws that can be greatly exploited by authoritarian governments.

Companies are scraping vast quantities of personal data from the internet.³⁶⁹ Scraping is a way that many data brokers gather data.³⁷⁰ Scrapers argue that public information is fair game, and many privacy laws permit scraping by excluding publicly available data from their protections.³⁷¹ The principle of obscurity, however, emphasizes that just because data is publicly accessible does not mean privacy is forfeited. Although the information may not be secret, its obscurity imposes significant limits on accessibility. Collecting personal data and making it easily discoverable fundamentally alters the level of privacy associated with that information.³⁷²

Rethinking the notion of publicly available information would close a gaping hole in privacy protection; it would prevent companies and the government from vacuuming up vast quantities of personal data; it would protect personal data online with important privacy safeguards and limitations.

³⁶⁶ See generally HILL, *supra* note 134 (discussing how companies gather data for facial recognition).

³⁶⁷ Solove & Hartzog, *supra* note 95, at 1558–66 (discussing publicly available information); Justin Sherman, *People Search Data Brokers, Stalking, and 'Publicly Available Information' Carve-Outs*, LAWFARE (Oct. 30, 2023), <https://www.lawfaremedia.org/article/people-search-data-brokers-stalking-and-publicly-available-information-carve-outs> [<https://perma.cc/89H6-FMY7>] (discussing private data collection).

³⁶⁸ CAL. CIV. CODE § 1798.99.140(o)(2) (West 2025).

³⁶⁹ Solove & Hartzog, *supra* note 95, at 1558–66.

³⁷⁰ Barbara Booth, *What Internet Data Brokers Have on You—and How You Can Start to Get It Back*, CNET (Oct. 11, 2024), <https://www.cnn.com/2024/10/11/internet-data-brokers-online-privacy-personal-information.html> [<https://perma.cc/TQ5N-NJY3>].

³⁷¹ Solove & Hartzog, *supra* note 95, at 1563.

³⁷² See generally SOLOVE, UNDERSTANDING PRIVACY, *supra* note 354 (explaining that how easy information is to access affects its privacy level).

F. Regulation of Surveillance Technologies

States should enact laws to regulate the development and sale of surveillance technologies. First, states can require privacy safeguards to be built into such technologies, such as end-to-end encryption. Perhaps surveillance cameras can have built-in blurring of faces that can only be de-blurred under certain circumstances. Aggregations of de-identified data can be protected with differential privacy—adding in noise to prevent learning “the underlying confidential data.”³⁷³

The Federal Trade Commission (FTC) has encouraged companies to use privacy enhancing technologies (PETs), which it defines as “a broad set of tools and methods aimed at providing ways to build products and functionality while protecting the privacy of users’ data.”³⁷⁴ But PETs must be more than a mere suggestion.

Regulating design is essential to protecting privacy.³⁷⁵ Technology need not be used only in privacy-invasive ways. Bennett Capers points out that surveillance technologies can be used to create better transparency, accountability, and oversight of policing.³⁷⁶ Thus, instead of banning technologies, they should be allowed if built with appropriate designs, just like cars must be built with seatbelts and airbags. Ideally, surveillance technologies should have built-in curbs on problematic uses. Of course, not all problematic uses can be curtailed by design, but at least the technologies should have built-in mechanisms of transparency and logging so that government officials can be held accountable.

Laws regulating design need not mandate specific designs. Instead, the laws can set certain goals and then leave it to industry to develop solutions, relying on reasonable industry standards. If large states were to pass laws to better regulate design, there would be a strong market incentive for companies to design technologies with greater safeguards even if not all states were to have such laws.

Second, states can pass laws that require accountability, oversight, and limitation for their own government’s use of surveillance cameras and facial recognition systems. These laws can require that surveillance technologies used by government entities in the state be designed to facilitate the ability to have greater accountability, oversight, and limitation. Audit trails can be built in; so can mechanisms of oversight. The technologies can be built in ways that

³⁷³ SIMSON L. GARFINKEL, *DIFFERENTIAL PRIVACY* 2 (2025).

³⁷⁴ Simon Fondrie-Teitler, *Keeping Your Privacy Enhancing Technology (PET) Promises*, FTC BLOG (Feb. 1, 2024), <https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2024/02/keeping-your-privacy-enhancing-technology-pet-promises> [<https://perma.cc/9JG4-NHHM>].

³⁷⁵ See generally HARTZOG, *supra* note 162 (arguing that the way technology is designed influences the privacy level of uses).

³⁷⁶ I. Bennett Capers, *Policing, Technology, and Doctrinal Assists*, 69 FLA. L. REV. 723, 724–26 (2017).

make them harder to abuse without being detected. If large states were to require these elements to be designed into the technologies, it might affect the entire market, as many companies might design the technologies in a more privacy-friendly way because these states have a large market share. States can establish themselves as leaders based on their own market power, creating better incentives for companies to design with privacy in mind.

G. How the Law Can Be Reformed

How can all these changes happen? There are many different ways, and to be most effective, they involve many different policymaking bodies in the system. Having recently fought a revolution, the Framers of the U.S. Constitution were quite concerned about authoritarian power. Their answer was separation of powers. Government power in the U.S. is spread between three branches—the Executive, Legislative, and Judiciary.³⁷⁷ In addition, government power in the U.S. is fractured between federal and state governments. Although not every branch or every state will step up to resist authoritarian power, as some might be under its thrall, hopefully some judges and states will attempt some of the measures proposed above.

1. Legislation

The U.S. Congress could certainly enact federal statutes—the strongest solution for many of my proposals, but this is probably unlikely at this moment. But state legislatures can enact statutes. A silver lining to the failure of the U.S. Congress to pass a comprehensive federal privacy law is that there is nothing to preempt states from passing statutes. The federal bills for a comprehensive federal privacy law proposed in the past few years would have preempted a significant amount of state legislation on privacy.³⁷⁸ Although most of the state laws were weaker than the proposed federal laws, preemption could have shut the door on states enacting stronger protections. In the U.S., it is a virtue that power is fragmented and that states are able to pass privacy laws. These laws might create some headaches for companies, but they also can help serve as an impediment to federal authoritarianism. Preemption works well as a floor to protection, but not as a ceiling. It is valuable to preserve state legislative power especially in a time when the federal government and some state governments might be moving in an authoritarian direction.

For state statutes, there are several key things that legislatures should do. First, the statutes should not contain any exemptions for government access to

³⁷⁷ See generally THE FEDERALIST No. 51 (James Madison) (Clinton Rossiter ed., 1961).

³⁷⁸ Daniel J. Solove, *A Faustian Bargain: Is Preemption Too High a Price for a Federal Privacy Law?*, TEACHPRIVACY (Feb. 1, 2022), <https://teachprivacy.com/a-faustian-bargain-is-preemption-too-high-a-price-for-a-federal-privacy-law/> [<https://perma.cc/QR3N-2MVD>].

personal data. Instead, they should address the issue and specify warrants or other sufficient protections against broad government access, dragnets, or the enforcement of laws that the state might deem to infringe upon fundamental freedoms.

Second, statutes should avoid exceptions for federal laws such as HIPAA, FERPA, and the Gramm-Leach-Bliley Act. Many of these federal laws do not preempt stricter state laws.

Third, the statutes should avoid small business exceptions for most provisions. Most state laws exempt a large number of businesses that fall below a certain size.³⁷⁹ But even small businesses can affect tens of thousands (sometimes even hundreds of thousands) of people. The laws strongly favor making things easier for small companies over protecting consumers. Why should people be unprotected just because they are a customer of a small business? Such businesses must still follow other safety and consumer protection laws, but privacy unfortunately is not considered important enough by policymakers to warrant equivalent treatment. In contrast, the EU's GDPR, does not exempt small businesses; instead, it exempts only personal or familial data collectors as well as journalistic, academic, literary, or artistic uses of data.³⁸⁰ U.S. state privacy laws should look to the GDPR's much better exemptions. Just because a business is small doesn't mean it can't cause harm to many people.

Fourth, the statutes should not exempt non-commercial organizations such as non-profits or state governmental entities. Authoritarian governments can obtain personal data from these sources.

Fifth, the laws should include private rights of action, which are one of the most effective enforcement mechanisms.³⁸¹ Far too often, government enforcement bodies lack the resources and political capital to enforce as widely, thoroughly, and consistently as they should. Private rights of action can greatly augment government enforcement with private party enforcement.

2. Judicial Actions

Courts can play an important role. Courts can apply common law torts such as breach of confidentiality and negligence to a wider range of cases. Courts can recognize new privileges. Courts can also broaden fiduciary law to treat entities that collect and use personal data as information fiduciaries.

³⁷⁹ See generally FUTURE OF PRIVACY FORUM, REPORT: ANATOMY OF STATE COMPREHENSIVE PRIVACY LAW (2024) (showing that most states have an exemption depending on business size).

³⁸⁰ GDPR, *supra* note 306, at 33–35, 83–84.

³⁸¹ See generally Lauren Henry Scholz, *Private Rights of Action in Privacy Law*, 63 WM. & MARY L. REV. 1639 (2022) (arguing that private rights of action have a role in enforcing privacy law).

Across all dimensions of privacy law, courts can better recognize privacy harms.³⁸² Many cases falter in the courts because judges fail to take privacy harms seriously. This undermines privacy statutes and encourages companies to disregard legal obligations, ignore data minimization, break their promises, engage in unexpected data collection and use, and otherwise protect privacy poorly. If courts trivialize privacy harms, it is difficult to expect companies to respect privacy, especially when the incentives are often to collect more data and use it more widely.

Additionally, the risk of government access to personal data should be considered a harm. Of course, there might be societal benefits to allowing the government to access personal data for particular crimes such as terrorism that might outweigh privacy, but this is a balancing that cannot occur if privacy harms are not even recognized. When harms aren't recognized, privacy is not balanced against countervailing interests. This balancing is important and should not be sidestepped by dismissing the privacy harm before the balancing takes place.

3. State Constitutional Reforms

States could enact a right to privacy in their constitutions akin to the right to privacy in California's constitution, which declares: "All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy."³⁸³ The California right to privacy applies not just to government action but also to the private sector.³⁸⁴

If interpreted and applied aggressively, the California constitutional right to privacy could mandate data minimization. As the California Supreme Court declared, "[T]he overbroad collection and retention of unnecessary personal information by government and business interests" was one of the "principal 'mischiefs' at which the [Privacy Initiative] [was] directed."³⁸⁵

Nicole Ozer contends that the California Supreme Court has undermined the constitutional right to privacy by interpreting it weakly when applied to private parties, forcing plaintiffs to prove a "serious invasion of privacy" and allowing the right to be outweighed rather easily in a balance against "countervailing interests."³⁸⁶ The California Supreme Court "manufactured a legal distinction

³⁸² See generally Danielle Keats Citron & Daniel J. Solove, *Privacy Harms*, 102 B.U. L. REV. 793 (2022) (explaining how courts should recognize more harms arising out of breaches of privacy).

³⁸³ CAL. CONST. art. I, § 1.

³⁸⁴ See generally *Hill v. Nat'l Collegiate Athletic Ass'n*, 865 P.2d 633 (Cal. 1994) (holding that claims under California privacy law apply to private actors).

³⁸⁵ *White v. Davis*, 533 P.2d 222, 234 (Cal. 1975) (en banc).

³⁸⁶ Nicole A. Ozer, *Golden State Sword: The History and Future of California's Constitutional Right to Privacy to Defend and Promote Rights, Justice, and Democracy in the Modern Digital Age*, 39 BERKELEY TECH. L.J. 963, 1007–08 (2024).

between information and autonomy privacy claims” and held that a compelling interest was required to outweigh autonomy privacy but information privacy would be subject to general balancing.³⁸⁷

Ozer argues that the California Supreme Court should revisit its interpretation of the right to privacy and reverse the faulty assumptions that it previously established, such as the notion that private parties are less of a danger than government or that there is a meaningful distinction between information and autonomy privacy claims.³⁸⁸

Other states can enact a similar constitutional protection of privacy to California’s, and hopefully avoid the unfortunate interpretation of the California Supreme Court. Even if a state does not enact an explicit right to privacy in its constitution, state courts can interpret their constitutions to recognize a constitutional right to information privacy, as is recognized under the U.S. Constitution. But unlike the California constitutional right to privacy, the constitutional right to information privacy only applies to the government. For many states, it would likely take an amendment to their constitutions to extend the right to private parties.

IV. OTHER IMPORTANT PROTECTIONS

Several additional privacy protections are needed to limit authoritarian power. These measures do not involve direct regulation of surveillance capitalism, but they have significant effects on privacy. Section A of this Part discusses the interrelationship between decisional privacy and information privacy.³⁸⁹ Section B argues for the need for privacy restrictions on discovery in civil litigation.³⁹⁰ Finally, Section C contends that privacy law must be reformed to better protect personal safety.³⁹¹

A. Protection of Decisional Privacy

It is impossible to fully protect informational privacy without protecting decisional privacy. Decisional privacy involves “the interest in independence in making certain kinds of important decisions.”³⁹² Decisional privacy is at the heart of the U.S. Supreme Court’s line of substantive due process right to privacy cases. These cases include the protection of the use of contraceptives,

³⁸⁷ *Id.* at 1008.

³⁸⁸ *Id.* at 1042.

³⁸⁹ See *infra* notes 392–395.

³⁹⁰ See *infra* notes 396–398.

³⁹¹ See *infra* notes 399–402.

³⁹² *Whalen v. Roe*, 429 U.S. 589, 599–600 (1977).

marriage, child-rearing, and sex, among other things.³⁹³ This line of cases included the right to abortion until it was eliminated in 2022, in the Supreme Court's decision in *Dobbs v. Jackson Women's Health Organization*. These types of matters are what Danielle Citron calls "intimate privacy."³⁹⁴

Decisional privacy and information privacy are interrelated.³⁹⁵ Without robust protection of informational privacy, decisional privacy is imperiled, as personal data can be used to oppress, control, manipulate, chill, and thwart decision-making. Failure to protect decisional privacy leads to grave threats to information privacy as government officials seek data to prosecute personal health and life decisions. If the underlying private decisions are criminalized, the government can use its vast law enforcement powers to gather data to carry out this enforcement. The best way to keep law enforcement officials from prying into one's health or sex life is not to infringe upon matters such as reproductive freedom.

Although it is unlikely that the U.S. Supreme Court will reverse *Dobbs* in the near future, state courts can hold that their constitutions guarantee a right to reproductive freedom. State courts can read their constitutions even more expansively, protecting greater rights over bodily autonomy more generally. Recognition of these rights in state constitutional law will buttress information privacy.

B. Civil Litigation and Discovery of Private Information

Civil discovery is another outlet that can potentially be abused in authoritarian times. Government officials—or allied individuals—could bring lawsuits and ferret out personal data through the civil litigation system. Allyson Haynes Stuart notes that there are scant limitations on civil discovery of private information housed in cell phones, wearable technology, geolocation applications or social media.³⁹⁶ States that allow civil lawsuits for people who have abortions could unleash civil discovery powers to obtain data from companies and organizations.

³⁹³ See generally *Griswold v. Connecticut*, 381 U.S. 479 (1965) (holding that there is a constitutional privacy right that includes the right to contraception); *Loving v. Virginia*, 388 U.S. 1 (1967) (holding that a ban on interracial marriage is unconstitutional); *Pierce v. Soc'y of the Sisters of the Holy Names of Jesus & Mary*, 268 U.S. 510 (1925) (holding that requiring all children to attend public school is unconstitutional); *Lawrence v. Texas*, 539 U.S. 558 (2003) (striking down a Texas law criminalizing same-sex intimacy).

³⁹⁴ See generally CITRON, *FIGHT FOR PRIVACY*, *supra* note 18 (explaining what types of things are intimate privacy).

³⁹⁵ See Neil M. Richards, *The Information Privacy Law Project*, 94 GEO. L.J. 1087, 1107–12 (2006) (noting that the Court's analysis in *Griswold* involved "freedom from intrusion and scrutiny").

³⁹⁶ See generally Stuart, *Privacy Paradox*, *supra* note 40 (discussing the implications of civil procedure on privacy law); Stuart, *Privacy in Discovery After Dobbs*, *supra* note 40 (discussing privacy in civil law).

As Allyson Haynes Stuart notes, there are few protections for privacy in civil discovery.³⁹⁷ Data is discoverable if relevant to a claim; courts have significant discretion to balance the proportionality of data demanded to the need for a claim. Stuart argues that civil discovery should do a better job at incorporating privacy interests in its equation.³⁹⁸ Stronger protections against civil discovery are needed rather than relying on protective orders and judicial discretion. As some states are weaponizing the civil justice system to allow individuals to sue people seeking or assisting abortions, then the best protection still remains data minimization by the businesses that collect and maintain personal data.

C. Protection of Safety

As discussed earlier, online mobs are increasingly attacking people who speak out and criticize the misinformation, agendas, and interests of authoritarian thought leaders. Threats are more chilling and dangerous because personal data such as people's home address and family information are readily available.

Privacy law has notable gaps in protecting people from being doxed and threatened online. This is due to privacy law's focus on the nature of data rather than on how it might be used. Privacy laws recognize strong protections for sensitive data, but there are many other types of data that are involved with online threats that are not sensitive. For example, home addresses are not considered to be sensitive data—and often not even considered to be private.³⁹⁹ But finding people's home address is often a key part of online threats of violence to a person and their family.

Policymakers have recognized the importance of protecting home addresses and other personal data that might cause safety issues when it comes to themselves and their families. For example, in New Jersey, Daniel's Law protects the privacy and safety of public officials by allowing them to request that their personal data be removed from public government websites.⁴⁰⁰ A federal law allows federal judges to remove their personal data from online databases and stop data brokers from reselling it.⁴⁰¹

But there is no law to protect everyone else, despite many individuals who are doxed, harassed, or receive death threats. In a free and democratic so-

³⁹⁷ See generally Allyson Haynes Stuart, *A Right to Privacy for Modern Discovery*, 29 GEO. MASON L. REV. 675, 675 (2022).

³⁹⁸ Stuart, *Privacy in Discovery After Dobbs*, *supra* note 40, at 30–31.

³⁹⁹ SOLOVE, THE DIGITAL PERSON, *supra* note 111, at 128.

⁴⁰⁰ N.J. STAT. ANN. § 47:1B-1 (West 2023).

⁴⁰¹ Daniel Anderl Judicial Security and Privacy Act of 2022, Pub. L. 117-263, 136 Stat. 3458 (2022).

ciety, everyone deserves to feel safe and should not have to worry about being harmed or killed or putting their family in danger for their speech.⁴⁰²

CONCLUSION

As the shadows of authoritarianism loom around us, it is essential to improve the way the law protects privacy. Modern technologies pose a grave danger when mixed with authoritarianism. They make authoritarianism more powerful, efficient, and totalizing in its control. The best defense against a totalitarian regime like Big Brother is not to let it grow into this. We must contain the fire using every possible tool. Judges, state legislators, and others who care about preventing authoritarianism must dramatically improve privacy protection. To understand the urgency, one need only imagine how much more potent and terrifying the authoritarian regimes of the previous century would have been had they existed in today's digital age.

⁴⁰² See generally FRANKS, *supra* note 32 (discussing how speaking without fear is essential to promoting free speech).

