LEGISLATIVELY ERASED: THE FAILURE OF PRIVACY LEGISLATION TO PROTECT PEOPLE CONNECTED TO THE CRIMINAL LEGAL SYSTEM

CHAZ ARNETT[†] & KATE WEISBURD[††]

TABLE OF CONTENTS

INTRODUCTION 64

I. POLICE EXEMPTIONS ARE IDENTICAL AND PREVALENT IN STATE DATA PRIVACY LEGISLATION.....66
A. The Need for a Police Exemption Typology.....66
B. Consumer Protection Laws Offer a Case Study of Police Exemptions 67
C. Exemptions Give Police Broad Power and Render People Second Class Consumers .68

II. POLICE EXEMPTIONS LEAVE PEOPLE CONNECTED TO THE CRIMINAL LEGAL SYSTEM WITH NO PRIVACY PROTECTIONS.....69
A. Laundering the Surveillance State.....69
B. Police Exemption Provisions Undermine the Stated Purpose of State Privacy Laws ..71
C. People Connected to the Criminal Legal System Have Rights, Including Privacy Rights 73
D. Police Exemptions Benefit Private Surveillance Companies.....74

III. THE PATH FORWARD: RECONCEPTUALIZING SAFETY AND PRIVACY 76
A. Ending the Era of Police Exemptions 76
B. Moving Beyond a Rights Framework 76
C. Privacy & Safety Beyond Data and Technology 77

IV. CONCLUSION.....78

[†] Chaz Arnett, Jacob A. France Professor of Law, University of Maryland Francis King Carey School of Law. We would like to thank Prescillia Messa for research assistance and editing, and we are especially grateful for the editing and feedback from the GW JOLT editorial team.

[††] Kate Weisburd, Professor of Law, University of California College of the Law, San Francisco.

INTRODUCTION

When it comes to legislation aimed at protecting people's digital privacy, all eyes are now on the states. State lawmakers must decide if—and how—they will hold the line against expanded federal surveillance and the dismantling of federal oversight agencies, such as the Consumer Financial Protection Bureau and the Privacy and Civil Liberties Oversight Board.[1] This is especially true in the context of consumer data. In the past few years, dozens of states have adopted new consumer data protection statutes, and more are considering adopting such laws.[2] Organizations such as the Electronic Privacy Information Center ("EPIC"), the Center for Democracy and Technology, and the U.S. Public Interest Research Group created model consumer protection laws and are supporting state lawmakers in getting these bills passed, as well as advocating for states to do more.[3] Yet one group is consistently left out of the privacy-legislation discourse: people suspected or convicted of committing crimes.

The vast majority of new consumer protection laws, as well as the model law created by EPIC, contain explicit language allowing for cooperation with law enforcement.[4] In particular, the following language appears in virtually all the new laws: "Nothing in this chapter shall be construed to restrict a controller's or processor's ability to . . . [c]ooperate with law enforcement agencies concerning conduct or activity that the business, service provider, or third party reasonably and in good faith believes may violate federal, state, or local law."[5]

This carveout provision for police, what this Article refers to as "police exemptions," means that people who have the most contact with police and criminal courts are the least likely to enjoy the benefits of the new consumer protection laws.[6] These police exemptions render people

---

[1] *See, e.g.*, Charles Savage, *Trump Seeks to Paralyze Independent Privacy and Civil Liberties Watchdog*, N.Y. TIMES (Jan. 22, 2025), https://www.nytimes.com/2025/01/22/us/trump-privacy-civil-liberties-oversight-board.html [https://perma.cc/9GS8-X5J4]; Josh Gerstein & Kyle Cheney, *DOGE's access to federal data is 'an absolute nightmare,' legal experts warn*, POLITICO (Feb. 3, 2025), https://www.politico.com/news/2025/02/03/doge-treasury-usaid-donald-trump-011538 [https://perma.cc/U7FZ-STPA]; Stacy Cowley, *Confusion Reigns as 'a Wrecking Ball' Hits the Consumer Bureau*, N.Y. TIMES (Feb. 10, 2025), https://www.nytimes.com/2025/02/10/business/cfpb-shutdown-confusion.html [https://perma.cc/H47V-SADG].

[2] *See* Philip Yannella & Tim Dickens, *New state privacy laws creating complicated patchwork of privacy obligations*, REUTERS (June 7, 2024), https://www.reuters.com/legal/legalindustry/new-state-privacy-laws-creating-complicated-patchwork-privacy-obligations-2024-06-07/ [https://perma.cc/M7B3-C5MS]; Jospeh Lazzarotti, *Privacy Blizzard Expected in January as Five State Laws Take Effect*, MONDAQ (Dec. 20, 2024), https://www.mondaq.com/unitedstates/privacy-protection/1562840/privacy-blizzard-expected-in-january-as-five-state-laws-take-effect [https:// perma.cc/B4CF-CS5Q].

[3] *See* ELEC. PRIV. INFO. CTR. & CONSUMER REPS., THE STATE OF DATA PRIVACY ACT: A PROPOSED COMPROMISE BY CONSUMER PRIVACY ADVOCATES (Sep. 2024), https://advocacy.consumerreports.org/wp-content/uploads/2024/09/EPIC_CR-CT-CLEAN-FINAL-1.pdf [https://perma.cc/L2Q7-K6FD]; ELEC. PRIV. INFO. CTR. & U.S. PIRG EDUC. FUND, THE STATE OF PRIVACY: THE STATE OF PRIVACY 2025: HOW STATE "PRIVACY" LAWS FAIL TO PROTECT PRIVACY AND WHAT THEY CAN DO BETTER (Jan. 2025), https://epic.org/wp-content/uploads/2025/04/EPIC-PIRG-State-of-Privacy-2025.pdf [https://perma.cc/T3P3-7T4D]; Caitriona Fitzgerald, *A Proposed Compromise: the State Data Privacy and Protection Act*, ELEC. PRIV. INFO. CTR. (Feb. 22, 2023), https://epic.org/a-proposed-compromise-the-state-data-privacy-and-protection-act [https://perma.cc/K3BS-6DDZ].

[4] *See id.*

[5] The following states adopted this language in their consumer protection bills: Cal., Colo., Conn., Ind., Iowa, Ky., Md., Minn., Mont., Neb., N.J., Or., R.I., Tenn., and Utah. *See infra* Part I.

[6] We are not the first to explore the question of exceptions for police in privacy or transparency-related legislation, though our piece is the first we know of that explores the particular question of carveouts for police in state consumer protection laws. *See, e.g.,* Christina Koningisor, *Police Secrecy Exceptionalism*, 123 COLUM. L. REV. 615, 645 (2023); Rebecca Wexler, *Life, Liberty, and Data Privacy: The Global Cloud, the Criminally Accused, and Executive Versus Judicial Compulsory Process Powers*, 101 TEX. L. REV. 1341 (2023); Vincent Southerland, *"The Master's Tools and a Mission: Using Community Control and Oversight Laws to Resist and Abolish Police*

suspected, charged, or convicted of crimes, invisible in terms of privacy. By offering no protection against the collection, sharing, and use of sensitive private data, these laws further solidify the ways in which privacy protections are not shared equally by all.[7]

Police exemptions directly undermine the stated purposes of these new consumer data privacy laws. The laws were meant to curb data discrimination and protect against the harms of private companies sharing sensitive data. Yet by allowing for cooperation with law enforcement, this is exactly what can—and does—happen. Indeed, just a few years ago, the Judiciary Committee of the U.S. House of Representatives published a report raising concerns about how federal law enforcement agencies obtain otherwise private consumer data from financial institutions.[8] But this type of coordination is expressly permitted in state privacy laws that have carveouts for police.

By focusing on recently passed consumer data privacy laws, this Article charts the extent to which people involved in the criminal legal system are left behind when it comes to digital privacy. Building on the work of scholars who have revealed the ways privacy laws systematically fail to protect people of color and poor people,[9] this Article adds another dimension to the literature by scrutinizing law enforcement carveouts in state legislation. As we argue, these carveouts directly facilitate the racial, gender, disability, citizenship-status, and economic inequities endemic not just in criminal law, but privacy law as well.

This Article proceeds in three parts. In Part I, we make the case for a typology of police exemptions in a broad range of privacy legislation and then use recently passed (or pending) state consumer protection laws as a case study of police exemptions and what these carveouts mean for expanded police powers. In Part II, we reveal the various ways that police exemption provisions create second-class consumers—large groups of people who simply do not get any of the benefits of consumer data laws. We argue that these police exemptions further normalize surveillance of groups already marginalized and discriminated against. Finally, in Part III, we suggest a path forward, including eliminating law enforcement carveouts or, at the very least, including a warrant requirement and reconceptualizing the meaning of safety and harm.

To be sure, privacy policy is at an inflection point. As the new federal administration rolls back the many significant and recent gains in privacy protections, it is tempting for privacy advocates to focus on policy reform that is most politically palpable, a position that rarely accounts

---

Surveillance Technologies," 70 UCLA L. REV. 2 (2023); Jonathan Manes, *Secrecy & Evasion in Police Surveillance Technology*, 34 BERKELEY TECH. L.J. 503 (2019); 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 (2013).

[7] *See* Khiara Bridge, THE POVERTY OF PRIVACY RIGHTS (2017); Anita L. Allen, *Dismantling the "Black Opticon:" Privacy, Race Equity, and Online Data-Protection Reform*, 131 YALE L.J. F. 907 (2022); Chaz Arnett, *Race, Surveillance, Resistance*, 81 OHIO STATE L.J. 1103 (2020); Scott Skinner-Thompson, *Privacy's Double Standards*, 93 WASH. L. REV. 2051 (2018); Michele Gilman & Rebecca Green, *The Surveillance Gap: The Harms of Extreme Privacy and Data Marginalization*, 42 N.Y.U. REV. L. & SOC. CHANGE 253 (2018); Prianka Nair, *Surveilling Disability, Harming Integration*, 124 COLUM. L. REV. 197 (2024); Khiara Bridges, *Privacy Rights and Public Families*, 34 HARV. J. L. & GENDER 113, 122–23 (2011).

[8] STAFF OF COMM. ON THE JUDICIARY & SELECT SUBCOMM. ON THE WEAPONIZATION OF THE FED. GOV'T, 118TH CONG., FINANCIAL SURVEILLANCE IN THE UNITED STATES: HOW FEDERAL LAW ENFORCEMENT COMMANDEERED FINANCIAL INSTITUTIONS TO SPY ON AMERICANS (2024).

[9] *See supra* note 7.

for people in the criminal legal system—people who are routinely "locked out of the democratic process."[10] To move forward without regard for people suspected or convicted of crimes jeopardizes the precise purpose of these laws, which is to limit the harm of data collection and push back against data discrimination.

I. POLICE EXEMPTIONS ARE IDENTICAL AND PREVALENT IN STATE DATA PRIVACY LEGISLATION

Numerous categories of state laws aimed at protecting individual privacy include specific provisions related to law enforcement. These statutes range in what type of privacy they protect, and what precisely police can or cannot do under the statute. Apart from Professor Erin Murphy's 2013 article tracing police exceptions in federal privacy legislation, the study of privacy legislation and policing has been notably siloed.[11] As a result, a deeper understanding of police exemptions is missing from privacy and policing discourse.

A. The Need for a Police Exemption Typology

While a detailed typology of police exemptions in state privacy laws is beyond the scope of this piece, the need for such a study is critical. Without such a study, it is impossible to appreciate the systematic ways that large groups of people are denied otherwise applicable privacy protections.

A typology of police exemptions must account for two different but intersecting axes. On one axis are the categories of state legislation that are aimed at protecting privacy. Included here are laws aimed at protecting certain groups or types of information, including data related to education, consumers, children, social media, employees, healthcare, and biometrics, to name just a few. Another category of laws directly regulates police use of otherwise private data. The most obvious examples being the California Electronic Communications Privacy Act (CalECPA) and the Illinois Freedom from Location Surveillance Act.[12] These acts limit how police may access and use data, but even these laws contain their own police exemptions. For example, the protections in these laws do not apply to data collected from people on probation, parole, or other forms of court supervision.[13]

On the other axis is the degree to which these laws regulate the police. With the exception of laws specifically aimed at police (such as CalECPA), state laws related to privacy and transparency have different types of police carveouts—some more permissive or protective than others. Just as Professor Murphy studied the types of law enforcement carveouts in federal legislation, the same study should be undertaken of state privacy laws. Although this piece does not offer such a study, we focus on consumer data protection bills as an example of police exemptions.

---

[10] Monica C. Bell, *Police Reform and the Dismantling of Legal Estrangement*, 126 YALE L.J. 2054, 2143 (2017).

[11] Murphy, *supra* note 6, at 487.

[12] Ill. Freedom From Location Surveillance Act, 725 ILL. COMP. STAT. 168 (2019); Cal. Elec. Commc'ns Priv. Act, 2015 Cal. Stat. ch. 651 (codified as amended at Cal. Penal Code § 1546.1(c)(1) (Supp. 2020)).

[13] Cal. Elec. Commc'ns Priv. Act, 2015 Cal. Stat. ch. 651 (codified as amended at Cal. Penal Code § 1546.1(c)(10) (Supp. 2020)).

B. Consumer Protection Laws Offer a Case Study of Police Exemptions

In the past few years, many states have either considered or passed new laws aimed at better protecting consumer data.[14] These laws generally limit what data private companies can collect and how they can use, analyze, or sell the data.[15] Rather than relying on a model of notice-and-choice (which requires consumers to opt in or consent to certain data collection processes), these laws directly limit private companies.[16] The laws also prohibit companies from selling or using sensitive data (including precise geolocation, health data, data about minors, and more) for targeted advertising.[17] Finally, the laws reflect a range of rights for consumers, including the right to access personal data, to correct inaccuracies in said data, and to request its deletion.[18]

These bills—both those proposed and passed—almost uniformly contain an exemption for police. In particular, of the 19 states that passed a consumer privacy protection bill in the last six years, all but one (New Hampshire) contained explicit language exempting law enforcement from the law's protections.[19] Of the 19 states, 15 adopted the following language under the "exemption" provision of the law:

> Cooperate with law enforcement agencies concerning conduct or activity that the controller or processor reasonably and in good faith believes may violate federal, state, or local law or regulations.[20]

Three states contained the following language in their "exemptions" section: "Comply with a civil, criminal, or regulatory inquiry, investigation, subpoena, or summons by federal, state, local, or other governmental authorities."[21] The same pattern can be seen in proposed but not yet passed laws. Of the seven states considering passing consumer data protection laws, most contain one of the two exemptions excerpted above.[22] Notably, a data privacy law pending in New York State prohibits companies from disclosing data to police unless pursuant to a warrant or subpoena.[23] New York, however, is the exception, not the norm.

The fact that the language is nearly identical across states—and is also reflected in many pending consumer privacy bills—is not surprising. Many of these laws were identical to model legislation published by the Electronic Privacy Information Center and endorsed by the Center for

---

[14] *See* ELEC. PRIV. INFO. CTR. & CONSUMER REPS., THE STATE DATA PRIVACY ACT: A PROPOSED COMPROMISE BY CONSUMER PRIVACY ADVOCATES (Apr. 2025), https://epic.org/wp-content/uploads/2025/04/State-Data-Privacy-Act-EPIC-CR-April2025.pdf [https://perma.cc/3P28-Z53Z] ("As of September 2024, 19 states have signed state privacy laws.").

[15] *Id.*

[16] *Id at 4*.

[17] *Id.*

[18] *Id.*

[19] For a list of bills, see IAPP US Privacy Law Tracker 2025, INT. ASSOC. OF PRIV. PROS., https://iapp.org/resources/article/us-state-privacy-legislation-tracker [https://perma.cc/R36W-RAWN] (last visited Oct. 15, 2025).

[20] The following states adopted this language (including functional equivalent) in their consumer protection bills: Cal., Colo., Conn., Ind., Iowa, Ky., Md., Minn., Mont., Neb., N. J., Or., R.I., Tenn., and Utah.

[21] Va. Code Ann. § 59.1-582 (West); Del. Code Ann. tit. 6, § 12D-110 (West); Tex. Bus. & Com. Code Ann. § 541.201 (West).

[22] States with pending laws that contain police exemptions: Haw., Ill., Mass., N.Y., Ohio, Okla., Pa., and Wash.

[23] S. 3044, 2025–2026 Leg. Sess. (N.Y. 2025).

Democracy and Technology, the United States Public Interest Research Group, and Public Knowledge.[24] While undoubtedly a victory for consumers generally, these police exemptions result in a large number of people not benefiting from the law's protections, nor having the same new privacy-protecting rights.

C. Exemptions Give Police Broad Power and Render People Second Class Consumers

The police exemptions contained in these new laws mean that people connected with the criminal legal system are removed from the protections of the law and become, in essence, second-class consumers. Far from limiting police access to data, the language of these exemptions is notably permissive. For example, no version requires police to obtain a warrant or for there to even be a showing of reasonable suspicion or probable cause that a crime has or will occur, or that the person in question is in fact a suspect. The approach taken by most states that have passed consumer laws merely requires that the controller or processor turn over data regarding conduct that they "reasonably and in good faith believe[] may violate federal, state, or local law."[25] In Delaware, Texas, and Virginia, the processor must not only comply with a warrant, but also any criminal "inquiry" or "investigation."[26]

By not even requiring a warrant, reasonable suspicion, or probable cause, police may circumvent these new laws with nothing more than a "hunch" that someone may be involved in a crime. These police exemptions, therefore, run directly contrary to clear Supreme Court law that police may not stop, search, or seize someone based on a hunch alone.[27] So long as law enforcement is interested in investigating someone, there is no state consumer law—other than New York's proposed law—stopping private companies from sharing otherwise private data. Under most state privacy laws, police have unencumbered access to geolocation data, health data, financial data, and more.

To be sure, police exemptions in privacy legislation are no anomaly. For example, as Professor Christina Koningisor exposed, laws governing public records and transparency often exempt police from disclosing otherwise publicly accessible material.[28] Indeed, in the context of high profile deadly attacks by police on predominantly Black and Brown people, police often rely on exemptions in public record laws to justify not disclosing police disciplinary records or body worn camera footage.[29] It is therefore all the more imperative to interrogate and scrutinize the various forms of police exemptions in the full range of state privacy laws.[30]

---

[24] ELEC. PRIV. INFO. CTR. & CONSUMER REPS., *supra* note 3.

[25] *See supra* note 20.

[26] *See supra* note 21.

[27] *See* Terry v. Ohio, 392 U.S. 1, 21–22 (1968).

[28] Koningisor, *supra* note 6, at 637–62.

[29] *Id*. at 619, 641; *see also* Rachel Moran, *Police Privacy*, 10 UC IRVINE L. REV. 153, 154 (2019).

[30] *See* Bell, *supra* note 10, at 2144 ("Transparency measures . . . contribute to the overall democratization of policing in a way that could begin to root out legal estrangement.").

II. POLICE EXEMPTIONS LEAVE PEOPLE CONNECTED TO THE CRIMINAL LEGAL SYSTEM WITH NO PRIVACY PROTECTIONS

Police exemptions not only expand police powers while betraying core logics of data privacy legislative movements, they also further a form of police exceptionalism[31] that normalizes the surveillance state. This rendering of police surveillance as banal and unremarkable is troubling because it leaves those who are the usual targets[32] of disparate police profiling, abuse, and overreach on the proverbial sidelines of the growing discourse and advocacy against data vulnerability and exploitation.

Removed from the promise of privacy, those on the economic margins, including Black, Indigenous, and other people of color, assume the very digitized subordinated status state data privacy laws purportedly aim to alleviate. While the constitutional parameters of privacy protections in the era of big data are still somewhat in flux,[33] those subject to police data surveillance are not without meaningful privacy protections and interests.[34] Thus legislative exemptions delegitimate privacy claims recognized as essential in jurisprudence and policy acknowledging the dangers of unfettered police power to surveil. They facilitate a form of tech-washing that disregards historical police misconduct and dismisses its victims at a time in which the lines between the state and private companies are blurring and surveillance capitalism is booming. This section wrestles with these realities and the data privacy precarity police exemptions engender for some of the most marginalized members of society.

A. Laundering the Surveillance State

Perhaps one of the most alarming aspects of police exemptions is that they background significant concerns and critiques of mass police surveillance through their remaking as ordinary necessities. The surveillance state operates through strategies, investments, and ideologies beholden to pervasive monitoring as a means to state governance and regulation, and ultimately, maintenance of the social status quo.[35] The police exemptions, therefore, reflect a continued commitment to inescapable police presence and access, and an implicit nod to an impenetrable surveillance state.[36] Yet, the surveillance state is neither natural, necessary, nor intractable. Scholars and advocates have built a robust critical discourse on the emergence and transformations

---

[31] For a detailed accounting of police and criminal law exceptionalism more generally, see Benjamin Levin, *Criminal Law Exceptionalism*, 108 VA. L. REV. 1381 (2022); Alice Ristroph, *An Intellectual History of Mass Incarceration*, 60 B.C. L. REV. 1949, 1953–55 (2019) (describing various types of "criminal law exceptionalism"); Alice Ristroph, *Exceptionalism Everywhere: A (Legal) Field Guide to Structural Inequality*, 65 ARIZ. L. REV. 921, 952 (2023).

[32] Arnett, *supra* note 7 at 1107–16.

[33] *See, e.g.*, ORIN KERR THE DIGITAL FOURTH AMENDMENT: PRIVACY AND POLICING IN OUR ONLINE WORLD 70 (2025); Maneka Sinha, *The Automated Fourth Amendment*, 73 EMORY L.J. 589 (2024); Daniel Solove, *The Limitations of Privacy Rights*, 98 NOTRE DAME L. REV. 975 (2023).

[34] DAVID GRAY, THE FOURTH AMENDMENT IN AN AGE OF SURVEILLANCE 16 (2017).

[35] Sarah Brayne, *Big Data Surveillance: The Case of Policing*, 82 AM. SOC. REV. 977, 979, 998, 1004 (2017).

[36] While the authors of these bills, along with advocates like EPIC, may argue that such legislation is designed to curb the surveillance state, the broad exemptions for law enforcement ultimately leave that state intact—ensuring that anyone targeted by police remains vulnerable to unchecked monitoring. Barry Friedman, *Lawless Surveillance*, 97 N.Y.U. L. REV. 1143, 1149, 1155, 1160, 1185 (2022).

of the surveillance state. This work notes the rise of the surveillance state, delineates its parameters, examines its constitutional contours, problematizes its historical lineage, charts challenges to its structural dimensions, and questions its internal logics.[37] In recent years these efforts to respond to the surveillance state have had to grapple with the rapidly progressing technological dimensions of monitoring in the age of big data policing, where greater amounts of data can be captured faster, for longer periods, and shared across multiple databases.[38]

Police surveillance has been critiqued in legal scholarship not only on the basis of its questionable constitutional grounding and extensive harm, but also for the role that law plays in making mass digital surveillance—and the corresponding forfeiture of privacy—a social norm.[39] Law has always had impacts that transcend the confines of narrow, doctrinal, theoretical, and ideological debates. Law maintains a reciprocal relationship with society where the law is shaped by, but also influences, social norms. In particular, the development and enactment of legislation that supposedly conveys the "will of people," also carries and conveys blatant or laden normative assumptions. Police exemptions work in this way to normalize police surveillance as above reproach, as police officers are largely assumed to be good-faith actors.[40] This subtle licensing by police exemptions functions to launder the surveillance state through data privacy law.

The norming of law enforcement personnel as disinterested good-faith actors also finds congruence in constitutional criminal procedure jurisprudence. In *United States v. Leon*, for example, the United States Supreme Court articulated the good faith exception to the exclusionary rule for unconstitutionally obtained evidence.[41] In this case, police officers conducted a search pursuant to a warrant and collected probative evidence by surveilling a home.[42] The search warrant was later found to be invalid because it lacked probable cause.[43] The majority dismissed the need to exclude the illegally obtained evidence in large part on the idea that police need only to be deterred under limited circumstances.[44] Those limited circumstances being when there is actual misconduct, which is presented as rarer than the occasional mistakes.[45] Yet a similar rationale was relied upon in *Whren v. United States*, where there was evidence of police acting upon racial biases in stopping a vehicle with Black occupants.[46] The Court ruled that the subjective intentions of

---

[37] *See generally* Neil Richards, *The Dangers of Surveillance*, 126 HARV. L. REV. (2013); Radha D'Souza, ACTIVISTS AND THE SURVEILLANCE STATE: LEARNING FROM REPRESSION, 23–31 (Aziz Choudry 2019); SIMONE BROWN, DARK MATTERS: ON THE SURVEILLANCE OF BLACKNESS (Duke Press 2015); Southerland, *supra* note 6, at 14; Friedman, *supra* note 36, at 1149, 1155, 1160, 1185; Arnett, *supra* note 7 at 1115–18; Andrew Guthrie Ferguson, *Generative Suspicion and the Risks of AI-Assisted Police Reports*, 120 NW. U. L. REV. 301, 314–15 (Oct. 13, 2025).

[38] Arnett, *supra* note 7 at 1115–18; Ferguson, *supra* note 37, at 314–15.

[39] ANDREW FERGUSON, THE RISE OF BIG DATA POLICING: SURVEILLANCE, RACE, AND THE FUTURE OF LAW ENFORCEMENT 131 (2017).

[40] *Id.* And to the extent that they are not, still presumed to be a necessary tradeoff for security.

[41] United States v. Leon, 468 U.S. 897, 922 (1984).

[42] *Id.* at 900–02.

[43] *Id.* at 903.

[44] *Id.* at 919–21.

[45] *Id.* at 923.

[46] Whren v. United States, 517 U.S. 806, 813 (1996).

police officers, even racially motivated ones, "play no role in ordinary, probable-cause Fourth Amendment analysis."[47]

Police exemption provisions in state privacy laws mimic this narrative of police officers as blameless actors—despite the fact that police officers have repeatedly been shown to be inadequate data stewards at best, and distrustful data purveyors at worst.[48]

Lastly, police exemptions act to background the surveillance state by furthering the fiction of a clear dichotomy between the state and Big Tech. While most state data privacy laws are aimed at regulating private technology companies, police carveouts belie a reality in which the surveillance state is deeply entangled with Big Tech.[49] Such obfuscation clouds the depth to which private interests are advanced through the marshalling of the state apparatus and surveillance, and vice versa.

One need not look much further than the current presidential administration. Throughout his campaign and within the first five months of his return to office, President Donald Trump relied upon and placed great power in the hands of Elon Musk, one of the world's most widely known tech moguls.[50] Musk used his position as the head of the Department of Government Efficiency (DOGE) to weaken the state's accountability mechanisms, removing barriers to further profiteering for himself and other Big Tech executives.[51] These efforts included targeted strategies to access sensitive data of private individuals.[52] Yet, police exemptions promote a fabricated dichotomy where state data access poses less concern and is distinct from corporate data extraction because state access is supposedly not driven by private profit interests.[53]

B. Police Exemption Provisions Undermine the Stated Purpose of State Privacy Laws

Much of the legislative history and advocacy efforts regarding consumer protection laws reflect the goal of protecting sensitive data and "avoiding harmful effects stemming from the overcollection of personal data."[54] The model legislation proposed by EPIC—and adapted by many states—also includes provisions aimed at curbing data discrimination based on race and other protected statuses.[55]

---

[47] *Id.*

[48] Arnett, *supra* note 32, at 1105.

[49] *Id.* at 1130.

[50] *Who is Elon Musk, Trump's Pick to Lead Department of Government Efficiency*, THE ECON. TIMES (Mar. 11, 2025), https://economictimes.indiatimes.com/news/international/global-trends/elon-musk-us-department-of-government-efficiency/articleshow/118818585.cms?from=mdr [https://perma.cc/7ZW2-VW6K].

[51] Tony Romm, *The CFPB Took Aim at Big Tech. Then Elon Musk Moved to Dismantle It.*, WASH. POST (Feb. 11, 2025), https://www.washingtonpost.com/business/2025/02/11/elon-musk-doge-cfpb-regulations/ [https://perma.cc/HW7G-LWHP]; Stacy Cowley et. al, *With Attack on Consumer Bureau, Musk Removes Obstacle to His 'X Money' Vision*, N.Y. TIMES (Feb. 12, 2025), https://www.nytimes.com/2025/02/12/business/elon-musk-cfpb-x-money.html [https://perma.cc/G2A8-KSYB].

[52] Rebecca Rainey, *Musk's Data Access Hinges on DOGE Status as Government Agency*, BLOOMBERG LAW (Feb. 14, 2025), https://news.bloomberglaw.com/daily-labor-report/musks-data-access-hinges-on-doge-status-as-government-agency-48 [https://perma.cc/LC65-KXA2].

[53] Christina Koningisor, *Police Security Exceptionalism*, 123 COLUM. L. REV. 615, 615–16 (2023) (noting that law enforcement specific exemptions reinforce the perception that state data access warrants less scrutiny than private data collection).

[54] Catriona Fitzgerald & Kara Williams, *The State Data Privacy Act: A Proposed Model State Privacy Bill*, ELEC. PRIV. INFO. CTR., https://epic.org/the-state-data-privacy-act-a-proposed-model-state-privacy-bill [https://perma.cc/F4BE-9NVY].

[55] In particular, the model legislation includes the following language: "A controller or processor may not collect, process, or transfer

Yet the police exemptions directly undermine these goals. By providing such permissive cooperation with law enforcement, these laws allow private companies to collect, share, and sell sensitive data in ways that directly harm the exact populations of people the laws aimed to protect. The harm falls into three general categories.

First, sharing data with police puts at risk the exact vulnerable populations that progressive lawmakers are concerned about.[56] For example, young people's data is meant to be especially protected, but if a young person has contact with police—or if police simply have a hunch that a young person is involved in a crime—the Consumer Protection Act simply does not apply. Likewise, if police have nothing more than a hunch that a person accessed abortion services, the consumer protection laws do not apply. Non-citizens are also at risk, as mere allegations of criminal conduct can be grounds for detention, deportation, or other adverse consequences.[57] By allowing police to access data based on a mere gut feeling and nothing more could harm all of these groups.

The second category of harm is related: allowing police unencumbered access to consumer data undermines civil rights and furthers data discrimination. In particular, the more law enforcement can access (or buy) data, the greater the risk that police will use such surveillance powers on the groups most historically targeted by police.[58] Indeed, as is now well documented, poor people and people of color are disproportionately investigated, arrested, charged, and convicted of crimes.[59] This means that police exemptions in privacy laws contribute to the race, class, gender, citizenship status, and disability discrimination that is endemic in the criminal legal system. To be sure, this type of data discrimination is not limited to the criminal legal system. The police exemptions also further discrimination in the broader context of privacy and data—a problem well documented in our prior work, and by scholars such as Khiara Bridges, Virginia Eubanks, and others.[60]

The final category of harm pertains to the way that police exemptions in consumer privacy laws work at cross purposes with other rules and laws. For example, allowing police to access

---

personal data in a manner that discriminates against an individual or class of individuals, or otherwise makes unavailable the equal enjoyment of goods or services, on the basis of an individual's or class of individuals' actual or perceived race, color, sex, sexual orientation, gender identity, disability, religion, ancestry or national origin." ELEC. PRIV. INFO. CTR. & CONSUMER REPS, *supra* note 3.

[56] *See generally* Arnett, *supra* note 7; Kate Weisburd, *The Carceral Home*, 103 B.U. L. REV. 1879 (2023).

[57] Sarah Vendzules, *Guilty After Proven Innocent: Hidden Factfinding in Immigration Decision-Making*, 112 CALIF. L. REV. 697 (2024); Immigrant Project of the Nat'l Lawyers Guild & Immigrant Legal Res. Ctr., Practice Advisory: Gathering Criminal Records for Immigration Cases 4 (Aug. 31, 2022*)*

[58] *See* Virginia Eubanks, *The Digital Poorhouse*, HARPERS MAG. (Jan. 2018), https://harpers.org/archive/2018/01/the-digital-poorhouse/ [https://perma.cc/H9HR-5RLR]. *See generally* Chaz Arnett, *Data, the New Cotton*, JUST TECH: SOC. SCI. RSCH. COUNCIL (May 25, 2022), https://just-tech.ssrc.org/articles/data-the-new-cotton [https://perma.cc/J3PM-46RN].

[59] Eubanks, *supra* note 58; Arnett, *supra* note 58; Nazgol Ghandmoosh & Luke Trinka, *One in Five: How Mass Incarceration Deepens Inequality and Harms Public Safety*, THE SENT'G PROJECT (Jan. 16, 2024), https://www.sentencingproject.org/reports/one-in-five-how-mass-incarceration-deepens-inequality-and-harms-public-safety/ [https://perma.cc/HH44-Y2QK]; PEW RESEARCH CENTER, *Racial Disparities Persist in Many U.S. Jails* (May 16, 2023), https://www.pew.org/en/research-and-analysis/issue-briefs/2023/05/racial-disparities-persist-in-many-us-jails [https://perma.cc/KG8S-LY2V].

[60] *See supra* note 7 and accompanying text; Arnett, *supra* note 58; Arnett, *supra* note 7; Weisburd, *supra* note 56; VIRGINIA EUBANKS, AUTOMATING INEQUALITY: HOW HIGH-TECH TOOLS PROFILE, POLICE, AND PUNISH THE POOR (St. Martin's Press 2018); BRIDGES, *supra* note 7.

geolocation data from a company like Lyft seems in direct conflict with *Carpenter* and its progeny.[61] Likewise, these exemptions also may be in conflict with state laws that limit when police can access people's data—such as CalECPA.[62]

It is notable that in reviewing the policy arguments and legislative history for the consumer privacy bills, there was no mention of cooperation with law enforcement. This silence suggests that the police exemption language was perhaps an afterthought or a concession. To be sure, there may be other reasons for the inclusion of the police exemption language, but initial research drew up no information one way or the other.

C. People Connected to the Criminal Legal System Have Rights, Including Privacy Rights

Involvement in the criminal legal system—or even being suspected of a crime—does not render privacy rights irrelevant, much less privacy interests and protections. As previously noted, contrary to the police exemption language, police are not permitted to search someone—or their data—based on a hunch alone. Moreover, as the Supreme Court has made clear—data is different and police must obtain a warrant before accessing, for example, geolocation data or data on a cellphone.[63] As we have argued elsewhere, these laws apply to everyone—including those in the criminal legal system.[64]

To be sure, as a matter of law, people convicted of crimes have a lower expectation of privacy, but that does not mean they have—or should have—no privacy.[65] This is perhaps most obvious in the context of prison, where the privacy interests of those detained are recognized and weighed against the need for prison administration and security.[66] Likewise, people on various forms of court supervision—such as probation or parole—retain more privacy rights than those in prison, but still may be searched at any time without a warrant.[67] In prior work, we explored how these traditional legal principles have failed to keep pace with advancements in surveillance technology and the increased reliance on data for purposes of police investigation and carceral control.[68]

Consumer protection laws that allow for broad cooperation with law enforcement further the problem of the law being out of sync with advancements in technology. Given that people in the criminal legal system already have fewer privacy protections as a matter of law, it is all the more imperative for advocacy organizations to take account of their unique needs and the specific

---

[61] Carpenter v. United States, 585 U.S. 296 (2018) (holding that accessing historical cell-site location information from a person's phone is a Fourth Amendment search and requires a warrant).

[62] *See* CAL. PENAL CODE §§ 1546–1546.4 (West 2020 & Supp. 2025) (prohibiting government entities from compelling the production of or accessing electronic communication information without a warrant or the user's consent, subject to limited exceptions).

[63] *Carpenter*, 585 U.S. 296 (geolocation data); California v. Riley, 573 U.S. 373 (2014) (data on a cellphone).

[64] Chaz Arnett, *From Decarceration to E-Carceration*, 41 CARDOZO L. REV. 641, 689 (2019); Kate Weisburd, *Punitive Surveillance*, 108 VA. L. REV. 147 (2022).

[65] *Id.*

[66] *See* Kate Weisburd, *Rights Violations As Punishment*, 111 CALIF. L. REV. 1305, 1368 (2023).

[67] Samson v. California, 547 U.S. 843, 851–52 (2006); United States v. Knights, 534 U.S. 112, 114–15 (2001).

[68] Arnett, *supra* note 64, at 689; Weisburd, *supra* note 64.

ways that consumer data is used in police surveillance.

D. Police Exemptions Benefit Private Surveillance Companies

Significant questions can be raised about who primarily benefits from police exemptions. However, corporations appear to be well positioned to reap financial gains. In recent years, private companies have experienced substantial growth due to government contracts for policing and correctional services.[69] A large part of this growth can be attributed to investments in digital surveillance and data collection. Whether it is ViaPath charging three to five cents per minute for inmates to read their "free" prison issued tablets,[70] CoreCivic partnering with Tracktech to use wristband monitors on people during pretrial or post-trial proceedings,[71] or Palantir providing predictive analytics to local jurisdictions to label individuals and neighborhoods as threats,[72] such practices are both popular and profitable.[73]

Private companies that market policing and correctional technology hold an advantageous position over other companies that may have more rigorous compliance mandates under new data privacy laws. Police exemptions not only allow for unencumbered data capture, but they may also free up new pathways for profiteering. Take for example Securus Technologies unabashed privacy violations with the phone calls of people detained in jails and prisons.[74] Securus—one of two companies that control a combined 80% of prison voice and video calls[75]—recorded phone conversations to develop unique biometric signatures, known as voice prints.[76] These voiceprints, compiled from thousands of detained individuals, were stored in databases used to train AI voice recognition and transcription tools.[77] Securus was so aggressive in its profit-driven efforts that

---

[69] Sophie Hurwitz, *The Gleeful Profiteers of Trump's Police State*, MOTHERJONES (Feb. 6, 2025), https://www.motherjones.com/politics/2025/02/palantir-alex-karp-trump-private-prisons-profiteers [https://perma.cc/T8E6-FV4L].

[70] Valerie Surret, *The High Costs of Free Prison Tablet Programs*, THE APPEAL (Mar. 27, 2024), https://theappeal.org/the-high-costs-of-free-prison-tablet-programs-books-through-bars [https://perma.cc/NNX6-2J7A]; Kate Wolffe, *Almost All People Incarcerated In California Now Have Free Tablets*, CAPRADIO (Jul. 19, 2023),

https://www.capradio.org/articles/2023/07/19/almost-all-people-incarcerated-in-california-now-have-free-tablets [https://perma.cc/QUE7-EH6V].

[71] *CoreCivic Partners with TRACKtech to Provide a High-Tech Monitoring Solution*, CORECIVIC (Oct. 17, 2024), https://www.corecivic.com/news/corecivic-partners-with-tracktech-to-provide-a-high-tech-monitoring-solution [https://perma.cc/6Q3X-9FVB].

[72] Maha Ahmed, *Aided by Palantir, the LAPD Uses Predictive Policing to Monitor Specific People and Neighborhoods, THE INTERCEPT* (May 11, 2018), https://theintercept.com/2018/05/11/predictive-policing-surveillance-los-angeles [https://perma.cc/3EZ9-PKD4].

[73] Samantha Subin, *Palantir Soars 24% To Record High As AI Powers Strong Earnings and Guidance*, CNBC (Feb. 4, 2025), https://www.cnbc.com/2025/02/04/palantir-soars-more-than-23percent-as-ai-powers-strong-earnings-and-guidance.html [https://perma.cc/XC7U-X39T]; *CoreCivic Reports Fourth Quarter and Full Year 2024 Financial Results*, CORECIVIC (Feb. 10, 2025), https://ir.corecivic.com/news-releases/news-release-details/corecivic-reports-fourth-quarter-and-full-year-2024-financial [https://perma.cc/D232-EF4H]; Michael Tobin & Paula Seligson, *Prison-Phone Company ViaPath Wraps Up $1.38 Billion Debt Sale After New FCC Rules*, BLOOMBERG (Jul. 30, 2024), https://www.bloomberg.com/news/articles/2024-07-30/prison-phone-company-viapath-wraps-up-1-4-billion-debt-sale-after-new-fcc-rules [https://perma.cc/8VYH-8JPB].

[74] George Joseph and Debbie Nathan, *Prisons Across the U.S. Are Quietly Building Databases of Incarcerated People's Voice Prints*, THE INTERCEPT (Jan. 30, 2019), https://theintercept.com/2019/01/30/prison-voice-prints-databases-securus [https://perma.cc/6UNA-ZBZT].

[75] Tatiana Walk-Morris, *Prison Telecom Providers are Shifting Strategy by Exploiting Tablet Services* (Dec. 12, 2024), https://prismreports.org/2024/12/09/prison-telcom-providers-exploit-tablet-services/ [https://perma.cc/4HYX-2DTY].

[76] *Id.*

[77] Molly Burke, *Advocates Concerned As AI Monitors the Communications of Inmates*, TIMES UNION (Nov. 9, 2023),

even privileged phone conversations with attorneys were recorded.[78] Furthermore, the company sold to law enforcement the location data of the people making calls to prisons, expanding the privacy violations beyond those who were detained to their family and friend networks.[79]

This level of surveillance and data sharing would violate state privacy laws, but police exemptions expressly permit these practices, thereby sanctioning private companies operating as the "robber barons of prison tech."[80]

The relationship between profiteering and police exemptions should come as no surprise, given the lobbying efforts of both parties. Leading law enforcement organizations have played pivotal roles in pushing back against efforts to establish a more robust data privacy protection regime.[81] In a letter sent in June 2024 to the House Committee on Energy and Commerce, a coalition including the National Sheriffs' Association, the National Alliance of State Drug Enforcement Agencies, the National District Attorneys Association, and the Federal Law Enforcement Officers Association pleaded for a reconsideration of the public safety implications of the American Privacy Rights Act (APRA).[82] According to the coalition, the APRA "would weaken or eliminate access to common investigative research services and other investigative tools that are used successfully every day by local, state, and federal law enforcement agencies . . . "[83] In October 2024, the National Association of Police Organizations (NAPO) met with the director of the Consumer Financial Protection Bureau (CFPB) to levy complaints and recommend caution as the CFPB embarked on the development of rules to rein in the work of data brokers.[84]

These lobbying efforts have coincided with Big Tech and data broker efforts to weaken state data privacy bills.[85] And while tech firms have fed off law enforcement lobbying efforts, echoing claims that heavy data privacy regulations will hamper work with police investigations and jeopardize safety, what is ultimately at stake, of course, is profit, not altruism.[86] Current

---

https://www.timesunion.com/capitol/article/advocates-concerned-securus-technologies-n-y-18459465.php [https://perma.cc/ZWT8-SGE7].

[78] *Id.*

[79] Letter, Senator Ron Wyden, Complaint to FCC (May 8, 2018), https://www.wyden.senate.gov/imo/media/doc/wyden-securus-location-tracking-letter-to-fcc.pdf [https://perma.cc/4VU3-S8RW].

[80] Nitish Pawha, *The Robber Barons of Prison Tech*, SLATE (Dec. 12, 2023), https://slate.com/technology/2023/12/prison-telecom-gtl-viapath-jpay-securus-private-equity.html [https://perma.cc/3ZWY-WJ36].

[81] Letter, National District Attorneys Association et al., Letter to H. Comm. on Energy & Com. (Jun. 10, 2024), https://ndaa.org/wp-content/uploads/Final-APRA-LE-concern-letter-June-2024.pdf [https://perma.cc/36D6-VP2Y].

[82] *Id.*

[83] *Id.*

[84] Suzanne Smalley, *Police Seek Compromise With CFPB As Regulator Mulls Reining In Investigator Access To Sensitive Data*, THE RECORD (Nov. 1, 2024), https://therecord.media/police-lobbying-cfpb-data-broker [https://perma.cc/6U9N-57WU]. Interestingly, the NAPO asked for greater protections for police officer personal information, while requesting continued access to personal information of the general public, including data broker provided names, addresses, dates of birth, and Social Security numbers. *See* NAPO, THE WASHINGTON REP. NEWSL. (Oct. 18, 2024), https://www.napo.org/wp-content/uploads/2024/10/Washington-Report-October-18-2024.pdf [https://perma.cc/EC2E-D734].

[85] Emma Davis, *'Death By A Thousand Cuts': A Look At Big Tech's Efforts To Influence Data Privacy*, MD. MATTERS (July 5, 2024), https://marylandmatters.org/2024/07/05/death-by-a-thousand-cuts-a-look-at-big-techs-efforts-to-influence-data-privacy; Brendan Bordelon & Alfred Ng, *Tech Lobbyists Are Running The Table On State Privacy Laws*, POLITICO (Aug. 16, 2023), https://www.politico.com/news/2023/08/16/tech-lobbyists-state-privacy-laws-00111363 [https://perma.cc/Y4EN-6PDV].

[86] Alfred Ng, *Privacy Bill Triggers Lobbying Surge by Data Brokers*, POLITICO (Aug. 28, 2022), https://www.politico.com/news/

estimates predict that the revenue generated from the global data broker market will reach over 600 billion in five years, continuing to ensure incentives to use state laws to create privacy ceilings versus floors.[87]

III. THE PATH FORWARD: RECONCEPTUALIZING SAFETY AND PRIVACY

A. Ending the Era of Police Exemptions

Privacy scholars and advocates alike should no longer overlook the privacy interests of people suspected or convicted of crimes. In the particular context of consumer data protection, police exemptions should either be eliminated or significantly narrowed. There is no reason that the data protection statutes should be more permissive than the Fourth Amendment. At a minimum, law enforcement should be required to obtain a warrant before seeking data that is otherwise protected by consumer privacy laws. Language about turning over data for any police "inquiry" or "investigation" should be eliminated and replaced with a warrant requirement.

Of course, when it comes to protecting privacy, the Fourth Amendment is the floor not the ceiling, and state privacy laws can—and should—do more. For example, rather than focus on the individual rights of consumers, the laws could more broadly account for privacy interests and general privacy protections that do not hinge on individuals. Likewise, the laws can and should better account for the unique harms that flow from police exemption provisions and what these harms mean for the thousands of people targeted by police.

B. Moving Beyond a Rights Framework

The promotion of more inclusive state data privacy laws is a double-edged sword. On one side, they signal to and reveal the most vulnerable and expendable in our society, those whose privacy, and consequently humanity, is deemed unworthy of protection as part of the larger body politic. While on the other side, the fight for recognition under these laws commits to an outdated rights framework, casting serious doubts on the possibility of achieving the sorts of meaningful protections and relief desired. Indeed, much of the passing of data privacy law is performative.[88] Often dictated by narrow conceptions of privacy, mainstream debates on these issues often follow a routine "song and dance" where both the harms and potential redress are individualized.

But are individual rights the correct conduits for just outcomes and dignity?[89] This question is not limited to privacy law.[90] Part of the issue in the individual rights-based approach is that it

---

2022/08/28/privacy-bill-triggers-lobbying-surge-by-data-brokers-00052958 [https://perma.cc/H9LX-LCTF].

[87] *Global Data Broker Market Predicted to Reach US$616.541 Billion by 2030*, GLOBE NEWSWIRE (Feb. 14, 2025), https://www.globenewswire.com/news-release/2025/02/14/3026669/0/en/Global-Data-Broker-Market-Predicted-to-Reach-US-616-541-Billion-by-2030.html [https://perma.cc/8JHL-8YET].

[88] Ari Ezra Waldman, *Privacy, Practice, and Performance*, 110 CALIF. L. REV. 1233 (2022).

[89] Ari Ezra Waldman, *Privacy's Rights Trap*, 117 N.W. UNIV. L. REV. 117 (2022).

[90] For a discussion of the failure of individual rights idiom in the international and human rights context, *See* MAKAU MUTUA, HUMAN RIGHTS: A POLITICAL AND CULTURAL CRITIQUE 71, 128 (Univ. of Pa. Press 2002). For a discussion of this issue in the context of data justice, *see generally* Chaz Arnett, *Dystopian Dreams, Utopian Nightmares: AI and the Permanence of Race*, 112 GEO. L.J. 1339 (2024).

has engendered a myopic view of the cascade of social harms presented by the expansive datafication of the state and private sector, and allowed for the shifting of accountability from Big Tech to individuals. When people are already marginalized through criminal legal system involvement, it makes the offering of the standard data privacy self-help "rights" (i.e., access and deletion) ring even hollower.

This is not to say that current rights language and practices are useless. They may be leveraged to the extent that they lessen immediate burdens for marginalized groups of people. But given that they tend to limit our vision versus broadening our imagination of what a fuller conception of privacy could entail, simple inclusion of "rights" language in privacy legislation cannot be satisfactory. Ultimately, this will likely require the untethering of data privacy from the confines of traditional data and technology discourse to a place where critical questions about data power[91] and data justice[92] are centered.

C. Privacy & Safety Beyond Data and Technology

Police exemptions are generally justified as being necessary for ensuring public safety. Yet, this presumed relationship between privacy and security, where increased privacy causes a deficit in safety, must be interrogated. The presumption demands a reckoning with how we understand and conceive of safety in privacy law. Despite them being portrayed as seemingly at odds with one another, privacy is an indispensable component of safety. Consider how the proliferation of crowdsourced surveillance measures, like police sponsored Ring doorbell camera programs, threatens the expansion of racial profiling and vigilante violence.[93] Or how cumbersome employment policies for individuals on electronic ankle monitors may force impossible choices between unemployment and risky work in underground economies.[94] These practices undermine efforts to strengthen family and community connections and render us less safe.[95]

Some laws attempt to make this idea of privacy as a necessity for safety more legible. Take for example the European Union's Artificial Intelligence Act. The EU AI Act conceives of safety through the prism of "risks," where there are minimal risks, high risks, and unacceptable risks.[96] The use of AI-powered facial recognition systems was recently identified as one of several prohibited practices under the Act.[97] These prohibitions on unacceptable risks convey that there are privacy lines that should never be crossed, as the dangers presented make for less safe spaces and people. Yet, a risks framework has its own shortcomings. While focusing on risks enables targeted action against specific technological practices, it fails to fully grapple with the disparate

---

[91] *See generally* Arnett, *supra* note 90.

[92] *Id.* at 1336.

[93] Chaz Arnett, *Crowdsourcing Surveillance*, 72 UCLA L. REV. DISCOURSE 362, 382 (2024).

[94] Weisburd, *supra* note 64.

[95] We have come to associate surveillance with safety and technology with security. However, surveillance technology and information/data gathering cannot make us safe. Safety comes from strong communities, social supports and opportunities.

[96] Commission Regulation 2024/1689, art. 5, Artificial Intelligence Act, 2024 O.J (L SERIES) 51 (EC).

[97] *Id.*

power imbalances between corporate interests and individuals. These solutions may only begin to scratch the surface of a truly meaningful and robust safety policy. Realizing such safety may be reliant upon the sorts of privacy protections that would arise from more wholistic and participatory tech governance, where ordinary people are empowered to usher in a new era of digital democracy and control.

IV. CONCLUSION

Police exemptions have become a normalized feature of state data privacy law. These carveouts leave those targeted and impacted by the criminal legal system on the margins of advancing privacy protection. This practice is troubling because, while the preoccupation with information and data gathering has facilitated lucrative windfalls in the information economy, it has failed to make us more secure, fair, or efficient.[98] Even more, the reflexive capitulation to police exemptions allows for the skirting of important questions of power and justice in the ever-growing automated society.[99] We understand that the inclusion of criminal system-involved people within the purview of arguably weak individual rights-centered data privacy regimes may leave much to be desired for those interested in transformative change. However, until such changes can be made, inaction toward police and correctional circumvention of constitutional rights may be just as discomforting. Requiring warrants as an initial threshold could at least be a starting point for alleviating some of the heavy burdens that system-connected people carry in the wake of expansive surveillance and data capitalism. Although ultimately, traditional data privacy approaches may need to be abandoned as a necessary step as we move toward something more resembling data justice.

[98] Waldman, *supra* note 88.

[99] *Id*. at 1265.