2017

Democratic Surveillance

Mary Anne Franks
University of Miami School of Law, mafranks@law.miami.edu

Harvard Journal of Law & Technology
Volume 30, Number 2 Spring 2017

DEMOCRATIC SURVEILLANCE

*Mary Anne Franks**

TABLE OF CONTENTS

---

* Professor of Law, University of Miami School of Law. I am grateful to Danielle Citron, Rachel Levinson-Waldman, Orin Kerr, Jon L. Mills, participants in the 2015 Privacy Law Scholars Conference, the 2015 New Voices in Legal Theory Workshop, and the Brooklyn Law School Faculty Workshop for feedback on previous versions, and to Emily Cabrera for research assistance.

I. INTRODUCTION: SURVEILLANCE IS FOR EVERYONE

Today, everyone is watched. While surveillance is not new, "mass surveillance" is a relatively recent phenomenon. The mainstreaming of surveillance has helped spark an anti-surveillance, pro-privacy movement that extends across legal scholarship, policy debates, civil rights advocacy, political discourse, and public consciousness. Edward Snowden's 2013 revelations about the breadth and depth of government spying unleashed a global conversation about surveillance that shows no signs yet of abating.[1] Academics, legal experts, journalists, and activists churn out reports, studies, and articles detailing the harmful effects of surveillance on privacy and the need for robust privacy protections.[2] Privacy dominates the agenda of countless symposia, conferences, and workshops. The topic is even the eponymous subject of a theater production starring Daniel Radcliffe of "Harry Potter" fame.[3]

For those who have long advocated for a thoughtful and robust theory of privacy,[4] this is mass surveillance's silver lining. The fact that surveillance now targets privileged members of society along with marginalized populations has unleashed the political will to challenge it. As Rachel Levinson-Waldman, Senior Counsel to the Brennan Center's Liberty and National Security Program, observes, the "hidden blessing" of revelations about the extent and reach of mass government surveillance is that "majorities are opposed to surveil-

1. A Google search of the terms "'Edward Snowden' & privacy" yields nearly three million results as of August 2015. A July 2016 search of "Edward Snowden" in the Westlaw legal database under "Law Reviews and Journals" yields more than 600 results, an impressive number for a time period that spans not even three full years. *See also* Mark Mazzetti and Michael S. Schmidt, *Officials Say U.S. May Never Know Extent of Snowden's Leaks*, N.Y. TIMES (Dec. 14, 2013), http://www.nytimes.com/2013/12/15/us/officials-say-us-may-never-know-extent-of-snowdens-leaks.html [https://perma.cc/NH9J-43AX] ("Mr. Snowden's disclosures set off a national debate about the expansion of the N.S.A.'s powers to spy both at home and abroad.").

2. *See* Part II, *infra*.

3. Alexis Soloski, *Is Nothing Secret? Daniel Radcliffe and the Art of 'Privacy'*, N.Y. TIMES (July 3, 2016), http://www.nytimes.com/2016/06/26/theater/daniel-radcliffe-privacy.html [https://perma.cc/Z5E4-Q79B].

4. Privacy is of course a highly contested concept. There is great disagreement not only among scholars but also the general public about how to define privacy. That is not the focus of this Article. This Article does not attempt to resolve the controversy over the definition of privacy and accepts that privacy can be defined in multiple ways. The very general definition of privacy on which this Article loosely relies is the right of individuals to decide for themselves if, when, and how intimate information about them should be made available to others.

lance when 'average Americans' are the target."[5] In addition to average Americans, elites too are learning how mass surveillance affects their interests: "major tech companies have lost overseas business over fears that they are sharing their customers' private information with the government, and could lose more. U.S. senators — not usually the subjects of government surveillance — are also seeing their communications captured."[6]

The pro-privacy narrative that has emerged in the wake of this increasingly democratic surveillance is accordingly an occasion for both praise and criticism. Derrick Bell's interest convergence theory of the anti-discrimination movement of the 1950s and 1960s offers useful insights into the contemporary anti-surveillance movement.[7] According to Bell, white support of racial equality goals extended only so far as those goals served the interests of or at least did not conflict with those of whites.[8] When the interests of whites and blacks diverged, white support for racial equality disappeared.[9] This fact, Bell suggests, demonstrates that white support of racial equality was fundamentally indifferent to the harms that racial inequality imposes on blacks.[10] Remedies for racial equality are instead likely "the outward manifestations of unspoken and perhaps subconscious judicial conclusions that the remedies, if granted, will secure, advance, or at least not harm societal interests deemed important by middle and upper class whites."[11]

The contemporary pro-privacy, anti-surveillance movement is similarly limited by interest convergence. The movement is not primarily concerned with the harms imposed on the most vulnerable members of society, but rather with threats to mainstream and elite interests. Surveillance and other privacy violations that were largely tolerated so long as they burdened marginalized groups are challenged now that they affect privileged interests. This kind of interest convergence in privacy will result not in privacy reform across the board, but primarily in privacy reform that will protect, or at least not harm, the most powerful groups. As the contemporary privacy movement is still evolving, it is an opportune time to evaluate its strengths and limitations.

---

5. Rachel Levinson-Waldman, *How the NYPD Became George Orwell's Worst Nightmare*, SALON (May 12, 2015, 11:35 AM), http://www.salon.com/2015/05/12/how_the_nypd_became_george_orwells_worst_nightmare/ [https://perma.cc/975N-378P].

6. *Id.*

7. *See* Derrick A. Bell, Jr., Brown v. Board of Education *and the Interest-Convergence Dilemma*, 93 HARV. L. REV. 518, 523 (1980).

8. *See id.* at 522–523.

9. *See id.*

10. *See id.* at 523–524.

11. *Id.* at 523.

With regard to its strengths, the popular privacy narrative rightly emphasizes two important and historically under-recognized insights: first, invasions of privacy have devastating effects on the human personality, and second, consent to reveal private information is always contextual. Current privacy scholarship and advocacy provide extensive accounts of the pernicious effects of state intrusion into private lives[12] and criticize the use of formalistic conceptions of consent to serve as a blanket justification for greater and greater encroachments upon privacy.[13] These insights are vital to the preservation of a meaningful concept of privacy.

But while the widespread concern about surveillance and subsequent defense of privacy is in many ways a positive development, it is severely limited by selective origins. Mass resistance to surveillance emerged only when average and elite individuals became the targets of surveillance, and their the interests and viewpoints now dominate the contemporary narrative about privacy. The contemporary anti-surveillance movement has done too little to acknowledge the longstanding surveillance of marginalized populations and has given too little thought to what that history means for the future of privacy. By largely ignoring the history of surveillance, focusing on data privacy to the exclusion of other privacy concerns, and failing to adequately recognize the threat to privacy posed by non-state actors, the popular privacy movement undermines its own revolutionary possibilities.

Long before the government began collecting phone metadata and mining Big Data, entire segments of society were subjected to invasive forms of surveillance that inhibited their rights to free expression, movement, and association. In particular, the surveillance of African-Americans, the poor, and women has been tolerated — even encouraged — by mainstream society and justified by rationales ranging from maintaining public order[14] to reinforcing the natural order.[15] The practices of slavery and its enduring after-effects, from racial classification laws to mass incarceration, require extensive and intimate state invasions of privacy of black bodies. The poor, often quite literally unable to shield themselves from the gaze of the state, have been subjected to ruthless investigation and regulation in matters ranging from

---

12. *See, e.g.*, DANIEL SOLOVE, NOTHING TO HIDE (2011); Julie E. Cohen, *What Privacy Is For,* 126 HARV. L. REV. 1904 (2013); Neil M. Richards, *The Dangers of Surveillance*, 126 HARV. L. REV. 1934 (2013).

13. *See, e.g.*, Julie E. Cohen, *Privacy, Ideology, and Technology: A Response to Jeffery Rosen*, 89 GEO. L.J. 2029, 2041 (2001); Scott R. Peppet, *Unraveling Privacy: The Personal Prospectus and the Threat of A Full-Disclosure Future,* 105 NW. U. L. REV. 1153, 1186 (2011).

14. *See, e.g.*, Dorothy E. Roberts, *Foreword: Race, Vagueness, and the Social Meaning of Order-Maintenance Policing*, 89 J. CRIM. L. & CRIMINOLOGY 775 (1999).

15. See, for example, anti-miscegenation and anti-contraception laws.

childrearing to housing arrangements. Women's second-class status as citizens — imposed through centuries of legal and social inequality in marriage, education, employment, and reproduction— entailed state scrutiny and control of their most private decisions. For those whose lives are intersected by multiple forms of subordination, for example, poor black women, surveillance is a particularly complex and oppressive reality. The extensive and disruptive reach of surveillance into the lives of marginalized populations has largely gone unremarked in the current popular privacy narrative.

The second limitation of the current privacy narrative, closely related to the first, is the outsized focus on matters of informational privacy. Concerns over online tracking, data breaches, and GPS monitor-monitoring dominate surveillance discourse.[16] While these invasions of privacy are troubling, they pale in comparison to those routinely inflicted upon marginalized groups, including the physical harassment and brutality young black men suffer at the hands of police, the scrutiny and criminalization of everyday activities by homeless individuals, and the epidemic of sexual assault and harassment of women generally and domestic violence victims in particular. While mass surveillance by its nature affects greater numbers of people than targeted surveillance, it also tends to engender greater and more effective resistance. Targeted surveillance of marginalized groups, by contrast, generates less enthusiasm and opportunities for effective resistance. What is more, surveillance based on pernicious and illegitimate prejudices towards certain groups inflicts discriminatory social harms on society in addition to individual harms. Focusing reform and resistance primarily on informational privacy interests obscures other, more insidious, forms of surveillance.

The third limitation of the dominant privacy narrative is its narrow focus on the government as the primary threat to privacy and the primary source of surveillance. While the government's powers of surveillance are formidable, they are now inextricably tied to the private sector. The distinction between state and private actors is increasingly more theoretical than actual: the technology that makes mass surveillance possible was developed through collaboration between the government and private corporations, and the surveillance powers of the state are increasingly exercised through private technology. Cell phone carriers, social media applications, and search engines function as huge information reservoirs for the government, and many of these entities are more than happy to hand over the intimate data of

16. See, for example, the books, conferences, and resources listed on the websites of major privacy organizations such as the Electronic Privacy Information Center (https://www.epic.org/), the International Association of Privacy Professionals (https://iapp.org/), and the Privacy + Security Forum (https://privacyandsecurityforum.com/).

their users, sometimes at a profit. What is more, an excessive focus on the government as the primary threat to privacy also ignores the potential of "social tyranny," as John Stuart Mill termed it, to wreak more damaging and intimate havoc than state oppression.[17]

The rise of government surveillance and the rapid pace of technological progress have given the more privileged classes of society a glimpse of the longstanding experiences of the less privileged classes. This democratization of surveillance provides a unique opportunity to democratize privacy. Now that everyone's interests are affected by surveillance, everyone's interests must be considered in resisting surveillance. By focusing on the concerns of the privileged, the privacy movement that has emerged from these developments undermines its own transformative potential.

Privacy reform fueled by interest convergence has two negative consequences. The first is that — predictably — the privacy rights of vulnerable populations continue to be diminished. The second, less intuitive result is that the quality of privacy for everyone else is also diminished. That is because marginalizing the experiences of those most vulnerable to surveillance is counter-productive to anti-surveillance goals. It is precisely those who have suffered the most, and in multiple ways, from social and legal injustices who are best positioned to lead the way in reforming them. Those who have experienced the harshest deprivations of privacy and the most oppressive forms of surveillance have the deepest understandings of their dynamics.

Accordingly, even those who do not care about the welfare of disadvantaged groups for their sake should care about it for their own sakes — an approach we might call enlightened interest convergence.[18] The revolutionary potential of privacy cannot be achieved without addressing the longstanding race, gender, and class inequalities that have plagued the theory and practice of privacy. A democratic conception of privacy, by emphasizing the experiences of those most vulnerable to its violation, offers the best chance of securing privacy for all.

Part II outlines what the contemporary popular narrative about privacy and surveillance gets right, including the emphasis on privacy as key to the development and flourishing of democracy and the human personality. Part III discusses the limitations of this narrative, in particular its erasure of the history of the surveillance of marginalized communities, its excessive focus on data privacy to the exclusion of other forms of privacy, and its overly simplistic view of the state as

17. *See infra* Section III.C.1.

18. For elaboration of the concept of enlightened self-interest from which I am borrowing, see ADAM SMITH, THE WEALTH OF NATIONS 26–27 (1976) and ALEXIS DE TOCQUEVILLE, DEMOCRACY IN AMERICA 528–29(1966).

the enemy of privacy and the source of surveillance. Part IV introduces the concept of "intersectional surveillance," which describes how those subjected to multiple sources of subordination are also subjected to multiple sources of surveillance, and provides specific examples focusing on black bodies, poor bodies, and female bodies. Part V offers two cautionary tales to illustrate the consequences of an undemocratic, interest-convergence approach to privacy and surveillance: the push for police body cameras and the resistance to sexual privacy legislation. It also discusses the contrast between two Supreme Court cases, *Terry v. Ohio* and *Papachristou v. City of Jacksonville,* to demonstrate privacy possibilities beyond interest-convergence. Part VI concludes by exploring how we can use the democratization of surveillance to democratize privacy.

II. WHAT THE CONTEMPORARY PRIVACY NARRATIVE GETS RIGHT

The contemporary anti-surveillance, pro-privacy narrative that is the focus of this Article has emerged from an amalgam of sources: scholars, politicians, security experts, policymakers, civil liberties organizations, media, and social media. The "popular" privacy narrative (as opposed to the academic narrative) tends to focus on the impact of surveillance for the middle class and elites. The academic privacy narrative suffers from this as well, though many scholars are attentive to the history and practice of various privacy inequalities.[19] The popular privacy narrative is significant because it sets the terms of debate for the discussion of privacy and surveillance that will have — and already has had — significant real-world consequences. There is much to praise and much to criticize in this popular narrative.

This Part focuses on the positive: how the narrative brings to the surface two key insights about privacy that have been submerged in the digital age. The first insight is that invasions of privacy are invasions of the human personality itself. The fear of surveillance inhibits individual freedoms of expression and association, which in turn undermines the possibility of an open and democratic society. The se-

19. *See , e.g.*, ANITA ALLEN, UNEASY ACCESS: PRIVACY FOR WOMEN IN A FREE SOCIETY (1988); VIRGINIA EUBANKS, DIGITAL DEAD END: FIGHTING FOR SOCIAL JUSTICE IN THE INFORMATION AGE (2012); JOHN GILLIOM, OVERSEERS OF THE POOR: SURVEILLANCE, RESISTANCE, AND THE LIMITS OF PRIVACY (2001); CHRISTIAN PARENTI, THE SOFT CAGE: SURVEILLANCE IN AMERICA FROM SLAVERY TO THE WAR ON TERROR (2004); Anita Allen, *Gender and Privacy in Cyberspace*, 52 Stan. L. Rev. 1175 (2000); Khiara M. Bridges, *Privacy Rights and Public Families*, 34 HARV. J.L. & GENDER 113 (2011); Michelle Estrin Gilman, *Welfare, Privacy, and Feminism*, 39 U. BALT. L.F. 1 (2008) [hereinafter Gilman, *Welfare*]; Michelle Estrin Gilman, *The Class Differential in Privacy Law*, 77 BROOK. L. REV. 1389 (2012) [hereinafter Gilman, *The Class Differential*]; Elizabeth M. Schneider, *The Synergy of Equality and Privacy in Women's Rights*, 2002 U. CHI. LEGAL F. 137 (2002).

cond is that consent to exposure is a contextual and nuanced affair, not an on-off switch. That is, an individual's consensual exposure of private information to one party does not imply consent to all parties. Privacy is not secrecy; it is the right of the individual to choose who can access private information and who cannot.

A. Privacy and Personality

The insight that privacy is essential to the human personality and that surveillance inhibits its flourishing has a long but uneven history in the United States. Since the late 1800s, the popularity of this idea has waxed and waned, approaching near obscurity in the techno-optimism[20] of the 1980s and 1990s. Contemporary privacy scholarship and activism has helped to revive this insight in the era of mass surveillance.

In their famous 1890 essay, *The Right to Privacy*, Samuel Warren and Louis Brandeis wrote that the right to privacy was not to be understood as a mere property right, but as something even more foundational: the right to human personality itself.[21] The right to privacy is part of the fundamental right "to be let alone" and is similar to "the right not to be assaulted or beaten, the right not to be imprisoned, the right not to be maliciously prosecuted, [and] the right not to be defamed."[22] According to Warren and Brandeis, the right to privacy should not be confused with a property right, but is based on an even more foundational and absolute principle: "that of an inviolate personality."[23]

Brandeis continued to advocate for a deeply personal and psychological concept of privacy as a Justice of the Supreme Court. In *Olmstead v. United States*, the infamous Fourth Amendment case from 1928 in which the majority maintained that privacy was fundamentally concerned with tangible property, Brandeis authored a stinging and influential dissent, insisting that the "makers of our Constitution . . . knew that only a part of the pain, pleasure, and satisfactions of life are to be found in material things. They sought to protect Americans in their beliefs, their thoughts, their emotions and their sensations."[24]

---

20. *See* Daniel Kao, *The Good and Bad of Techno-Optimism in the Valley*, DIPLATEEVO (June 2015), https://www.diplateevo.com/the-good-and-bad-of-techno-optimism-in-the-valley/ [https://perma.cc/Y8GP-NYWY] (defining techno-optimism as "a phrase used to describe the mindset that the future is getting better due to the advances and application of technology in all industries").

21. *See* Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 196–97 (1890).

22. *Id.* at 205.

23. *Id.*

24. Olmstead v. United States, 277 U.S. 438, 478 (1928).

Brandeis's view was vindicated in 1967, when the Supreme Court overruled *Olmstead* to find that the Fourth Amendment "protects people, not places."[25] Justice Harlan's concurrence in *Katz v. United States* offered a two-part test to elaborate upon this protection: people are protected by the Fourth Amendment when they "have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'"[26]

The Court, however, soon began thinning out this conception of privacy in cases such as *United States v. White,* where a plurality of the Court ruled that evidence obtained from an informant wearing a wire transmitter while he spoke with the defendant could be used against the defendant at trial.[27] Justice William O. Douglas, dissenting in that case, emphasized the link between privacy and freedom of expression.[28] Monitoring "kills free discourse and spontaneous utterances," he wrote, and each individual must be "the sole judge of as to what must be said and what must remain unspoken. This is the essence of the idea of privacy implicit" in the First Amendment."[29]

Justice Douglas elaborated upon the relationship between privacy and the development of the human personality by quoting former United States Attorney General William Ramsey Clark at length:

> Privacy is the basis of individuality. To be alone and be let alone, to be with chosen company, to say what you think, or don't think, but to say what you will, is to be yourself. . . .
>
> Few conversations would be what they are if the speakers thought others were listening. Silly, secret, thoughtless and thoughtful statements would be affected. . . . To penetrate the last refuge of the individual, the precious little privacy that remains, the basis of individual dignity, can have meaning to the quality of our lives that we cannot foresee.[30]

Justice Douglas's dissent highlights the fact that privacy as a constitutional right is not just a matter of the Fourth or Fourteenth Amendments, but also of the First and Fifth Amendments. At one time, privacy was quite strongly associated with the Fifth Amendment

---

25. Katz v. United States, 389 U.S. 347, 361 (1967).
26. *Id.*
27. *See* United States v. White, 401 U.S. 745, 745 (1971).
28. *See id.* at 762.
29. *Id.* at 762–63.
30. *Id.* at 763.

privilege against self-incrimination.[31] In 1964, the Supreme Court found that the privilege "reflects many of our fundamental values and most noble aspirations," including "our respect for the inviolability of the human personality and of the right of each individual 'to a private enclave where he may lead a private life.'"[32]

Legal scholar Arthur R. Miller's *The Assault on Privacy*, published in 1971, detailed the extensive threat that technology and surveillance pose to privacy. One of the many potential negative effects of what Miller referred to as the "dossier society" was that "people may increasingly base their decisions and fashion their behavior in terms of enhancing their record image in the eyes of those who may have access to it in the future."[33] Miller was reacting to the fetish of "openness" that seemed to characterize the era of new technology,[34] a fetish that only increased in the ensuing decades. As the Internet began to transform everything from personal communication to record-keeping to commerce, the phrase "information wants to be free" became a rallying cry.[35]

The contemporary privacy narrative has, to its great credit, rediscovered the destructive disciplinary effects of surveillance that were submerged during the era of techno-optimism in the 80s and 90s.[36] These insights have taken on a new urgency in recent years, triggered in large part by the increasingly invasive surveillance measures adopted by the U.S. government post-9/11 and the measures adopted in the global "war on terror." Edward Snowden's 2013 revelations about the depth and breadth of United States and other government surveillance programs pushed the question of surveillance into public view and made the concern over privacy go viral, and not only in legal or academic circles. Countless books, law review articles, op-eds, news stories, conferences, classes, blog posts, studies, and hashtags have been dedicated to the question of privacy in the modern age,[37] most focusing heavily on the facilitation of government surveillance through technology and data mining.

In 2014, Human Rights Watch and the American Civil Liberties Union ("ACLU") published a report, *With Liberty to Monitor All:*

---

31. *See, e.g.*, Christopher Slobogin, *Subpoenas and Privacy*, 54 DePaul L. Rev. 805, 809–10 (2005) (noting that "the Court's early Fifth Amendment decisions were focused on protection of privacy").

32. Murphy v. Waterfront Comm'n of N.Y. Harbor, 378 U.S. 52, 55 (1964) (internal citations omitted).

33. ARTHUR MILLER, THE ASSAULT ON PRIVACY 50 (1971).

34. *See* ASTRA TAYLOR, THE PEOPLE'S PLATFORM 1–10 (2014).

35. *See* Cory Doctorow, *Saying Information Wants to be Free Does More Harm Than Good*, THE GUARDIAN (May 18, 2010, 2:00 PM), https://www.theguardian.com/technology/2010/may/18/information-wants-to-be-free [https://perma.cc/M98V-PMUX].

36. *See* DANIEL J. SOLOVE, NOTHING TO HIDE: THE FALSE TRADEOFF BETWEEN PRIVACY AND SECURITY 11 (2011).

37. *See* Mazzetti and Schmidt, *supra* note 1.

How Large-Scale US Surveillance is Harming Journalism, Law, and American Democracy.[38] The report references Snowden's revelations regarding U.S. spying programs, including the collection of "vast quantities of information — known as 'metadata' — about phone calls made to, from, and within the US. . . . [,] the content of international chats, emails, and voice calls. . . . [, and] massive amounts of cell phone location data," as well as "millions of images so the NSA can run facial recognition programs" and "hundreds of millions of email and chat contact lists around the world . . . ."[39]

Such programs, according to the report, stifle journalists, lawyers, and ultimately democracy itself.[40] Journalists interviewed for the report say that surveillance programs "constrain[] their ability to investigate and report on matters of public concern, and ultimately undermine[] democratic processes by hindering open, informed debate."[41] Lawyers "expressed concern over their ability to satisfy their professional duty of confidentiality, maintain their attorney-client relationships, and effectively represent their clients."[42] The report asserts, "Everyone has the right to communicate with an expectation of privacy, including privacy from unwarranted or indiscriminate surveillance by governments. This right . . . is essential not just to individual freedom of expression, but to the fair and accountable functioning of a democracy."[43]

In January 2014, the PEN American Center, the largest branch of the literary and human rights organization PEN International, published a report titled *Global Chilling: The Impact of Mass Surveillance on International Writers*.[44] One of the report's key findings was that "writers around the world are engaging in self-censorship due to fear of surveillance."[45] According to the report, "40% of U.S. writers surveyed by PEN in October 2013 reported curtailing or avoiding activities on social media, or seriously considered doing so";[46] 33% "deliberately steered clear of certain topics in personal phone conversations or email messages, or seriously considered doing so";[47]

---

38. G. Alex Sinha & Aryeh Neier, *With Liberty to Monitor All: How Large-Scale US Surveillance is Harming Journalism, Law, and American Democracy*, HUMAN RIGHTS WATCH (July 28, 2014), https://www.hrw.org/report/2014/07/28/liberty-monitor-all/how-large-scale-us-surveillance-harming-journalism-law-and [https://perma.cc/W3HC-S5HJ].

39. *Id.*

40. *See id.*

41. *Id.*

42. *Id.*

43. *Id.*

44. PEN AMERICAN CENTER, GLOBAL CHILLING: THE IMPACT OF MASS SURVEILLANCE ON INTERNATIONAL WRITERS 1 (2015), http://www.pen.org/sites/default/files/globalchilling_2015.pdf [https://perma.cc/QE7Y-Q4TY].

45. *Id.* at 9.

46. *Id.* at 10.

47. *Id.* at 11.

and 27% "refrained from conducting internet searches or visiting websites on topics that may be considered controversial or suspicious, or seriously considered doing so."[48]

A 2014 Harris poll found that nearly half of all respondents (43%) had "changed their online behavior and think more carefully about where they go, what they say, and what they do online" in the wake of the National Security Agency [("NSA")] revelations, including 26% doing less banking online, 24% less inclined to use email, and 26% doing less online shopping. [49] A 2016 study published in the *Journalism & Mass Communication Quarterly* found empirical evidence that "the government's online surveillance programs may threaten the disclosure of minority views and contribute to the reinforcement of majority opinion."[50] All of these reports and surveys seem to reinforce the Deputy Legal Director of the ACLU Jameel Jaffer's statement in the *New York Times*: "The chilling effect of surveillance makes our public debates narrower and more inhibited and our democracy less vital."[51] Several legal scholars have offered similar conclusions about the harmful impact of surveillance on individual autonomy and expression. Neil Richards, for example, argues that surveillance is harmful because it can "chill the exercise of our civil liberties. . . . [S]urveillance of people when they are thinking, reading, and communicating with others in order to make up their minds about political and social issues. . . . is especially dangerous because it can cause people not to experiment with new, controversial, or deviant ideas."[52] Julie Cohen maintains that privacy "shelters dynamic, emergent subjectivity from the efforts of commercial and government actors to render individuals and communities fixed, transparent, and predictable."[53] This focus on privacy's importance for the human personality, and on the inhibiting and disciplinary effects of privacy invasions, is both important and necessary in the new surveillance era.

---

48. *Id.* at 11.

49. Stephen Cobb, *New Harris Poll Shows NSA Revelations Impact Online Shopping, Banking, and More*, WELIVESECURITY (April 2, 2014), http://www.welivesecurity.com/2014/04/02/harris-poll-nsa-revelations-impact-online-shopping-banking/ [https://perma.cc/6MA4-WS7K].

50. Elizabeth Stoycheff, *Under Surveillance: Examining Facebook's Spiral of Silence Effects in the Wake of NSA Internet Monitoring*, JOURNALISM & MASS COMM. Q. 296, 307 (2016).

51. Jameel Jaffer, Eric Posner & Joshua Foust, *Is the N.S.A. Surveillance Threat Real or Imagined?*, N.Y. TIMES (June 9, 2013), http://www.nytimes.com/roomfordebate/2013/06/09/is-the-nsa-surveillance-threat-real-or-imagined [https://perma.cc/6VTW-KHF8].

52. Neil Richards, *The Dangers of Surveillance*, 126 HARV. L. REV. 1934, 1935 (2013).

53. Cohen, *supra* note 12, at 1905.

B. The Context of Consent

The other key insight rehabilitated by the contemporary surveillance narrative concerns the contextual nature of consent. In *The Assault on Privacy*, Miller explained how formalistic and absolutist understandings of consent are used to counter invasion of privacy claims.[54] If a person engaged "in activity inconsistent with a desire to maintain his privacy" or "consented to the dissemination of personal information," the argument goes, then he has not truly experienced an invasion of privacy.[55] This attitude has been clearly displayed in the Supreme Court's Fourth Amendment jurisprudence since the 1970s, and it is one that many contemporary privacy scholars and activists are actively attempting to resist.

As mentioned above, a plurality in *United States v. White* found that the defendant did not have a reasonable expectation of privacy in information he voluntarily relayed to another party, despite being unaware that the third party was wearing a wire.[56] Similarly, in the 1976 case *United States v. Miller*, the Court found that a defendant who had voluntarily turned over his financial information to his bank extinguished his expectation of privacy in that information.[57] In *Smith v. Maryland*, the Court found that people have no legitimate expectation of privacy in telephone numbers they dial, as these numbers are available to and recorded by telephone companies.[58] In *California v. Greenwood*, the Court found that there is no reasonable expectation of privacy in trash left out for garbage collection.[59] In these and several other cases, the Court developed what has come to be known as the third party doctrine, which holds that a person retains no expectation of privacy in information made available to another party. This doctrine has also been characterized as equating privacy with secrecy:[60] retaining a constitutionally protected right to privacy in information requires keeping that information completely secret.

The rationale for the third party doctrine rests on a highly formalistic conception of consent that has become even more formalistic over time. In cases such as *White,* the Court was able to point to the fact that the defendants had freely and deliberately chosen to disclose

---

54. *See* MILLER, *supra* note 33, at 185–186.

55. *Id.* at 185.

56. *See supra* Section I.A.

57. *See* United States v. Miller, 425 U.S. 435, 443–45 (1976).

58. *See* Smith v. Maryland 442 U.S. 735, 735 (1978).

59. *See* California v. Greenwood, 486 U.S. 35, 41, 43 (1988).

60. Daniel J. Solove, *Conceptualizing Privacy*, 90 CAL. L. REV. 1087, 1107 (2002) ("In a variety of legal contexts, the view of privacy as secrecy often leads to the conclusion that once a fact is divulged in public, no matter how limited or narrow the disclosure, it can no longer remain private.").

information to third parties.[61] But in *Miller*, *Smith*, and *Greenwood*, the disclosures could not be said to be more than nominally consensual. As Justice Brennan observed in his dissent in *Miller*, "[f]or all practical purposes, the disclosure by individuals or business firms of their financial affairs to a bank is not entirely volitional. It is impossible to participate in the economic life of contemporary society without maintaining a bank account."[62] Justice Marshall voiced a similar objection in *Smith v. Maryland*, where he asserted that "privacy is not a discrete commodity, possessed absolutely or not at all. Those who disclose certain facts to a bank or phone company for a limited business purpose need not assume that this information will be released to other persons for other purposes."[63] Justice Brennan, dissenting in *Greenwood*, pointed out that Greenwood was required by a county ordinance to dispose of his trash on the curb.[64] What is more, Justice Brennan noted, "the voluntary relinquishment of possession or control over an effect does not necessarily amount to a relinquishment of a privacy expectation in it."[65] If privacy really were the same thing as secrecy, "a letter or package would lose all Fourth Amendment protection when placed in a mailbox or other depository with the 'express purpose' of entrusting it to the postal officer or a private carrier."[66] The rejection of privacy-as-secrecy arguably underpins *Katz* itself, holding what an individual "seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected."[67]

In *The Assault on Privacy*, Miller similarly criticizes the idea that nominal consent destroys a reasonable expectation of privacy. Miller noted that a key problem with the "consent defense" is that it tends to overlook the coercive pressures often involved in transactions that expose individuals' private information.[68] Miller contended that "[w]hether a particular disclosure really is voluntary obviously depends on the circumstances surrounding it, as well as the individual's personality and chemistry."[69]

This sophisticated view of consent and the sensitivity to its contextual nature, like the insights into the negative impact of surveillance, receded in the era of techno-optimism. As technology raced ahead of the comprehension of its consequences, increasingly lengthy and complex contracts regarding the use of private information became common, contracts that virtually no one reads before accept-

61. *See* United States v. White, 401 U.S. 745, 749–752 (1970).
62. United States v. Miller, 425 U.S. 435, 451 (1976) (Brennan, J., dissenting).
63. *Smith*, 442 U.S. at 749 (Marshall, J., dissenting).
64. *See* California v. Greenwood, 486 U.S. 35, 54–55 (1988) (Brennan, J., dissenting).
65. *Id.* at 55.
66. *Id.*
67. Katz v. United States, 389 U.S. 347, 351 (1967).
68. *See* MILLER, *supra* note 33, at 185–86.
69. *Id.* at 186.

ing.[70] Consent was increasingly "aggregated": the acceptance of use of information in one context became acceptance of use in very different contexts. Formal — what at least one scholar would called "fictional"[71] — consent to terms and conditions of Internet use, retail purchases, social media products, and government services became the basis on which to justify aggregating and redistributing information about users on a scale few had anticipated.[72]

The emerging popular privacy narrative has highlighted the contextual nature of consent and begun to push back against the idea that privacy equals secrecy. This can be seen in Justice Sotomayor's concurring opinion in *United States v. Jones*, a case involving the warrantless placement by law enforcement of a GPS tracking device on a vehicle. Justice Sotomayor considers that the time may have come to rethink the third-party doctrine of *United States v. Miller* and its ilk:

> [I]t may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties. This approach 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. People disclose the phone numbers that they dial or text to their cellular providers; the URLs that they visit and the e-mail addresses with which they correspond to their Internet service providers; and the books, groceries, and medications they purchase to online retailers. . . . I for one doubt that people would accept without complaint the warrantless disclosure to the Government of a list of every Web site they had visited in the last week, or month, or year. . . . I would not assume that all information voluntarily disclosed to some member of the public for a limited purpose is, for that reason alone, disentitled to Fourth Amendment protection.[73]

Justice Sotomayor here emphasizes the significance of context with regard to voluntary disclosures of information. Professor Helen

---

70. *See, e.g.*, Omri Ben-Shahar and Carl E. Schneider, *The Failure of Mandated Disclosure*, 159 U. PA. L. REV. 647 (2011).

71. *See* Margaret Jane Radin, *Boilerplate Today: The Rise of Modularity and the Waning of Consent*, 104 MICH. L. REV. 1223, 1231 (2006).

72. *See* Danielle Keats Citron & Frank Pasquale, *Network Accountability for the Domestic Intelligence Apparatus*, 62 HASTINGS L.J. 1441 (2011).

73. United States v. Jones, 565 U.S. 400, 417–18 (2012) (Sotomayor, J., concurring). *But see* Orin Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561 (2009).

Nissenbaum coined the term contextual integrity to describe the key to preserving privacy.[74] Nissenbaum defines contextual integrity as "compatibility with presiding norms of information appropriateness and distribution," specifying that privacy violations should be assessed according to multiple factors, including "the nature of the situation or context; the nature of the information in relation to that context; the roles of agents in receiving information; their relationships to information subjects; on what terms the information is shared by the subject; and the terms of further dissemination."[75] Professor Daniel Solove urges privacy law to directly confront questions of consent:

> What does consenting to something really mean? What should the law recognize as valid consent? Many transactions occur with some kind of inequality in knowledge and power. When are these asymmetries so substantial as to be coercive? The law's current view of consent is incoherent, and the law treats consent as a simple binary (that is, it either exists or it does not). Consent is far more nuanced, and privacy law needs a new approach that accounts for the nuances without getting too complex to be workable.[76]

The contemporary privacy narrative's emphasis on the complexities of consent is an urgently needed corrective in the age of rapidly advancing technology.

III. THE LIMITATIONS OF THE CONTEMPORARY PRIVACY NARRATIVE

The foregoing demonstrates how the contemporary narrative about surveillance has resurfaced two important insights about the nature of privacy: first, surveillance is harmful because of its disciplinary impact on human personality and democratic association; second, equating privacy with secrecy overlooks the importance of contextual consent. This has been accomplished, however, in a way generally inattentive to how this disciplinary impact of surveillance and the equation of privacy with secrecy affect — and have always affected — marginalized populations far more intimately and destruc-

74. *See* Helen Nissenbaum, *Privacy as Contextual Integrity*, 79 WASH. L. REV. 119, 155 (2004).

75. *Id.*

76. Daniel J. Solove, *Introduction: Privacy Self-Management and the Consent Dilemma*, 126 HARV. L. REV. 1880, 1901 (2013).

tively than mainstream society. As Derrick Bell argued with regard to racial equality, the interests and experiences of those who suffer the most harm are considered the least.[77] The attention paid to the effects of privacy violations on the human personality and the contextual nature of consent is highly selective. The privacy narrative emphasizes the experiences of relatively privileged members of society, which produces a distorted picture of the history, theory, and practice of surveillance. This Part addresses three flaws in this narrative that have particularly negative consequences for the future of privacy: 1) the erasure of marginalized individuals' longstanding experiences of surveillance; 2) an outsized emphasis on data privacy to the exclusion of other forms of privacy; and 3) an unjustifiably narrow focus on the state as the primary threat to privacy.

A. Erasing Histories of Surveillance: Marginalized Bodies

The surveillance of marginalized populations has a long and troubling history. Race, class, and gender have all helped determine who is watched in society, and the right to privacy has been unequally distributed according to the same factors. If the current privacy movement is genuinely concerned about the harms of surveillance, it should focus on the experiences of those individuals who have suffered under it the most. The surveillance of marginalized bodies is key to understanding the history and the lessons of surveillance.

1. Black Bodies

The institution of slavery imposed wide-ranging and diverse harms that can be understood in many ways, from physical cruelty to entrenchment of racism to economic appropriation. Slavery is less often described in terms of its destructive effects on human privacy,[78] but the description is no less true for that. Beyond obvious brutality and dehumanization, slavery entailed the routine inspection and exposure of black bodies. The bodies of slaves were constantly monitored through investigations of their fitness for work, the sexual assault of female slaves, and beatings of both male and female slaves. Families were routinely split up, denying enslaved individuals the freedom of intimate association and ability to care for their children — freedoms later recognized in American jurisprudence as essential to the concept of privacy.[79] Sexual assault deprived female slaves of the possibility

77. *See* Bell, *supra* note 7, at 523–24.

78. One exception is DECKLE MCLEAN, PRIVACY AND ITS INVASION 32 (1995).

79. *See* Eisenstadt v. Baird, 405 U.S. 438, 452–53 (1972); Griswold v. Connecticut, 381 U.S. 479, 482 (1965); Pierce v. Soc'y of Sisters, 268 U.S. 510, 534–35 (1925); Meyer v. Nebraska, 262 U.S. 390, 400 (1923).

of reproductive control, forcing them to gestate and bear the children of white masters while prohibiting them from engaging in consensual intimacy and reproduction.[80] The Fugitive Slave Act of 1850 legalized the monitoring and pursuit of African-Americans who escaped their slaveholders, stripping away even the most basic opportunities for self-determination.[81]

The abolition of slavery brought with it new methods of control over black bodies. Racial classification laws, segregation laws, anti-miscegenation laws, and adoption laws all served not only to brutalize and subordinate African-Americans but also to keep them under constant regulation.[82] The slightest rumor of impropriety could lead to beatings, property damage, or lynching.[83] The actions of black people, especially any actions perceived as affecting white interests, were aggressively scrutinized and subject to violent discipline.

In the modern era, mass incarceration provides extensive opportunities to monitor and control the bodies of prisoners, a population that is overwhelmingly made up of black men.[84] In prison, bodies are literally stripped, examined, and subject to routine inspections.[85] Beatings by other inmates or by guards are common, and sexual assaults are frequent.[86] No true privacy exists for intimate activities, and there is little or no space for decisional privacy[87] — that is, almost no opportunity to exert control over how and when one associates with others or how to spend one's time. The effects of incarceration persist long after a sentence has been served, often entailing years of moni-

---

80. *See* DOROTHY ROBERTS, KILLING THE BLACK BODY: RACE, REPRODUCTION, AND THE MEANING OF LIBERTY 22–55 (1997); Zanita E. Fenton, *An Essay on Slavery's Hidden Legacy: Social Hysteria and Structural Condonation of Incest*, 55 HOWARD L.J. 319, 331–32 (2012).

81. *See* STANLEY W. CAMPBELL, THE SLAVE-CATCHERS: ENFORCEMENT OF THE FUGITIVE SLAVE LAW, 1850–1860 121 (1968).

82. *See* Kevin Noble Maillard & Rose Cuison Villazor, *Introduction* to LOVING V. VIRGINIA IN A POST-RACIAL WORLD: RETHINKING RACE, SEX, AND MARRIAGE 1, 1–2 (Kevin Noble Maillard & Rose Cuison Villazor eds. 2012).

83. *See generally* IDA B. WELLS, SOUTHERN HORRORS AND OTHER WRITINGS: THE ANTI-LYNCHING CAMPAIGN OF IDA B. WELLS 1892–1900 (Jacqueline Jones Royster ed., 1997).

84. *See generally* MICHELLE ALEXANDER, THE NEW JIM CROW (2010).

85. While it is true that some forms of surveillance in prisons are significantly different in kind from surveillance outside of prisons, particularly those that are conducted for safety purposes, the harm of the privacy invasion is still significant.

86. *See* Mary Anne Franks, *How to Feel Like A Woman, or Why Punishment Is A Drag*, 61 UCLA L. REV. 568, 572 (2014).

87. *See* Anita L. Allen, *The Proposed Equal Protection Fix for Abortion Law: Reflections on Citizenship, Gender, and the Constitution*, 18 HARV. J.L. & PUB. POL'Y 419, 440 (1995) ("Decisional privacy can be understood as the liberty, freedom or autonomy to make choices about one's own life, minimally constrained by unwanted government or other outside interference.").

toring by the state through conditions of probation and severely constraining professional, educational, intimate, and civic opportunities.[88]

Today, the black population is subject to extensive, literal, daily policing in many cities across the United States. From disproportionate uses of force in police encounters to frequent stops and frisks, black bodies are under constant suspicion and scrutiny. This extends beyond state actors to private citizens, from "subway vigilantes" like Bernhard Goetz, who shot four unarmed young black men after they demanded five dollars,[89] to "neighborhood watchmen" like George Zimmerman, who stalked and ultimately killed a young, black, unarmed teenager named Trayvon Martin.[90] Young black men and women are taught that their bodies are considered threats in themselves, and that because of this they can expect to be followed, investigated, questioned, and evaluated wherever they go.[91]

2. Poor Bodies

In a 1991 article titled *Are the Poor Entitled to Privacy?*, Professors Robin and Robert Collin detailed the multiple ways in which poor people are denied privacy, from housing to subsistence benefits to reproductive choices to government searches.[92] They deplored the "commodification" of privacy that essentially treats privacy as a privilege that must be paid for. The authors argued that "privacy must mean something both more and less than money and the things that money can buy"[93] and that "the privacy we allot to poor people is a measure of our own humanity and the withholding of privacy and dignity is a measure of our inhumanity."[94]

The lack of privacy for homeless individuals is compounded by the "criminalization of the homeless," which refers to the ways that

---

88. *See, e.g.*, Molly Carney, *Correction Through Omniscience: Electronic Monitoring and the Escalation of Crime Control*, 40 WASH. U. J.L. & POL'Y 279, 280 (2012); Reuben Jonathan Miller & Amanda Alexander, *The Price of Carceral Citizenship: Punishment, Surveillance, and Social Welfare Policy in an Age of Carceral Expansion*, 21 Mich. J. Race & L. 291, 292 (2016).

89. *See* People v. Goetz, 497 N.E.2d 41, 43 (N.Y. 1986).

90. *See Trayvon Martin Shooting Fast Facts*, CNN (last updated Feb. 7, 2016), http://www.cnn.com/2013/06/05/us/trayvon-martin-shooting-fast-facts/ [https://perma.cc/S5BS-BHZ4].

91. *See generally* Mary Anne Franks, *How Stand Your Ground Laws Hijacked Self-Defense,* in GUNS AND CONTEMPORARY SOCIETY: THE PAST, PRESENT, AND FUTURE OF FIREARMS AND FIREARM POLICY (2015); Heather Digby Parton, *Black Bodies Are Not Weapons: Why White Supremacists Insist Michael Brown Was 'Armed'*, SALON (Nov. 26, 2014), http://www.salon.com/2014/11/26/black_bodies_are_not_weapons_why_white_supremacists_insist_michael_brown_was_armed/ [https://perma.cc/6MKM-5NDP].

92. Robin Morris Collin & Robert William Collin, *Are the Poor Entitled to Privacy?*, 8 HARV. BLACKLETTER J. 181, 215 (1991).

93. *Id.* at 219.

94. *Id.*

homeless people are surveilled, harassed, and arrested for engaging in activities that would be perfectly legal inside a home: standing or sitting in one place for long periods of time, sleeping, drinking alcohol, and engaging in sexual activity.[95] Violent physical attacks on homeless individuals are frequent, as are assumptions about drug use, sexual predation, and laziness.[96] Homeless individuals have few opportunities to shield themselves from view of either law enforcement or an unsympathetic public. Fourth Amendment jurisprudence makes clear that the home is the most protected site of privacy[97]; those without homes, of course, have no means of accessing these protections.

Professor Christopher Slobogin has observed that the law governing constitutional seizures, which allows for arrests to be made in public without a warrant, results in very different protections for those with homes and those without:

> the police virtually never need a warrant to arrest either a homeless person or a person who spends most of his time outdoors because his home is crowded, in a state of disrepair, or simply unpleasant. In contrast, the person with a good home is generally protected from warrantless arrest in non-exigent circumstances.[98]

Echoing Robin and Robert Collin, Slobogin has also pointed out that the Supreme Court's assessment of the "reasonable expectation of privacy" largely turns on the resources one can deploy to protect privacy:

> Instead of declaring that one's living space and belongings are automatically entitled to constitutional protection — a conclusion that would seem to follow

---

95. *See* NAT'L L. CENTER ON HOMELESSNESS AND POVERTY, *No Safe Place: The Criminalization of Homelessness in U.S. Cities*, http://www.nlchp.org/documents/No_Safe_Place [https://perma.cc/9W5Q-ZHMP]. *See also* Paul Boden and Jeffery Selbin, *California is Rife with Laws Used to Harass Homeless People*, L.A. TIMES (Feb. 25, 2015), http://www.latimes.com/opinion/op-ed/la-oe-0216-boden-california-vagrancy-laws-target-homeless-20150216-story.html [https://perma.cc/4LCH-7SSP].

96. *See* ANTI-DEFAMATION LEAGUE, *Beyond Stigma and Stereotypes: What is Homelessness?* (2015), http://www.adl.org/assets/pdf/education-outreach/beyond-stigma-and-stereotypes-what-is-homelessness.pdf [https://perma.cc/6NZ7-95AV].

97. *See, e.g.*, Welsh v. Wisconsin, 466 U.S. 740, 748 (1984) ("It is axiomatic that the 'physical entry of the home is the chief evil against which the wording of the Fourth Amendment is directed.'") (quoting United States v. United States District Court, 407 U.S. 297, 313 (1972)). *See also* Kyllo v. United States, 533 U.S. 27, 34 (2001) (noting that the home is "the prototypical and hence most commonly litigated area of protected privacy").

98. Christopher Slobogin, *The Poverty Exception to the Fourth Amendment*, 55 FLA. L. REV. 391, 404–05 (2003). *See also* Collin & Collin, *supra* note 92.

> from the Fourth Amendment's explicit mention of "houses" and "effects" — the Court has signaled that the reasonableness of privacy expectations in such areas is contingent upon the existence of "effective" barriers to intrusion. In other words, one's constitutional privacy is limited by one's actual privacy. That stance ineluctably leads to the conclusion that Fourth Amendment protection varies depending on the extent to which one can afford accouterments of wealth such as a freestanding home, fences, lawns, heavy curtains, and vision- and sound-proof doors and walls.[99]

This "poverty exception" to the Fourth Amendment has received little attention in the popular privacy narrative, which tends to focus on law enforcement intrusion into cell phones, social media, and search engine histories.

For those who are impoverished but not homeless, the violations of privacy are still extensive. Obtaining welfare benefits or other social services often requires enduring intrusive questioning about one's family life, intimate associations, attempts at gainful employment, and drug and alcohol use, as well as home inspections.[100] Several states, such as Florida, have tried to require drug testing for welfare recipients as a prerequisite for obtaining benefits.[101]

In short, the bodies, habits, and decisions of poor people are closely monitored by both the state and general public. Fourth Amendment law, tasked with safeguarding the privacy interest of citizens against the government, effectively sets out different constitutional standards for the haves and the have-nots, and the criminalization of poverty and homelessness ensures that those with fewer resources are forced to accept daily surveillance of their daily activities and choices.

3. Female Bodies

In American culture, as in many cultures, women's bodies have long been treated as property. The doctrine of coverture, which held sway until the mid-1800s, held that women were "covered" by their

---

99. Slobogin, *supra* note 98, at 400–01.

100. *See* Danielle Keats Citron, *Technological Due Process*, 85 WASH. U. L. REV. 1249, 1263–64 (2008); Gilman, *Welfare*, *supra* note 19, at 2.

101. *See* Gilman, *Welfare*, *supra* note 19, at 11–12; Lizette Alvarez, *Court Strikes Down Drug Tests for Welfare Applicants,* N.Y. TIMES (Dec. 3, 2014), http://www.nytimes.com/2014/12/04/us/politics/court-strikes-down-drug-tests-for-florida-welfare-applicants.html [https://perma.cc/SJ9X-DQDY].

husbands upon marriage, losing whatever limited independent status they may have enjoyed prior to marriage.[102] As William Blackstone relates in his *Commentaries*, men had the legal right to discipline their wives through physical assaults.[103] The writings of Lord Hale make it clear that married women had no right to refuse sexual activity after marriage because marriage signified their irrevocable consent to their husband's sexual desires.[104] In other words, women were expected to accept beatings and rape as part of normal married existence. In addition to the obvious harms imposed by such expectations, this state of affairs also deprived women of physical privacy and disciplined them to conform their lives to men's desires.[105]

Coverture as such does not exist today in the U.S., but its legacy lives on. Domestic violence was not seriously recognized as a crime until the 1970s.[106] The typical response even today to the plight of battered women continues to be "why doesn't she leave?" — a question that not only erases male responsibility and ignores basic abuser dynamics, but also presumes that women facing unlawful violence should leave their homes. This flies directly in the face of the much-lauded protections of one's "castle."[107] One should not have to retreat from one's own home, as the home is supposed to *be* one's place of retreat. The casual expectation that women should give up the privacy protections of their own homes when faced with illegitimate aggression speaks volumes about social and legal views of women's privacy rights. To leave one's home is to forego solitude and privacy; wherever an abuse victim is forced to flee — whether to the home of a family member, to a shelter, or to the streets — she will face serious deprivations of her freedom of movement and her decisional and bodily privacy. Reporting abuse to the police subjects a victim to invasive,

---

102. *See* Reva B. Siegel, *The Modernization of Marital Status Law: Adjudicating Wives' Rights to Earnings, 1860–1930*, 82 GEO. L.J. 2127, 2127 (1994).

103. *See* WILLIAM BLACKSTONE, COMMENTARIES ON THE LAWS OF ENGLAND *421 (1765). *See also* Reva B. Siegel, *"The Rule of Love": Wife Beating As Prerogative and Privacy*, 105 YALE L.J. 2117, 2121–2122 (1996).

104. *See* SIR MATTHEW HALE, THE HISTORY OF THE PLEAS OF THE CROWN 629 (1847); Michelle J. Anderson, *Marital Immunity, Intimate Relationships, and Improper Inferences: A New Law on Sexual Offenses by Intimates*, 54 HASTINGS L.J. 1465, 1477–85 (2003).

105. *See* Kimberly D. Bailey, *It's Complicated: Privacy and Domestic Violence*, 49 AM. CRIM. L. REV. 1777 (2012).

106. *See Domestic Violence Law*, CRIMINAL JUSTICE, http://criminal-justice.iresearchnet.com/crime/domestic-violence/domestic-violence-law/ [https://perma.cc/39K3-WLRF] ("Domestic violence, specifically violence against women, was not recognized as a social problem until the mid-1970s.").

107. *See* Mary Anne Franks, *Real Men Advance, Real Women Retreat: Stand Your Ground, Battered Women's Syndrome, and Violence As Male Privilege*, 68 U. MIAMI L. REV. 1099, 1106–07 (2014) ("In traditional self-defense law, the 'castle doctrine' stipulates that one is not required to retreat from one's own home, even if it is possible to do so in complete safety.").

humiliating questioning and in many cases triggers an investigative process that puts her under quite literal surveillance.[108]

It is worth noting that popular conceptions of privacy have also historically been used as a shield for domestic violence.[109] For more than a century, the state invoked the concept of family privacy as a reason not to acknowledge or interfere with domestic relations.[110] While this misuse of privacy has lost some of its force in recent decades, respect for privacy is still often invoked to protect men's actions in intimate relationships.[111] This underscores the need to ensure that our conception of privacy is focused on the needs and interests of the most vulnerable.

Sexual assault, whether within marriage or not, is one of the most privacy-destroying forms of abuse. Victims are denied the most basic rights to refuse the intimate exposure and use of their bodies. The psychological after-effects of sexual assault can be lifelong and crippling, hindering victims' ability to feel in control of their bodies and of their most intimate decisions. Sexual harassment in the street, on public transportation, at work, and at school, remind women that their bodies are not truly their own.[112]

Technology has greatly exacerbated the surveillance and discipline of women's bodies, as women must now also navigate hidden cameras, the possibility of recorded sexual assaults, threats of "revenge porn," and the proliferation of online mobs engaging in vicious campaigns of sustained sexualized abuse.[113] Advances in surveillance technology have made stalking easier, cheaper, and more insidious.

---

108. *See, e.g.*, Andrea L. Dennis & Carol E. Jordan, *Encouraging Victims: Responding to a Recent Study of Battered Women Who Commit Crimes*, 15 Nev. L.J. 1, 13–14 (2014).

109. *See* CATHERINE A. MACKINNON, TOWARD A FEMINIST THEORY OF THE STATE 193 (1989), ("[T]he legal concept of privacy can and has shielded the place of battery, marital rape, and women's exploited domestic labor. It has preserved the central institutions whereby women are deprived of identity, autonomy, control, and self-definition."); *see generally* Elizabeth M. Schneider, *The Violence of Privacy*, 23 CONN. L. REV. 973 (1991).

110. *See* Rebecca Hulse, *Privacy and Domestic Violence in Court*, 16 WM. & MARY J. WOMEN & L. 237, 238 (2010); Suzanne A. Kim, *Reconstructing Family Privacy*, 57 HASTINGS L.J. 557, 557 (2006); *Domestic Violence and Privacy*, ELECTRONIC PRIVACY INFORMATION CENTER, https://epic.org/privacy/dv/ [https://perma.cc/FRH2-VXS6] ("Victims of domestic violence often need to protect their personal contact data from their abusers. However, the personal data industry in the United States makes this difficult."). *But see* Jeannie Suk, *Is Privacy a Woman?*, 97 GEO. L.J. 485, 488 (2009).

111. *See* Margaret Talbot, *Matters of Privacy*, NEW YORKER (Oct. 6, 2014), http://www.newyorker.com/magazine/2014/10/06/matters-privacy [https://perma.cc/P6SV-PENQ].

112. *See* Cynthia G. Bowman, *Street Harassment and the Informal Ghettoization of Women*, 106 HARV. L. REV. 517, 542 (1993) ("[T]he continuation and near-general tolerance of street harassment has serious consequences both for women and for society at large. It inflicts the most direct costs upon women, in the form of fear, emotional distress, feelings of disempowerment, and significant limitations upon their liberty, mobility, and hopes for equality.").

113. *See* Danielle Keats Citron & Mary Anne Franks, *Criminalizing Revenge Porn*, 49 WAKE FOREST L. REV. 345, 347 (2014).

Spyware, GPS monitoring, and webcam hijacking can turn a stalked woman's life into an unending nightmare.[114] Stalkers and abusive partners can now monitor virtually every move their targets make, whether that is searching the Internet for domestic violence support resources, dialing a family member's number from a cellphone, or driving their car to a friend's house.[115]

The denial of reproductive rights is yet another incursion into the privacy rights of women.[116] Interfering with a woman's most intimate decisions regarding her own body, including how to manage the risk of pregnancy, whether to bring a pregnancy to term, or how to control the timing and spacing of pregnancies, violates basic privacy rights. Requiring women to undergo unnecessary procedures such as transvaginal ultrasounds before allowing them to obtain abortions forces women to "consent" to physical invasions of their bodies — a form of legalized and medicalized sexual assault.[117] Requirements for abortions such as parental or spousal consent or notification also limit women and girls' access to reproductive health care and facilitate surveillance.[118] The increasing criminalization of pregnancy, including arrests of women who attempt suicide or use illegal drugs while pregnant, entails invasive scrutiny of women's most private struggles.[119]

Women can expect that nearly every detail of their intimate lives will be subject to multiple forms of surveillance by state as well as private actors, from domestic violence to sexual objectification to the denial of reproductive control. These forms of surveillance have serious, well-documented effects, ranging from loss of employment and educational opportunities, restrictions on the freedom to move, asso-

---

114. *See* Cindy Southworth & Sarah Tucker, *Technology, Stalking, and Domestic Violence Victims*, 76 MISS. L.J. 667, 667 (2007).

115. *See* Aarti Shahani, *Smartphones Are Used to Stalk, Control Domestic Abuse Victims*, NPR (Sept. 15, 2014), http://www.npr.org/blogs/alltechconsidered/2014/09/15/346149979/smartphones-are-used-to-stalk-control-domestic-abuse-victims [https://perma.cc/V36Z-AS7S].

116. *See* Linda McClain, *The Poverty of Privacy?*, 3 COLUM. J. GENDER & L. 119, 125 (1992).

117. *See* Kelsey Anne Green, *Humiliation, Degradation, Penetration: What Legislatively Required Pre-Abortion Transvaginal Ultrasounds and Rape Have in Common*, 103 J. CRIM. L. & CRIMINOLOGY 1171, 1172–73 (2013); Note, *Physically Intrusive Abortion Restrictions As Fourth Amendment Searches and Seizures*, 128 HARV. L. REV. 951, 958–67 (2015).

118. *See generally* Helaine F. Lobman, *Spousal Notification: An Unconstitutional Limitation on a Woman's Right to Privacy in the Abortion Decision*, 12 HOFSTRA L. REV. 531 (1984).

119. *See* Ferguson v. City of Charleston, 532 U.S. 67, 67 (2001). *See generally* ROBERTS, *supra* note 80; Michele Goodwin, *Prosecuting the Womb*, 76 GEO. WASH. L. REV. 1657 (2008); Emily Bazelon, *Purvi Patel Could Be Just the Beginning*, N.Y. TIMES MAG. (Apr. 1, 2015), https://www.nytimes.com/2015/04/01/magazine/purvi-patel-could-be-just-the-beginning.html [https://perma.cc/A36M-DU4H].

ciate, or dress as one wishes, interference with parenting abilities, and loss of general confidence.[120]

4. Bodies At the Intersection

The forces that marginalize individuals, whether race, poverty, or gender, do not exist in isolation from each other. Civil rights advocate and legal scholar Kimberle Crenshaw coined the term "intersectionality" to describe the "multidimensionality" of lived experience, in particular how certain individuals may face discrimination from multiple sources and on multiple levels.[121] She writes,

> Consider an analogy to traffic in an intersection, coming and going in all four directions. Discrimination, like traffic through an intersection, may flow in one direction, and it may flow in another. If an accident happens at an intersection, it can be caused by cars traveling from any number of directions, and, sometimes, from all of them.[122]

Using black women as her primary example, Crenshaw writes, "[I]f a Black woman is harmed because she is in the intersection, her injury could result from sex discrimination or race discrimination."[123] Though this Article focuses on the discussion of unequal surveillance based on race, class, and gender, an individual's experience may also be marked by any combination of class, disability, sexual orientation, gender identity, age, or other features.

In 2015, applying an intersectional analysis to the phenomenon of police brutality, Crenshaw explained that "[a]lthough Black women are routinely killed, raped, and beaten by the police, their experiences are rarely foregrounded in popular understandings of police brutality . . . . [I]nclusion of Black women's experiences in social movements, media narratives, and policy demands around policing and police brutality is critical to effectively combating racialized state violence for Black communities and other communities of color."[124] Pro-

120. *See* Tara Culp-Ressler, *This is What Women Are Forced to Do to Avoid Street Harassment*, THINK PROGRESS (Apr. 16, 2015), http://thinkprogress.org/health/2015/04/16/3647702/street-harassment-women-impact/ [https://perma.cc/6A3V-M9AR] (comparing the ways in which society expects women to alter their routines to avoid street harassment to the ways it tells women to change their behavior to avoid rape).

121. *See* Kimberle Crenshaw, *Demarginalizing the Intersection of Race and Sex: A Black Feminist Critique of Antidiscrimination Doctrine, Feminist Theory and Antiracist Politics*, 1989 U. CHI. LEGAL F. 139, 140 (1989).

122. *Id.* at 149.

123. *Id.*

124. *#SayHerName: Resisting Police Brutality Against Black Women*, AFR. AM. POL'Y F. (July 2015), http://www.aapf.org/sayhernamereport/ [https://perma.cc/YL4Z-XETT].

fessor Michele Gilman highlights how class and gender work together to intensify surveillance inequality, observing that "poor women have always had less privacy than other women,"[125] and detailing how poor women's economic needs translate into multiple forms of invasive surveillance along both class and gender axes: "As a condition of receiving welfare benefits, poor women have been subjected to drug tests, and they continue to face unannounced home inspections by government officials, fingerprinting, and restrictions on their reproductive choices."[126]

Attention to intersectionality is important for both ethical and pragmatic reasons. Understanding intersectionality is necessary to focus our attention on the most vulnerable members of society. We also cannot fully understand social problems without acknowledging how they are distributed unevenly across society and how they interact with each other.[127] The harms of surveillance are complex and compounding, and effective resistance requires confronting that fact. An intersectional approach to privacy recognizes that marginalized individuals are what the critical race scholar Mari Matsuda calls "epistemological sources."[128] Those with the longest and deepest experiences with subordination and oppression are the ones best equipped to develop strategies to conquer them.

B. Is Everything Data? Is Data Everything?

There is general agreement across the political spectrum that surveillance is harmful at least in part because it constrains individual autonomy and expression, which in turn jeopardizes the possibility of a truly democratic society. The disciplinary and inhibiting effects of surveillance can be very serious.[129] Beyond the impassioned rhetoric about chilling effects, however, specific articulation of the harm of mass surveillance can be difficult to find in privacy scholarship. For example, Bernard Harcourt's 2015 book *Exposed: Desire and Disobedience in the Digital Age* is full of dark proclamations about how

---

125. Gilman, *Welfare*, *supra* note 19, at 2.

126. *Id.*

127. *See* Lior Jacob Strahilevitz, *Toward a Positive Theory of Privacy Law*, 126 HARV. L. REV. 2010, 2010 (2013).

128. Mari J. Matsuda, *Looking to the Bottom: Critical Legal Studies and Reparations*, 22 HARV. C.R.-C.L. L. REV. 323, 325 (1987).

129. *See* Margot Kaminski & Shane Witnov, *The Conforming Effect: First Amendment Implications of Surveillance, Beyond Chilling Speech*, 49 U. RICH. L. REV. 465, 465–67 (2015). Some scholars have argued that the empirical evidence offered in support of the harm of surveillance alone is thin. *See* David Alan Sklansky, *Too Much Information: How Not to Think About Privacy and the Fourth Amendment*, 102 CAL. L. REV. 1069, 1094–101 (2014) (noting scant empirical evidence of what he calls the "stultification thesis"). *See also* Leslie Kendrick, *Speech, Intent, and the Chilling Effect*, 54 WM. & MARY L. REV. 1633, 1657–58 (2013).

we are all becoming "marketized subjects — or rather subject-objects who are nothing more than watched, tracked, followed, profiled at will, and who in turn do nothing more than watch and observe others."[130] While Harcourt raises compelling questions about the metaphysical consequences of a surveillance society, he never quite articulates what the actual harm of surveillance is. The closest the reader gets to a sense of the harm is in a personal anecdote Harcourt relates about being photographed by a security guard before a speaking engagement:

> I could not resist. I did not resist. I could not challenge the security protocol. I was embarrassed to challenge it, so I gave in without any resistance. But it still bothers me today. Why? Because I had no control over the dissemination of my own identity, of my face. Because I felt like I had no power to challenge, to assert myself.[131]

Clearly, Harcourt is troubled by the experience, but it is difficult to discern exactly why. There is no indication that the security guard is sadistic or voyeuristic, no suggestion that the photograph was ever used for anything other than its ostensible and fairly innocuous purpose. What is most striking is that being photographed as a routine security measure in a luxury Manhattan skyscraper appears to be the closest Harcourt has come to feeling under surveillance.[132] The presumption of harm, rather than the precise articulation of harm, is a common characteristic of the contemporary surveillance narrative.[133] When concrete examples of chilling effects of surveillance are described, they tend to be decidedly middle-class in nature: changes in one's online shopping, banking, and search engine habits due to concerns of being tracked.[134]

---

130. BERNARD HARCOURT, EXPOSED: DESIRE AND DISOBEDIENCE IN THE DIGITAL AGE 26 (2015).

131. *Id.* at 222.

132. *Id.* at 221–22. For a more extensive critique of Professor Harcourt's book, see Mary Anne Franks, *Unequal Exposure*, CONCURRING OPINIONS (March 18, 2016), https://concurringopinions.com/archives/2016/03/unequal-exposure.html [https://perma.cc/P69K-P4U3] (contribution to online symposium).

133. *See* DANIEL CASTRO & ALAN MCQUINN, INFO. TECH. & INNOVATION FOUND., THE PRIVACY PANIC CYCLE: A GUIDE TO PUBLIC FEARS ABOUT NEW TECHNOLOGIES 1–4 (2015), http://www2.itif.org/2015-privacy-panic.pdf [https://perma.cc/MHY4-S2YA]; Omri Ben-Shahar, *Privacy Paranoia: Is Your Phone Spying on You*?, FORBES (July 5, 2016), http://www.forbes.com/sites/omribenshahar/2016/07/05/privacy-paranoia-is-your-smartphone-spying-on-you/#2c63be345210 [https://perma.cc/8N6K-XR8K] (characterizing privacy fears of smart devices as "alarmist").

134. *See supra* Section II.A.

As Michele Gilman writes, low-income Americans do not strike the same "surveillance bargains" as middle- and high-income Americans: "Low-income Americans travel more often by bus than plane, they lack money to shop at Amazon.com, and they are less likely to have a computer that makes social networking possible in the first place."[135] That is, the kind of digital trail mostly left by middle- and upper-class Americans, and the primarily informational privacy interests at stake — financial data, shopping habits, search engine queries, and the like — are marked by class considerations.[136] Poor people, having far fewer possibilities of consumption, produce much less data of this kind compared to wealthy people.[137] Marginalized individuals, such as the imprisoned, the homeless, and the disabled, leave considerably fainter digital trails than the middle or upper class.[138] The focus on informational privacy also obscures other, arguably more significant, privacy interests. These factors are particularly significant when it comes to understanding the destructive effects of invasions of privacy and crafting solutions to the problem.

In *Too Much Information: How Not to Think About Privacy and the Fourth Amendment*, Professor David Sklansky argues that privacy, at least in terms of Fourth Amendment law, is "overloaded with information";[139] that is, "a preoccupation with data flows has led to the neglect of important dimensions of privacy."[140] While Sklansky acknowledges that some privacy scholars are "careful to avoid claiming that privacy can be reduced to information privacy,"[141] he notes that the information-based approach to privacy "now dominates the way most judges and scholars think about the Fourth Amendment,"[142] and the Fourth Amendment tends to dominate the way many people think about privacy.[143] Sklansky calls for a richer conception of privacy, one that focuses not just on information streams but also on embodied reality. Sklansky calls his alternative vision of privacy "privacy as refuge," focusing on searches of homes, strip searches, investigatory stops and frisks, and informants.[144]

Sklansky's analysis illuminates many of the shortcomings of an approach to privacy that focuses too heavily on information streams. Such a focus pushes arguably higher-stakes privacy invasions to the

135. Gilman, *The Class Differential*, *supra* note 19, at 1389–90.

136. *See* Sklansky, *supra* note 129, at 1086.

137. For a nuanced discussion of the digital divide, see EUBANKS, *supra* note 19, at 8.

138. KATHRYN ZICKUHR & AARON SMITH, PEW RES. CTR., INTERNET & AM. LIFE PROJECT, DIGITAL DIFFERENCES 2 (2012), http://pewinternet.org/Reports/2012/Digital-differences.aspx [https://perma.cc/MK6Q-8L5G].

139. Sklansky, *supra* note 129, at 1069.

140. *Id.*

141. *Id.* at 1102.

142. *Id.* at 1103.

143. *See id.*

144. *Id.* at 1113–21.

margins and privileges data over bodies. While Sklansky may overstate the distinction between informational privacy and bodily privacy (discussed below), his assessment of the limitations of a data-driven approach to privacy and surveillance is incisive. The harms caused by data privacy violations are certainly not trivial, especially in the age of data aggregation, when seemingly innocuous pieces of information can be combined with hundreds of other seemingly innocuous pieces of information to compose a comprehensive profile of an individual.[145] The point is not that such harms are not serious, but rather that they should encourage us to take even more seriously other, more substantial harms that bear a much more direct relationship with an individual's freedom. As Gilman points out, the digital divide "does not mean . . . that the poor are insulated from privacy intrusions."[146] On the contrary, they endure a barrage of information-collection practices that are far more invasive and degrading than those experienced by their wealthier neighbors.[147] If being forced to alter one's online search habits is considered a chilling effect that undermines democracy, being forced to alter one's clothing, job, school, choice of friends, communication with family, romantic relationships, or freedom of movement should surely be viewed even more seriously. For the less privileged members of society, surveillance does not simply mean inhibited Internet searches or decreased willingness to make online purchases; it can mean an entire existence under scrutiny, with every personal choice carrying a risk of bodily harm.

C. Determining the Real Threat: The State/Private Dichotomy

The contemporary privacy narrative tends to assume that the threat of surveillance emanates from the state. Numerous recent studies, surveys, and articles on privacy focus exclusively on violations by the government.[148] In the first instance, this position presumes that

---

145. *See* David E. Pozen, *The Mosaic Theory, National Security, and the Freedom of Information Act*, 115 Yale L.J. 628, 630 (2005).

146. Gilman, *The Class Differential*, *supra* note 19, 1389–90.

147. *See id.* at 1390–91.

148. *See, e.g.*, Emily Berman, *Quasi-Constitutional Protections and Government Surveillance*, 2016 B.Y.U. L. Rev. 771, 771 (2016); Ryan Calo, *Can Americans Resist Surveillance?*, 83 U. Chi. L. Rev. 23, 23 (2016); Orin S. Kerr, *A Rule of Lenity for National Securi-Security Surveillance Law*, 100 Va. L. Rev. 1513 (2014); Stephanie K. Pell & Christopher Soghoian, *A Lot More Than a Pen Register, and Less Than a Wiretap: What the StingRay Teaches Us About How Congress Should Approach the Reform of Law Enforcement Surveillance Authorities*, 16 Yale J.L. & Tech. 134 (2013); John Yoo, *The Legality of the National Security Agency's Bulk Data Surveillance Programs*, 37 Harv. J.L. & Pub. Pol'y 901 (2014); GALLUP, *Americans Disapprove of Government Surveillance Programs* (June 12, 2013), http://www.gallup.com/poll/163043/americans-disapprove-government-surveillance-programs.aspx [https://perma.cc/PUY5-X5ZW]; GLOBAL STRATEGY GROUP, PRIVACY RESEARCH SURVEY (May 18, 2017), https://www.aclu.org/sites/default/files/field_

government and private entities can be meaningfully distinguished from one another. On some level this is true, in that the government formally makes decisions about who and what to surveil, but the surveillance powers of the state are exercised by and through private technology, particularly Internet technology. The government was instrumental in the development of the Internet itself and was deeply involved in the creation of Google, the dominant search engine in the United States.[149]

Cell phone carriers, social media applications, and search engines now possess huge troves of user information. The information that the government uses to spy on its citizens is more often than not handed to them by private actors, sometimes for profit,[150] and many of these private technology actors are more than willing to hand over their users' intimate data to the government.[151] It should be widely known by now that technology giants such as Google and Facebook are not in fact free services, but rather platforms that essentially trade in users' private information. These companies' knowledge of the average citizen's browsing habits, intimate relationships, political views, and health status almost certainly outstrips that of any government entity. Many U.S. citizens seem unconcerned (or least comparatively less concerned) about the vast amounts of information they voluntarily hand over to these corporations, even though it has been repeatedly pointed out that these companies often work hand in hand with the government.[152] In any event, these companies' bottom lines are hardly in alignment with privacy-minded individuals.

Conventional wisdom would also indicate that we should worry most about the state's ability to intrude into our lives because of its power to incarcerate. But very few U.S. citizens have in fact found themselves facing incarceration or even investigation merely for their online searches or their metadata. Again, this does not mean that fear of such consequences are unfounded or trivial, but it does present a stark contrast to the actual deprivations of physical liberty experienced by, for example, black men, poor people, and women at the hands of both government and private actors.

The government's ever-increasing ability to exploit and aggregate data networks to spy on its citizens certainly does present new, powerful, and terrifying challenges to individual privacy, but the fixation on

---

document/privacy_poll_results.pdf [https://perma.cc/HP39-3BVV]; PEN AMERICAN CENTER, *supra* note 44.

149. *See infra* Section III.C.1.

150. *See, e.g.*, Heidi Boghosian, *The Business of Surveillance*, 39 A.B.A. HUM. RTS. 2, 3 (2013) (noting that "[i]n exchange for government contracts and funding, corporations amass and store a wealth of personal information on individuals easily retrievable by law enforcement agencies.").

151. *See infra* Section III.C.1.

152. *See, e.g.*, HARCOURT, *supra* note 130, at 14.

state as opposed to private surveillance demonstrates blindness to the harms of private surveillance, which for many people can have more far-reaching and serious consequences than official state surveillance.

1. There Is Nothing Outside the State

The groundwork for the Internet was laid in the 1960s, when the U.S. government created an organization called the Advanced Research Projects Agency ("ARPA") to develop a communications system that could withstand enemy attacks.[153] In the 1970s, the agency was taken over by the Department of Defense and renamed DARPA, or Defense Advanced Research Projects Agency.[154] In the 1980s, the National Science Foundation ("NSF"), a U.S. government agency; the National Aeronautics and Space Administration ("NASA"); and the U.S. Department of Energy provided backbone communication system facilities for the Internet.[155] While the Internet now functions as a result of collaboration among government agencies of many countries, private technology companies, and the academic community, it is important to bear in mind that the Internet was initially founded and developed by the U.S. government for military purposes.

According to a lengthy and detailed exposé by investigative journalist Dr. Nafeez Ahmed, the U.S. government — in particular its intelligence agencies — also played a key role in the development of what would become the country's most popular search engine, Google.[156] As Ahmed writes, "the United States intelligence community funded, nurtured and incubated Google as part of a drive to dominate the world through control of information. Seed-funded by the NSA and CIA, Google was merely the first among a plethora of private sector start-ups co-opted by US intelligence to retain 'information superiority.'"[157] Ahmed describes how, for the last two decades, a secret group sponsored by the Pentagon "has functioned as a bridge between the US government and elites across the business, industry, finance, corporate, and media sectors."[158] This group, known as the Highlands Forum, "has allowed some of the most powerful

153. *See* MITCH WALDROP, DEF. ADVANCED RESEARCH PROJECT AGENCY, DARPA AND THE INTERNET REVOLUTION (2008), http://www.darpa.mil/attachments/(2O15)%20Global%20Nav%20-%20About%20Us%20-%20History%20-%20Resources%20-%2050th%20-%20Internet%20(Approved).pdf [https://perma.cc/B8X6-ARNS].

154. *See id.*

155. *See A Brief History of NSF and the Internet*, NAT'L SCI. FOUND. (Aug. 13, 2003), https://www.nsf.gov/news/news_summ.jsp?cntn_id=103050 [https://perma.cc/57QVVJDR].

156. *See* Nafeez Ahmed, *How the CIA Made Google: Inside the Secret Network Behind Mass Surveillance, Endless War, and Skynet – Part 1*, MEDIUM (Jan. 22, 2015), https://medium.com/@NafeezAhmed/how-the-cia-made-google-e836451a959e [https://perma.cc/M53S-RBWV].

157. *Id.*

158. *Id.*

special interests in corporate America to systematically circumvent democratic accountability and the rule of law to influence government policies, as well as public opinion in the US and around the world."[159] The forum helped produce our current state of mass surveillance, which Ahmed claims serves sinister "operational purpose[s]," including:

> [A]ssisting with the lethal execution of special operations, selecting targets for the CIA's drone strike kill lists via dubious algorithms, for instance, along with providing geospatial and other information for combatant commanders on land, air and sea, among many other functions. A single social media post on Twitter or Facebook is enough to trigger being placed on secret terrorism watch-lists solely due to a vaguely defined hunch or suspicion; and can potentially even land a suspect on a kill list.[160]

Private companies regularly turn over user data in response to government requests.[161] Google provides information about how many of these requests it receives per year and how often it complies with the requests in its Transparency Report.[162] In the first half of 2014, Google received nearly 32,000 data requests from governments, providing information for 65% of the requests.[163] According to one estimate, AT&T and Verizon combined received one request from U.S. authorities every minute in 2013.[164] National Security Agency documents disclosed in August 2015 revealed that AT&T had assisted the agency on a much larger scale than previously thought.[165] According to the *New York Times*:

---

159. *Id.*

160. Nafeez Ahmed, *How the CIA Made Google: Inside the Secret Network Behind Mass Surveillance, Endless War, and Skynet – Part 2*, MEDIUM (Jan. 22, 2015), https://medium.com/insurge-intelligence/why-google-made-the-nsa-2a80584c9c1#.t2y8gqgg7 [https://perma.cc/P37B-WWC7].

161. *See* Spencer Ackerman & Dominic Rushe, *Microsoft, Facebook, Google and Yahoo Release US Surveillance Requests*, GUARDIAN (Feb. 3, 2014, 4:40 PM), https://www.theguardian.com/world/2014/feb/03/microsoft-facebook-google-yahoo-fisa-surveillance-requests [https://perma.cc/H8YU-M237].

162. *See* GOOGLE TRANSPARENCY REPORT, http://www.google.com/transparencyreport/userdatarequests/ [https://perma.cc/NC8F-L4WA].

163. *See id.*

164. *See* Brian Fung, *AT&T and Verizon Got Government Data Requests Once Every 60 Seconds Last Year. And That's Probably Lowballing It.*, WASHINGTON POST: THE SWITCH (May 5, 2014), http://www.washingtonpost.com/blogs/the-switch/wp/2014/05/05/att-and-verizon-got-government-data-requests-once-every-60-seconds-last-year-and-thats-probably-lowballing-it/ [https://perma.cc/GQ6G-E9VZ].

165. *See* Julia Angwin et al., *AT&T Helped U.S. Spy on Internet on a Vast Scale*, N.Y. TIMES (Aug. 15, 2015), http://www.nytimes.com/2015/08/16/us/politics/att-helped-nsa-spy-on-an-array-of-internet-traffic.html?_r=0 [https://perma.cc/TU7N-WSJF].

> The N.S.A.'s top-secret budget in 2013 for the AT&T partnership was more than twice that of the next-largest such program . . . . The company installed surveillance equipment in at least 17 of its Internet hubs on American soil, far more than its similarly sized competitor, Verizon. And its engineers were the first to try out new surveillance technologies invented by the eavesdropping agency.[166]

The true scale of government inquiries regarding user data is unknown, as many telecommunications companies do not disclose how many requests they receive, and neither National Security Letter ("NSL") or Foreign Intelligence Surveillance Act ("FISA") requests are disclosed.[167]

Sometimes the government takes an even more direct approach: as reported by the German newspaper *Der Spiegel*, experts in the NSA's Office of Tailored Access Operations hack PCs, routers, and servers for surveillance purposes, including physically intercepting hardware, installing backdoors, and then sending it along to the recipients.[168] While some private companies turn over user data reluctantly, other companies are quick to turn a profit. In December 2013, Senator Ed Markey released documents that revealed "[m]ajor U.S. cellphone providers received more than $20 million from law enforcement agencies in conjunction with more than 1.1. [sic] million user information requests in 2012 . . . ."[169]

One response to the ever-increasing invasiveness of governmental surveillance and the collusion between private and government entities has been the rise in popularity of privacy tools such as the Tor

---

166. *Id.*

167. *See* Lee Munson, *New Google Transparency Report Details Hike in Government User Data Requests*, SOPHOS: NAKED SECURITY (Sept. 17, 2014), https://nakedsecurity.sophos.com/2014/09/17/new-google-transparency-report-details-hike-in-government-user-data-requests/ [https://perma.cc/3F89-ST2S].

168. Jacob Appelbaum et al., *Inside TAO (Part 3: The NSA's Shadow Network)*, DER SPIEGEL: SPIEGEL ONLINE (Dec. 29, 2013), http://www.spiegel.de/international/world/the-nsa-uses-powerful-toolbox-in-effort-to-spy-on-global-networks-a-940969-3.html [https://perma.cc/7984-9PG6] ("If a target . . . orders a new computer . . . TAO can divert the shipping delivery to its own secret workshops. . . . At these so-called 'load stations' agents carefully open the package in order to load malware onto the electronics . . . that can provide backdoor access for the intelligence agencies."); *see also* Darlene Storm, *17 Exploits the NSA Uses to Hack PCs, Routers and Servers for Surveillance*, COMPUTER WORLD: SECURITY IS SEXY (Jan. 3, 2014, 1:47 PM), http://www.computerworld.com/article/2474275/cybercrime-hacking/17-exploits-the-nsa-uses-to-hack-pcs--routers-and-servers-for-surveillance.html [https://perma.cc/HB6K-MXN6].

169. Steven Nelson, *Cell Providers Collect Millions From Police for Handing Over User Information*, U.S. NEWS & WORLD REP. (Dec. 9, 2013, 3:04 PM), http://www.usnews.com/news/articles/2013/12/09/cell-providers-collect-millions-from-police-for-handing-over-user-information [https://perma.cc/E3NC-7RPC].

Network, free software that allows users to communicate anonymously by masking their location and usage from network surveillance and traffic analysis.[170] Both the Electronic Frontier Foundation ("EFF")[171] and Edward Snowden[172] have recommended using Tor to evade government surveillance. Unsurprisingly, then, the revelation in July 2014 that the NSA was targeting Tor users[173] was met with outrage from the privacy community. However, as Yasha Levin in *Pando Daily* points out, Tor itself was "developed, built and financed by the US military-surveillance complex."[174] Tor's famed "onion routing"[175] was not developed to protect privacy; it was developed "to allow intelligence and military personnel to work online undercover without fear of being unmasked by someone monitoring their Internet activity."[176] Levine notes a curious lack of acknowledgment by the EFF and others of the role the U.S. government has played and continues to play in Tor's development. He states, "[i]t's a nice story, pitting scrappy techno-anarchists against the all-powerful US Imperial machine. But the facts about Tor are not as clear cut or simple as these folks make them out to be . . . ."[177]

As Harcourt writes in *Exposed*, the idea of an enemy surveillance state is outdated and inaccurate.[178] Contemporary surveillance "involves a larger amalgam of corporate, intelligence, and security interests, . . . a 'surveillance-industrial empire' that includes those very telecommunication companies, as well as social media, retailers, and intelligence services . . . ."[179] Confronting contemporary surveillance requires acknowledging that state action is inextricably linked to private action, and vice versa.[180]

---

170. *About Tor*, TOR, https://www.torproject.org/about/overview.html.en [https://perma.cc/KW5P-QGXS].

171. *See* Eva Galperin et al., *Dear NSA, Privacy is a Fundamental Right, Not Reasonable Suspicion*, ELEC. FRONTIER FOUND. (July 3, 2014), https://www.eff.org/deeplinks/2014/07/dear-nsa-privacy-fundamental-right-not-reasonable-suspicion [https://perma.cc/GY8B-B76A].

172. *See* Max Eddy, *Snowden to SXSW: Here's How to Keep the NSA Out of Your Stuff*, PCMAG.COM (March 11, 2014), http://securitywatch.pcmag.com/security/321511-snowden-to-sxsw-here-s-how-to-keep-the-nsa-out-of-your-stuff [https://perma.cc/K9P8-5FTA].

173. *See* J. Appelbaum et al., *NSA Targets the Privacy-Conscious*, DAS ERSTE, http://daserste.ndr.de/panorama/aktuell/nsa230_page-1.html [https://perma.cc/K54U-CV5T].

174. Yasha Levine, *Almost Everyone Involved in Developing Tor Was (or Is) Funded by the US Government*, PANDO DAILY (July 16, 2014), http://pando.com/2014/07/16/tor-spooks/ [https://perma.cc/Y8WC-QEV4].

175. *See Onion Routing: Executive Summary*, ONION-ROUTER.NET, http://www.onion-router.net/Summary.html [https://perma.cc/WC6Y-U63Y].

176. Levine, *supra* note 174.

177. *Id.*

178. *See* HARCOURT, *supra* note 130, at 27–28.

179. *Id.* at 27.

180. *See* David Thaw, *Surveillance at the Source*, 103 KY. L.J. 405, 405–06 (2014–2015).

2. The State Is Not Always the Enemy

The contemporary surveillance narrative — and the contemporary civil liberties narrative that tends to accompany it — seems to take as a given that the state is evil and that any expansion of its powers is presumptively illegitimate. Not only does this perspective rest on a rigid distinction between state and non-state actors that, as demonstrated above, is more theoretical than real, it is also a deeply cynical position that ignores the power (indeed the obligation) of the state to safeguard shared values such as safety, security, and equality. The skepticism and cynicism towards the state that characterizes much civil liberties discourse is often justified, but can also be irrational, overblown, and self-defeating.

The state, at least in Western democratic societies, is at least theoretically accountable to the people. While one can dispute the extent and effectiveness of that accountability, it is arguably far greater than that of private entities. If government officials engage in surveillance, there is a possibility that these officials can be reprimanded or voted out. When a powerful company, offering products that no one pays for but everyone wants, engages in surveillance, it is more difficult to detect and much more difficult to address. Google, for example, has no particular incentive to care what the public thinks of its policies except to the extent that it affects the company's profitability. It is not bound, even theoretically, to the will of the people. Google's motto might have long been "Don't be evil,"[181] but if Google decides to be evil, who would be able stop it, and how? For that matter, why should anyone trust the judgment of a for-profit company with regard to what constitutes evil?

These questions are equally applicable to other non-state entities, even seemingly well-meaning ones advancing supposedly democratic causes. WikiLeaks, for example, has been praised for many years by civil libertarians and the mainstream media for its disclosure of classified information to the public.[182] In response to concerns about the

181. The company changed its motto to "Do the right thing." in February 2016. *See* David Mayer, *Why Google Was Smart to Drop its "Don't Be Evil" Motto*, FAST COMPANY (Feb. 9, 2016, 5:00 AM), http://www.fastcompany.com/3056389/the-future-of-work/why-google-was-smart-to-drop-its-dont-be-evil-motto [https://perma.cc/5QFB-G39K].

182. *See, e.g.*, Megan Friedman, *Julian Assange: Readers' Choice for TIME's Person of the Year 2010*, TIME (Dec. 13, 2010), http://newsfeed.time.com/2010/12/13/julian-assange-readers-choice-for-times-person-of-the-year-2010/ [https://perma.cc/47V3-JH9J]; Index on Censorship, *Winners of Index on Censorship Freedom of Expression Awards Announced*, XINDEX (April 22, 2008), https://www.indexoncensorship.org/2008/04/winners-of-index-on-censorship-freedom-of-expression-award-announced/ [https://perma.cc/5DX8-8Z8T] (announcing that WikiLeaks was awarded The Economist New Media Award in 2008 for being "an invaluable resource for anonymous whistleblowers and investigative journalists"); Editorial, *First, They Came for WikiLeaks. Then…*, THE NATION (Dec. 9, 2010), https://www.thenation.com/article/first-they-came-wikileaks-then/ [https://perma.cc/4CJE-

power of a private entity to make unilateral decisions about the disclosure of sensitive information, WikiLeaks founder Julian Assange assured an audience in 2010 that the organization has "a harm minimization policy" and would safeguard what he termed "legitimate secrets."[183] The *Associated Press* reported in August 2016 that WikiLeaks's disclosures have not just revealed information about international espionage and governmental misconduct; they have "also included the personal information of hundreds of people — including sick children, rape victims and mental health patients."[184] Critics say some of the information literally put people's lives at risk.[185] During the 2016 presidential election, WikiLeaks exposed information damaging to the Democratic National Committee and the Democratic presidential candidate, Hillary Clinton, a move that was viewed by some as an attempt to influence the outcome of the election.[186] In January 2017, WikiLeaks was criticized for threatening to expose the private information of thousands of verified Twitter users.[187] While WikiLeaks was lauded for helping to expose state surveillance, it did so by engaging in its own forms of surveillance, and not just of state actors. There is little reason to treat an entity such as WikiLeaks as more trustworthy or less dangerous than the state.

The presumption that the state has evil intentions, moreover, often forecloses other more trenchant analyses: for example, analyses focused on equal protection, arbitrariness, or power imbalances. If surveillance is being deployed to further marginalize vulnerable groups, that is certainly a cause for deep concern. If certain groups are being targeted for more invasive and inhibiting forms of surveillance than other groups, that too is a cause for concern. In other words, an analysis of government surveillance should be attentive to the role of social and cultural power. That is precisely what does not tend to happen in

---

NEEJ]; Paulina Reso, *5 Pioneering Web Sites That Could Totally Change the News*, N.Y. DAILY NEWS (May 19, 2010, 4:46 PM), http://www.nydailynews.com/news/money/5-pioneering-web-sites-totally-change-news-article-1.182979 [https://perma.cc/JGY9-BFN2]; *Julian Assange*, SAM ADAMS ASSOCIATES FOR INTEGRITY IN INTELLIGENCE, http://samadamsaward.ch/julian-assange/ [https://perma.cc/ZWV8-8PNE] (announcing the 2010 Sam Adams Associates for Integrity in Intelligence Award as WikiLeaks and Julian Assange).

183. *See* Raphael Satter & Maggie Michael, *Private Lives Are Exposed as WikiLeaks Spills Its Secrets*, ASSOCIATED PRESS (Aug. 23, 2016, 5:09 PM), http://bigstory.ap.org/article/b70da83fd111496dbdf015acbb7987fb/private-lives-are-exposed-wikileaks-spills-its-secrets [https://perma.cc/2JPE-PLGH].

184. *Id.*

185. *Id.*

186. *See, e.g.*, Kyle Cheney, *Assange Denies WikiLeaks Trying to Influence Election Outcome*, POLITICO (Nov. 8, 2016, 11:26 AM), http://www.politico.com/story/2016/11/julian-assange-election-day-statement-230931 [https://perma.cc/FT8W-PANG].

187. *See* Jessica Guynn, *WikiLeaks Threatens to Publish Twitter Users' Personal Info*, USA TODAY (Jan. 6, 2017, 2:54 PM), http://www.usatoday.com/story/tech/news/2017/01/06/wikileaks-threatens-publish-twitter-users-personal-info/96254138/ [https://perma.cc/2VYR-UFZY].

the dominant privacy narrative, which flattens out the distinctions between different kinds of privacy invasions and between different groups of people with varying histories and relationships to government power.

A more nuanced analysis of privacy and power might in fact lead us to conclude that at least in some contexts, the right answer might be more, not less, surveillance, at least in a distributional sense. For instance, if what is broadly referred to as overcriminalization is also a surveillance and privacy issue, we should also consider that the hyper-policing of poor minority individuals and their neighborhoods exists alongside the under-policing of privileged individuals and their neighborhoods.[188] Studies have shown that while stop and frisk policies and pretextual traffic stops are disproportionately targeted at minority individuals, white individuals are statistically considerably more likely to be carrying contraband.[189] While law enforcement focuses on black and Hispanic neighborhoods for drug surveillance, the majority of drug dealers are white.[190] Also significant: law enforcement's excessive investigative focus on drugs means that other crimes, such as sexual assault, are ignored. Sexual assault is one of the most under-investigated crimes, along with other crimes that disproportionately affect women, for example domestic violence and stalking.[191] As Bill Piper, the director of national affairs for the Drug Policy Alliance, observes, "Every dollar and police hour spent on nonviolent drug offenders is money and time not spent on real crime."[192] The over-policing of minority individuals for the perpetra-

---

188. *See generally* MICHAEL JAVEN FORTNER, BLACK SILENT MAJORITY: THE ROCKEFELLER DRUG LAWS AND THE POLITICS OF PUNISHMENT (2015).

189. *Ferguson Police Department Compared to New York Police Department*, INFOGR.AM, https://infogr.am/ferguson-police-department-compared-to-new-york-police-department [https://perma.cc/GU2Y-E2SZ]; New York Civil Liberties Union, STOP AND FRISK: REPORT ON 2011 FINDINGS, http://www.nyclu.org/files/stopandfrisk-factsheet.pdf [https://perma.cc/3BY5-J2RK]; Aviva Shen, *White People Stopped by New York Police Are More Likely to Have Guns or Drugs Than Minorities*, THINK PROGRESS (May 22, 2013), http://thinkprogress.org/justice/2013/05/22/2046451/white-people-stopped-by-new-york-police-are-more-likely-to-have-guns-or-drugs-than-minorities/ [https://perma.cc/2BA4-J4MD].

190. *See* Jamie Fellner, *Race, Drugs, and Law Enforcement in the United States*, 20 STAN. L. & POL'Y REV. 257, 261 (2009) ("Although the majority of those who shared, sold, or transferred serious drugs in Seattle are white . . . almost two-thirds (64.2%) of drug arrestees are black. . . . The researchers could not find a 'racially neutral' explanation for the police prioritization of the downtown drug markets and crack." (citation omitted)).

191. In cases of violence and abuse of women, the law is often remarkably solicitous towards privacy concerns — of the alleged perpetrators. *See, e.g.*, Talbot, *supra* note 111.

192. Bill Piper, *Thousands of Rapists Are Not Behind Bars Because Cops Focus on Marijuana Users*, THE HUFFINGTON POST (Jun. 17, 2014, 3:18 PM), http://www.huffingtonpost.com/bill-piper/rape-kit-backlog_b_5504287.html [https://perma.cc/W8HM-FA4D].

tion of minor, non-violent crimes is often coupled with the under-policing of serious crimes against minority victims.[193]

3. The Tyranny of Non-State Actors

In addition to reinforcing a false dichotomy between state and private entities and promoting an unjustifiably totalizing view of the ills of state surveillance, the hyper-focus on the state as the enemy in surveillance discourse also obscures and understates the harms caused by non-state actors. In his classic libertarian text, *On Liberty*, John Stuart Mill takes pains to note that the role played by "public authorities" and "political functionaries" in undermining liberty often pales in comparison to the role of what he refers to as "society."[194] Mill cautions against focusing exclusively on the power of state, rather than private, action to undermine liberty:

> Like other tyrannies, the tyranny of the majority was at first, and is still vulgarly, held in dread, chiefly as operating through the acts of the public authorities. But reflecting persons perceived that when society is itself the tyrant — society collectively, over the separate individuals who compose it — its means of tyrannizing are not restricted to the acts which it may do by the hands of its political functionaries.[195]

Mill observes how, despite the fact that the state has more brute power, the dictates of non-state actors are often more destructive of liberty:

> Society can and does execute its own mandates: and if it issues wrong mandates instead of right, or any mandates at all in things with which it ought not to meddle, it practises a social tyranny more formidable than many kinds of political oppression, since, though not usually upheld by such extreme penalties, it leaves fewer means of escape, penetrating much more deeply into the details of life, and enslaving the soul itself.[196]

Accordingly, Mill called for safeguards not only against the state's interference with the development of the human personality, but of

193. *See* JILL LEOVY, GHETTOSIDE: A TRUE STORY OF MURDER IN AMERICA 9 (2015).
194. JOHN STUART MILL, ON LIBERTY 7–30 (2nd ed. 1859).
195. *Id.* at 13.
196. *Id.*

society's, which has its own powerful means of destroying individuality and autonomy:

> Protection, therefore, against the tyranny of the magistrate is not enough: there needs protection also against the tyranny of the prevailing opinion and feeling; against the tendency of society to impose, by other means than civil penalties, its own ideas and practices as rules of conduct on those who dissent from them; to fetter the development, and, if possible, prevent the formation, of any individuality not in harmony with its ways, and compel all characters to fashion themselves upon the model of its own.[197]

Mill's call for vigilance against the power of private society to enforce conformity was echoed a century later by William Ramsey Clark, who noted that "[w]hen a government degrades its citizens, or permits them *to degrade each other*, however beneficent the specific purpose, it limits opportunities for individual fulfillment and national accomplishment,"[198] a passage quoted by Justice Douglas in his dissent in the 1971 case *United States v. White*.[199] But these sentiments have been largely drowned out by the dire assurances of contemporary civil libertarians that the state is the real enemy.

Thus, even as police brutality rightly becomes an object of nationwide scrutiny, much less attention is paid to the role that private racism and violence plays in violating the privacy of minority individuals and pushing them towards conformity, from being followed around in stores by suspicious salespeople[200] to confrontations with angry or fearful armed white men.[201] In the wake of shootings of unarmed black men by would-be vigilantes, many in the black community expressed their fear that there was nothing a young black man could wear, do, or say, that would not raise his chances of being as-

---

197. *Id.* at 13–14. *See also* Mary Anne Franks, *Unwilling Avatars: Idealism and Discrimination in Cyberspace*, 20 COLUM. J. GENDER & L. 224, 252 (2011).

198. RAMSEY CLARK, CRIME IN AMERICA 287 (1970) (emphasis added).

199. United States v. White, 401 U.S. 745, 764 (1971).

200. *See* Angela Fichter, *The Emotional Toll of Shopping While Black*, THE ESTABLISHMENT (June 10, 2016), https://theestablishment.co/the-emotional-toll-of-shopping-while-black-bcda5e51a7fd#.i0ejh5mx3 [https://perma.cc/VS52-YES7].

201. *See* Kasai Rex, *Fear and the Gun Lobby*, GOOD (Mar. 9, 2015), http://magazine.good.is/articles/nra-racism-fear-gun-control [https://perma.cc/SB52-8RVZ] ("Yes, our police on overdrive are symptomatic of a violent, gun-obsessed culture. Yet, as a black male, I have as much reason to fret over being shot dead just for walking on someone's porch to ask for help . . . as I do getting the wrong cop on a routine traffic stop.").

saulted or killed by a violent white citizen.[202] Similarly, little attention is paid to the inhibiting effects of harassment of women, both online[203] and offline,[204] despite evidence that such harassment forces women to change everything from their paths to work to their clothing choices to their intimate relationship choices, to say nothing of the fact that many women and girls simply withdraw from political participation, from jobs, and from social media in response to surveillance by private individuals ranging from violent intimate partners to online mobs.[205]

IV. INTERSECTIONAL SURVEILLANCE

Attentiveness to race, class, and gender is vital to understanding the true scope of the surveillance threat. Marginalized populations, especially those who experience the intersection of multiple forms of subordination, also often find themselves at the intersection of multiple forms of surveillance: high-tech and low-tech, virtual and physical. That is, to return to Crenshaw's analogy of a woman being hit by several vehicles at an intersection,[206] the vehicles can represent not only various categories of identity but various categories of surveillance. The contemporary populist privacy narrative, in general, tends to overlook both Crenshaw's intersectionality of identities and the intersectionality of varying forms of surveillance. The following case studies are examples of surveillance intersectionality that have affected marginalized individuals.

A. Case Study on the Surveillance of Black Bodies: Florence v. Burlington

In 2012, the Supreme Court decided an important Fourth Amendment case, *United States v. Jones*, holding that the govern-

---

202. *See* Christian Nwachukwu Jr. & Dana Forde, *Not a Threat, but Threatened*, AL JAZEERA AM. (Feb. 26, 2014), http://america.aljazeera.com/features/2014/2/young-black-men-intheageoftrayvonandjordan.html [https://perma.cc/C7YY-2QST].

203. *See* Marlisse Silver Sweeney, *What the Law Can (and Can't) Do About Online Harassment*, THE ATLANTIC (Nov. 12, 2014), http://www.theatlantic.com/technology/archive/2014/11/what-the-law-can-and-cant-do-about-online-harassment/382638/ [https://perma.cc/B2ZQ-UEQM].

204. *See* The Advocates for Human Rights, *Prevalence of Street Harassment and Its Consequences*, STOP VIOLENCE AGAINST WOMEN (Aug. 2, 2013), http://www.stopvaw.org/prevalence_street_harassment [https://perma.cc/6EHA-V6WS]; *Statistics — The Prevalence of Street Harassment*, STOP STREET HARASSMENT, http://www.stopstreetharassment.org/resources/statistics/statistics-academic-studies/ [https://perma.cc/8H7D-NUL6].

205. *See, e.g.*, Amanda Hess, *Why Women Aren't Welcome on the Internet*, PAC. STANDARD (Jan. 6. 2014), http://www.psmag.com/health-and-behavior/women-arent-welcome-internet-72170 [https://perma.cc/3EWE-K734].

206. *See* Crenshaw, *supra* note 121, at 149.

ment's attachment of a GPS device to a vehicle for purposes of tracking its driver was an unconstitutional search.[207] This case received a great amount of attention not only from scholars but also from the media and the general public. Another important Fourth Amendment case decided that year, *Florence v. Burlington*,[208] received far less attention.[209] This latter case found that suspicion-less strip searches of individuals placed into the general prison population did not violate the Fourth Amendment.[210] The differing outcomes as well as the differing public interest in these two cases are telling. The first involved the use of technology to monitor a vehicle; the second involved the physical stripping and inspection of a human body. Both the Court and the general public seem to consider the former conduct far more alarming than the latter; this is likely due in part to the fact that while the former implicates the interests of the middle and upper class, the latter is most likely to affect racial minorities and the poor.

It has been suggested that the ruling in *Jones* turned in no small part on this exchange between the Chief Justice and Deputy Solicitor General Michael Dreeben:

> CHIEF JUSTICE ROBERTS: You think there would also not be a search if you put a GPS device on all of our cars, monitored our movements for a month? You think you're entitled to do that under your theory?
>
> MR. DREEBEN: The Justices of this Court?
>
> CHIEF JUSTICE ROBERTS: Yes. (Laughter.)
>
> . . .
>
> CHIEF JUSTICE ROBERTS: So, your answer is yes, you could tomorrow decide that you put a GPS device on every one of our cars, follow us for a month; no problem under the Constitution?[211]

The Justices were confronted in this case by state action that they could easily contemplate being used to affect their own personal pri-

---

207. *See* United States v. Jones, 565 U.S. 400, 400 (2012).

208. Florence v. Burlington, 566 U.S. 318 (2012).

209. *See* Sklansky, *supra* note 129, 1103–05.

210. *See Florence*, 566 U.S. at 318.

211. Transcript of Oral Argument at 9–10, United States v. Jones, 565 U.S. 400 (2012) (No. 10 1259), http://www.supremecourt.gov/oral_arguments/argument_transcripts/10-1259.pdf [https://perma.cc/56CZ-R722].

vacy. This is not the first time the Court has shown selective empathy in Fourth Amendment cases,[212] but it is a particularly poignant example when considered in juxtaposition to *Florence*.

Albert Florence, an African-American man, was wrongfully arrested on the basis of an outdated warrant.[213] Before the error was discovered, he was detained for six days at two correctional facilities, where he was subjected to an invasive strip search that involved squatting naked in front of officers and coughing to demonstrate that he was not hiding any weapons or contraband inside his orifices.[214] Seven years before the wrongful arrest, Florence had driven away from a traffic stop and for this had been charged with obstruction of justice and use of a deadly weapon (the vehicle).[215] He was fined $1500 in exchange for a guilty plea to lesser charges, and at some point fell behind in payment.[216] After failing to appear at an enforcement hearing, a bench warrant was issued for his arrest.[217] Florence paid the balance less than a week later.[218] As a precaution, Florence, a finance manager for a car dealership, kept a certified document stating that he had paid the fine in the glove department of his BMW: "Just in case that situation was to come up, I had that document."[219] Two years later, as he was on the way to dinner with his pregnant wife, April, and their four-year-old son to celebrate their purchase of a home, the Florences' vehicle was pulled over by a state trooper.[220] April was driving, but when the trooper ran a check on Florence as the owner of the vehicle, he came across the warrant. Florence produced the document from the glove compartment, but the trooper said "he had to go by what was in the computer."[221]

Florence was first taken to Burlington County Detention Center, where he was held for six days.[222] Intake procedures at Burlington included showering with a delousing agent while officers check ar-

---

212. *See* Tamara Rice Lave, *Protecting Elites: An Alternative Take on How* United States v. Jones *Fits into the Court's Technology Jurisprudence*, 14 N.C. J.L. & TECH. 461, 462–63 (2013).

213. *See Florence*, 566 U.S. at 323.

214. *See id.* at 323–24.

215. *Id.* at 323.

216. *See* Robert Barnes, *Supreme Court Is Asked About Jails' Blanket Strip-Search Policies*, WASH. POST (Sept. 12, 2011), http://www.washingtonpost.com/politics/supreme-court-is-asked-about-jails-blanket-strip-search-policies/2011/09/09/gIQAuc6vNK_story.html [https://perma.cc/7ZET-2J52].

217. *Florence*, 566 U.S. at 323.

218. *Id.*

219. Barnes, *supra* note 216.

220. *See id.*; Angela J. Davis, *Supreme Court's Disconcerting Opinion Supporting Jailhouse Strip-Searches*, AM. CONST. SOC'Y: ACSBLOG (Apr. 5, 2012), http://www.acslaw.org/acsblog/all/florence-v.-burlington [https://perma.cc/BF78-7G5U].

221. Barnes, *supra* note 216.

222. *Florence*, 566 U.S. at 323.

restees' bodies for contraband, tattoos, and scars.[223] Florence was also "instructed to open his mouth, lift his tongue, hold out his arms, turn around, and lift his genitals."[224] Florence was then transferred to the Essex County Correctional Facility, whose intake procedures for all arriving detainees include passing through a metal detector and waiting in a group holding cell for further search.[225] During that further search, "they were instructed to remove their clothing while an officer looked for body markings, wounds, and contraband. . . . [A]n officer looked at their ears, nose, mouth, hair, scalp, fingers, hands, arms, armpits, and other body openings."[226] According to Florence, "he was required to lift his genitals, turn around, and cough in a squatting position as part of the process."[227] These procedures were imposed "regardless of the circumstances of the arrest, the suspected offense, or the detainee's behavior, demeanor, or criminal history."[228] Florence brought a Section 1983 claim[229] alleging violations of his Fourth and Fourteenth Amendment rights. He argued that the invasive strip search procedures should be required only when there is individualized suspicion that the arrestee might be concealing contraband.[230]

Justice Kennedy, writing for the majority, disagreed: "[C]ourts must defer to the judgment of correctional officials" with regard to the appropriateness of intake procedures "unless the record contains substantial evidence showing their policies are an unnecessary or unjustified response to problems of jail security."[231] In arriving at this conclusion, Justice Kennedy referred to the fact that ten thousand assaults on corrections staff occur each year and noted several incidents of inmates smuggling contraband or weapons.[232] However, as Justice Breyer noted in dissent, the total number of assaults on corrections staff hardly sheds light on the question of the necessity or even usefulness of invasive strip searches of arrestees, especially when there is no reason to suspect that they are carrying contraband.[233] The total number of assaults on staff presumably includes assaults by the entire inmate population, not just arrestees, as well as by other staff members. The reference to assaults moreover does not indicate whether contraband played any role in such assaults. In determining whether suspicion-less invasive searches of arrestees for contraband are neces-

223. *Id.*
224. *Id.*
225. *Id.* at 324.
226. *Id.*
227. *Id.*
228. *Id.*
229. A Section 1983 claim is a civil claim brought by a citizen against a state actor for violation of constitutional rights. 42 U.S.C. § 1983 (2012).
230. *Florence*, 566 U.S. at 324.
231. *Id.* at 322–23.
232. *Id.* at 333.
233. *Id.* at 352–53 (Breyer, J., dissenting).

sary or even advisable, the relevant information should instead be the number of assaults committed by arrestees using contraband and who did not present any individualized suspicion of possessing contraband. Justice Breyer cited an Orange County study that found one successful suspicion-less search out of twenty-three thousand searches.[234]

Albert Florence's case is a study in intersectional surveillance targeted at a marginalized member of society: as a black man, Florence was vulnerable to racial profiling by law enforcement. Florence was so acutely aware of this vulnerability that he made sure to keep a physical copy of proof that he had paid his previous fines in the vehicle his wife was driving. While the exact circumstances of the traffic stop are unclear, it is possible that the couple's race was a factor in the trooper's decision to pull them over in the first place. The erroneous database record was a form of data surveillance, which was compounded by the trooper's insistence that "he had to go by what was in the computer."[235]

Why did the Supreme Court respond so differently to the attachment of a GPS device to a suspected drug dealer's vehicle, parked in a public area, as opposed to the forced stripping and intimate bodily inspection of a man wrongfully arrested due to a computer error? The answer may have to do with the Court's inability or unwillingness to acknowledge the intersectionality of Florence's situation. As indicated by the Chief Justice's pointed questioning in *Jones*, GPS tracking of one's vehicle is clearly the kind of violation the Justices could imagine themselves experiencing, whereas they may have had a harder time contemplating the possibility of being an arrestee subjected to an invasive strip search before being admitted into the general population of a jail. As attorney John W. Whitehead observed in the *Huffington Post*,

> I doubt that Anthony M. Kennedy, John G. Roberts Jr., Antonin Scalia, Clarence Thomas and Samuel A. Alito Jr. — the five justices who seemed to have no trouble inflicting such humiliations on the populace — would be inclined to condone such dehumanizing treatment were there even the slightest possibility that they might be subjected to it. It is a testament to the elitist mindset that prevails in our judicial system today that these five men can rest easy knowing that they will never be subjected to any such violation of their persons. It is only average Americans — the so-called "great unwashed mass-

234. *Id.* at 349.
235. Barnes, *supra* note 216.

> es" — who will have to worry about being subjected to this state-sanctioned brand of humiliation and bodily violation.[236]

It may be, as Professor Tamara Rice Lave suggests, that the Supreme Court's Fourth Amendment jurisprudence "can be best understood as reaching resolutions that best protect the interests of elites,"[237] and that cases that do not seem to impact those interests simply do not merit the same kind of consideration.

It is not only the Supreme Court that is more interested in the privacy implications of GPS tracking than those of invasive strip searches. A July 2016 search of Westlaw's "Law Reviews and Journals" database of the case citation for *U.S. v. Jones* yields over a thousand results; a search for the case citation for *Florence v. Burlington* yields 13 results. A search for "U.S. v. Jones" and "GPS"[238] in Westlaw's "News" database yields 239 results; a search for "Florence v. Burlington" yields 14 results. The legal academy and the general public seem to share in the Supreme Court's privacy hierarchy.

B. Case Study on the Surveillance of Poor Bodies: U.S. v. Pineda-Moreno

The Supreme Court had the opportunity to take up a different GPS tracking case in its 2012 term: one that, on its face, seemed to present an even more serious violation of the Fourth Amendment protection against unreasonable searches than *Jones*. That case was *United States v. Pineda-Moreno*, from the Ninth Circuit.[239] In 2007, Juan Pineda-Moreno came under suspicion of engaging in drug activities by the Drug Enforcement Administration ("DEA").[240] As part of their investigation, the agents installed mobile tracking devices on Pineda-Moreno's Jeep on several occasions, often while the vehicle was parked in a public area.[241] Twice, however, the agents installed the device in the early hours of the morning while the Jeep was parked in the driveway of Pineda-Moreno's trailer home.[242] These devices gathered detailed information about the vehicle's movements, including one occasion in which the information indicated that the vehicle was

---

236. John W. Whitehead, *Strip-Searching America:* Florence v. County of Burlington, HUFFINGTON POST (April 4, 2012, 11:12 AM), http://www.huffingtonpost.com/john-w-whitehead/supreme-court-strip-searches_b_1401063.html [https://perma.cc/DMH9-7PV2].

237. *See* Lave, *supra* note 212, at 467.

238. To distinguish the 2012 Supreme Court case from other cases involving parties named Jones.

239. *See* United States v. Pineda-Moreno, 591 F.3d 1212 (9th Cir. 2010).

240. *See id.*

241. *See id.* at 1213.

242. *See id.*

departing a site where the agents believed marijuana was grown.[243] When agents pulled over Pineda-Moreno's Jeep, they claimed to have smelled marijuana on a passenger in the back seat.[244] The three occupants of the vehicle were arrested for immigration violations.[245] Pineda-Moreno consented to the search of his vehicle and his home, where marijuana was discovered.[246] Pineda-Moreno moved to suppress the information obtained by the tracking devices as the fruit of an unconstitutional search — namely, the attachment of the tracking device to his vehicle while the vehicle was parked within the curtilage of his home.[247] In an illustration of Slobogin's "poverty exception," a panel of judges on the Ninth Circuit found that Pineda-Moreno had no reasonable expectation of privacy in his driveway because he "did not take steps to exclude passersby" from it.[248] Pineda-Moreno petitioned for a rehearing en banc, which was denied.[249]

Judge Kozinski, then Chief Judge of the Ninth Circuit, wrote a blistering dissent from the denial of rehearing en banc.[250] Judge Kozinski opined that the panel's decision effectively "spells the end of Fourth Amendment protections for most people's curtilage" — and by most people, he meant those unable to afford the protections of gated communities and sophisticated security systems.[251] Judge Kozinski condemned what he perceived to be elitism infecting the court's reasoning, which he attributed to the lack of genuine class diversity in the judiciary generally:

> Poor people are entitled to privacy, even if they can't afford all the gadgets of the wealthy for ensuring it. . . . When you glide your BMW into your underground garage or behind an electric gate, you don't need to worry that somebody might attach a tracking device to it while you sleep. But the Constitution doesn't prefer the rich over the poor; the man who parks his car next to his trailer is entitled to the same privacy and peace of mind as the man whose urban fortress is guarded by the Bel Air Patrol. The panel's breezy opinion is troubling on a number of grounds,

243. *See id.* at 1214.
244. *See id.*
245. *See id.*
246. *See id.*
247. *See id.*
248. *See id.* at 1214–15.
249. *See* United States v. Pineda-Moreno, 617 F.3d 1120, 1121 (9th Cir. 2010), *cert. denied*, 617 F.3d 1120 (9th Cir. 2010).
250. *See id.* at 1121 (Kozinski, J., dissenting).
251. *See id.* at 1123.

> not least among them its unselfconscious cultural elitism.[252]

With his case on remand in light of *Jones*, Pineda-Moreno still received no relief. The panel found that the officers had acted on "then-binding circuit precedent."[253] The Supreme Court, by taking on *Jones* instead of *Pineda-Moreno*, passed up an opportunity to directly address the issues regarding economic privilege raised by Judge Kozinski.[254]

Pineda-Moreno's low-income status made him vulnerable to a wide range of privacy invasions. As Judge Kozinski detailed, people who live in trailer homes are already at the mercy of nosy neighbors, curious children, and scavenging animals in ways that people who live in more glamorous housing are not. The panel used this very vulnerability against Pineda-Moreno, in effect arguing that people who cannot afford to protect their privacy from the general public cannot complain when the state violates that privacy as well. Pineda-Moreno's story is one of a vulnerable member of society targeted by both low-tech (trespass and in-person tracking) and high-tech (GPS monitoring) surveillance.

C. Case Study on the Surveillance of Female Bodies: United States v. Petrovic[255]

Jovica Petrovic and M.B. began a relationship in 2006 and were married in 2009.[256] During their relationship, M.B. allowed Petrovic to take sexually explicit photographs of her.[257] M.B. also confided in Petrovic about the sexual abuse she had experienced as a child, her struggle with suicidal thoughts, and her fears about her fitness as a mother.[258] M.B. attempted suicide by slitting her wrists in Petrovic's home after she discovered that he had been having an affair and had impregnated his mistress.[259] Petrovic took pictures of the pool of blood on the floor left by the attempt after M.B. was taken to the hospital.[260] On several occasions, Petrovic secretly filmed M.B. when they were having sex.[261] After M.B. informed Petrovic that she was

---

252. *See id.*

253. *See* United States v. Pineda-Moreno, 688 F.3d 1087, 1091 (9th Cir. 2012).

254. *Cf.* Lave, *supra* note 212, at 463.

255. *See* United States v. Petrovic, 701 F.3d 849 (8th Cir. 2012).

256. *Id.* at 852.

257. *See id.* at 852.

258. Nicholas Phillips, *Sext Fiend*, RIVERFRONT TIMES (Apr. 18, 2013), http://www.riverfronttimes.com/2013-04-18/news/sext-fiend/ [https://perma.cc/4QL3-AWU7].

259. *See id.*

260. *See id.*

261. *See id.*

leaving him in December of 2009, Petrovic told her about these secret recordings and that he had also saved all of her text messages to him.[262] Petrovic threatened to publish this information online if M.B. did not agree to stay in the relationship.[263]

After M.B. failed to acquiesce, Petrovic began an intense campaign of harassment and abuse against M.B.[264] He mailed dozens of postcards to people in M.B.'s community, including her family members, co-workers, and local businesses that featured a barely-dressed M.B. accompanied by epithets such as "whore."[265] The postcards directed recipients to a website that Petrovic had created, where he offered twenty to thirty thousand pages of material about M.B., includ-including links to dozens of images and videos of M.B. naked and engaged in sex acts.[266] Petrovic included links to pictures of M.B.'s children (not fathered by Petrovic) as well as M.B.'s intimate text messages, the picture of the pool of blood left by M.B.'s suicide attempt, as well as M.B.'s contact information and the social security numbers of her children.[267] Petrovic also sent several packages containing enlarged photographs of M.B. engaged in sexual acts to M.B.'s employer and family members.[268] One of these packages was opened and viewed by M.B.'s seven-year-old son.[269] Petrovic was convicted of four counts of interstate stalking and two counts of interstate extortionate threat.[270]

The *Petrovic* case is in many respects not unusual. As discussed above, technology is a force multiplier for domestic abuse, enabling abusers to exert unprecedented levels of control over their targets and to crowdsource their surveillance campaigns.[271] The case illustrates how the greatest threat to privacy and security for women is more likely to be former partners or acquaintances than the government. Keylogging software allows abusers to see everything their targets type into a search engine or email;[272] GPS trackers lets abusers know where their targets are at all hours of the day;[273] and an entire sexual humiliation industry has sprung up online fed by embittered exes and

---

262. *See Petrovic*, 701 F.3d at 852.
263. *Id.*
264. *See id.* at 853
265. *See id.*
266. *See id.*
267. *See id.*
268. *See id.*
269. *See id.*
270. *See id.* at 849.
271. *See Technology Abuse: Experiences of Survivors and Victim Service Agencies*, NATIONAL NETWORK TO END DOMESTIC VIOLENCE (Apr. 29, 2014), http://nnedv.org/news/4272-new-survey-technology-abuse-experiences-of-survivors-and-victim-service-agencie.html [https://perma.cc/JE5Z-N9HN].
272. *See* Shahani, *supra* note 115.
273. *See id.*

misogynist consumers.[274] What is unusual about the *Petrovic* case is that the abuser was actually apprehended and punished. Victims fear retaliation and escalation from their abusers, and the threat of sexual exposure in the practice commonly referred to as "revenge porn" ensures that many victims will never reach out for help. Perpetrators have incentives to engage in this conduct — whether a desire for vengeance, social status, or profit — and little incentive to refrain because disclosing private sexual imagery without consent at the time of this case was not yet a crime in the majority of U.S. states.[275]

M.B.'s gender made her uniquely vulnerable to multiple forms of intimate surveillance, both low-tech and high-tech. Petrovic engaged in in-person stalking of M.B. as well as secretly filming the two having sex and using both electronic communications and the mail to distribute the footage, putting M.B. in fear for her physical safety and wreaking havoc on her professional and personal life. Though M.B. was able to obtain some justice in her case, the majority of women subjected to multiple forms of intimate surveillance have had little or no recourse.

V. CAUTIONARY TALES

The foregoing case studies highlight the way marginalized individuals experience multiple, insidious layers of surveillance. They are the kinds of cases that should be, but are not, receiving widespread public attention. They are the kinds of cases that should be, but are not, inspiring calls for legal and political change. Instead, they are relegated to the margins, while the experiences of elite and mainstream society dominate the political and cultural conversation about privacy and surveillance. The failure to pay adequate attention to the way surveillance practices are shaped by race, class, and gender does more than divert social attention away from cases like these; it also distorts our fundamental understanding of privacy. This distortion undermines even well-intentioned efforts to address social problems. When the theory of privacy is incomplete or flawed, so will be the practice. This Part offers two illustrations of how an underdeveloped, elitist, interest-convergence approach to privacy and surveillance can cause serious harm.

---

274. *See* Jill Filipovic, *Revenge Porn is About Degrading Women*, THE GUARDIAN (Jan. 28, 2013, 17:23 EST), https://www.theguardian.com/commentisfree/2013/jan/28/revenge-porn-degrades-women [https://perma.cc/5VPR-797D].

275. *See* Mary Anne Franks, *The ACLU's Frat House Take on Revenge Porn*, HUFFINGTON POST (Apr. 1, 2015), http://www.huffingtonpost.com/mary-anne-franks/the-aclus-frat-house-take_b_6980146.html [https://perma.cc/K75W-TG7W].

A. Police Body Cameras

Longtime concerns over police misconduct and brutality, especially against racial minorities, reached a peak in the summer of 2014, following the shooting of an unarmed teenager named Michael Brown by a police officer in Ferguson, Missouri.[276] The killing led to numerous protests and sparked a national conversation about racism and violence in law enforcement.[277] The death of Brown was followed by a series of other deaths, mostly of young black men, during police confrontations or in police custody.[278] The public outcry was reflected in the social media hashtag #BlackLivesMatter, which quickly became a social movement, engendering organized demonstrations, civil rights investigations, institutional research, and political interventions.[279]

One of the reforms that activists have frequently and loudly called for, and municipalities have increasingly implemented, is mandatory body cameras for police.[280] Proponents argue that such cameras are an essential tool for reducing police misconduct and brutality, with some even arguing that they are the only tool that can save racial minorities from police violence.[281] Many lawmakers and politicians have called for mandatory body cameras for police,[282] including Hillary Clinton.[283] In May 2015, the Obama administration announced that it

---

276. *See Ferguson Unrest: From Shooting to Nationwide Protests*, BBC (Aug. 10. 2015), http://www.bbc.com/news/world-us-canada-30193354 [https://perma.cc/H7CW-Z9G6].

277. *See id.*

278. *See* Daniel Funke and Tina Susman, *From Ferguson to Baton Rouge: Deaths of Black Men and Women at the Hands of Police*, L.A. TIMES (July 12, 2016), http://www.latimes.com/nation/la-na-police-deaths-20160707-snap-htmlstory.html [https://perma.cc/6FFQ-XVT].

279. *See* Josh Hafner, *How Michael Brown's Death, Two Years Ago, Pushed #BlackLivesMatter into a Movement*, USA TODAY (Aug. 8, 2016), http://www.usatoday.com/story/news/nation-now/2016/08/08/how-michael-browns-death-two-years-ago-pushed-blacklivesmatter-into-movement/88424366/ [https://perma.cc/S6XM-D6EU]; Jay Caspian Kang, *Our Demand is Simple: Stop Killing Us*, N.Y. TIMES (May 4, 2015), http://www.nytimes.com/2015/05/10/magazine/our-demand-is-simple-stop-killing-us.html?_r=0 [https://perma.cc/DL5Q-ACCE].

280. *See* Mary D. Fan, *Privacy, Public Disclosure, Police Body Cameras: Policy Splits*, 68 ALA. L. REV. 395, 408–09 (2016).

281. *See* Nick Gillespie, *Make Cops Wear Cameras*, TIME (Aug. 14, 2014), http://time.com/3111377/ferguson-police-cameras/ [https://perma.cc/JL85-KNVQ]; James S. Muller, *To Police the Police, Body Cameras are a Must*, L.A. TIMES (May 11, 2015), http://www.latimes.com/opinion/op-ed/la-oe-muller-body-camera-data-shows-unnecessary-force-20150508-story.html [https://perma.cc/T4UY-8YD2].

282. *See* Kels Dayton & Bob Wilson, *Lawmakers Vote to Spend $15 Million on Body Cameras*, WTNH.COM (June 29, 2015), http://wtnh.com/2015/06/29/lawmakers-vote-to-spend-15-million-on-body-cameras/ [https://perma.cc/4WWC-CNTN]; Dennis Romboy, *Utah Lawmakers, Police Closer to Statewide Body Camera Rules*, DESERET NEWS (Aug. 19, 2015), http://www.deseretnews.com/article/865634886/Utah-lawmakers-police-closer-to-statewide-body-camera-rules.html?pg=all [https://perma.cc/DV8Y-UA9W].

283. *See* Emily Schultheis, *Hillary Clinton Calls for Body Cameras for All Police Officers Nationwide*, NATIONAL JOURNAL (April 29, 2015), http://www.nationaljournal.com/

would be providing $20 million to police departments for body cameras.[284]

There are many compelling arguments in favor of mandatory police body cameras.[285] When a confrontation between a police officer and a civilian results in the death of the latter, it can be very difficult to determine what transpired before the use of deadly force. It is not uncommon for police officers to lie about their encounters, and even honest police officers may misremember events or fail to recognize the role implicit biases[286] may have played in their actions. Without video evidence, it is likely that many cases of police brutality would never have come to light.[287] Some studies have suggested that the use of body cameras greatly reduces the use of force in police encounters and the number of complaints lodged against police.[288]

However, there are many reasons to be cautious about the use of police body cameras as well.[289] Much of the video footage that proved crucial to spotlighting instances of police brutality was shot by civilians on cellphones or other devices, not by police cameras.[290] There are questions about how police officers can manipulate the technology, from selectively turning cameras on and off to deceptively editing, mishandling, or losing the footage. There are also serious issues to be raised about the belief in the objectivity of video footage, especially as research has shown that it is possible for two people to view the

---

2016-elections/hillary-clinton-calls-for-body-cameras-for-all-police-officers-nationwide-20150429 [https://perma.cc/MZ7G-6BQ5].

284. *See* David Jackson, *Obama Team Will Fund Police Body Camera Project*, USA TODAY (May 1, 2015), http://www.usatoday.com/story/news/nation/2015/05/01/obama-police-body-cameras-josh-earnest-baltimore/26696517/ [https://perma.cc/KF5A-8SCS].

285. *See* MARC JONATHAN BLITZ, AM. CONSTITUTION SOC'Y FOR LAW AND POLICY, POLICE BODY-WORN CAMERAS: EVIDENTIARY BENEFITS AND PRIVACY THREATS 5–7 (2015).

286. *See* L. Song Richardson, *Arrest Efficiency and the Fourth Amendment*, 95 MINN. L. REV. 2035, 2039 (2011) ("The science of implicit social cognition demonstrates that individuals of all races have implicit biases in the form of stereotypes and prejudices that can negatively and nonconsciously affect behavior towards blacks.").

287. For example, that Officer Michael Slager shot Walter Scott in the back as he ran away. *See* Mark Berman, *South Carolina Police Officer in Walter Scott Shooting Indicted on Murder Charge*, WASH. POST (June 8, 2015), http://www.washingtonpost.com/news/post-nation/wp/2015/06/08/police-officer-who-shot-walter-scott-indicted-for-murder/ [https://perma.cc/2N2P-MH5D].

288. *See* Fan, *supra* note 280, at 410–11; Alexandra Mateescu et al., *Police Body-Worn Cameras* (Data & Soc'y Research Inst., Working Paper, 2015).

289. *See Developments in the Law — Policing*, 128 HARV. L. REV. 1794, 1796 (2015) ("[B]ody cameras are a powerful — and indiscriminate — technology. Their proliferation over the next decade will inevitably change the nature of policing in unexpected ways, quite possibly to the detriment of the citizens the cameras are intended to protect.") [hereinafter *Developments*].

290. *See* Mike Ludwig, *Body Cameras Are Not Pointed at the Police: They're Pointed At You*, TRUTHOUT (May 24, 2015), http://www.truth-out.org/news/item/30940-body-cameras-are-not-pointed-at-the-police-they-re-pointed-at-you [https://perma.cc/KW9Q-GU24] ("'It's bystander and civilian video, along with popular uprisings, that brought the issue of police brutality and murder to the national stage — not police body cameras.'").

same video evidence and arrive at completely different conclusions about what transpired.[291] Some studies have shown that police use of force actually increased following the implementation of body cameras.[292]

With regard to the concerns of this Article, there is yet another reason to hesitate, which has to do with the privacy and surveillance implications of mandatory police body cameras. Many well-meaning lawmakers, activists, and members of the general public do not seem particularly attentive to the fact that no matter how benign or socially useful, police cameras are a powerful form of surveillance that have the potential to jeopardize the privacy of individuals at their most vulnerable. As noted in a 2015 *Harvard Law Review* article, "although police body cameras have the potential to benefit citizens and officers alike, they nevertheless represent another substantial step toward a surveillance state."[293] As Wade Henderson, CEO of the Leadership Conference on Civil and Human Rights, put it in a Senate subcommittee hearing on police body cameras: "[B]ody-worn cameras won't be operated by concerned citizens and won't be recording officers. They will instead be directed at members of the community."[294] Henderson went on to warn that:

> body cameras would exacerbate the dramatic disparities in how different communities are policed, if the technology becomes a 'multiuse surveillance tool' for law enforcement. . . . [F]acial recognition and other biometric technologies, along with body cameras, . . . would give law enforcement unprecedented abilities to peer into heavily policed neighborhoods,

---

291. *See* BLITZ, *supra* note 285, at 7–8; Dan M. Kahan et al., *Whose Eyes Are You Going to Believe?* Scott v. Harris *and the Perils of Cognitive Illiberalism*, 122 HARV. L. REV. 838, 841 (2009); Mateescu et al., *supra* note 288, at 26 ("Existing biases can . . . manifest in interpretation of body-worn camera footage. Various studies have highlighted the biases that shape people's judgments and how interpersonal interactions can draw on conscious and unconscious stereotypes.").

292. *See* Jacob Gershman, *Study Links Police Bodycams to Increase in Shooting Deaths*, WALL ST. J. (Aug. 12, 2016), http://blogs.wsj.com/law/2016/08/12/study-links-police-bodycams-to-increase-in-shooting-deaths/ [https://perma.cc/CY3T-7G38]; Chris Martin, *San Diego Police Are Using Body Cameras But Their Impact on Police Force May Not Be As Expected*, INDEPENDENT JOURNAL REVIEW (Sept. 2015), http://ijr.com/2015/09/424065-san-diego-police-using-body-cameras-devices-curbing-use-force-cops-city/ [https://perma.cc/7JZE-WF2R] ("Interdepartmental research shows that during that 12-month period when body cameras were in use, instances of some types of force by San Diego police officers actually rose by 10%.").

293. *See Developments*, *supra* note 289, at 1811.

294. Ludwig, *supra* note 290.

> where stationary surveillance cameras are already abundant.[295]

As the discussion above detailed, black bodies, poor bodies, and female bodies have historically been disproportionately subjected to surveillance, often in the service of law enforcement or other forms of state monitoring. Black men, especially poor black men, are overrepresented in the criminal justice system, from racial profiling to investigations, convictions to probation. Always-on recording capacity in law enforcement will create opportunities to intimidate vulnerable communities who fear interaction with police even if they are engaged in no wrongdoing. As noted in a February 2015 Working Paper by the Data & Society Research Institute, police departments have significant discretion when deciding how, when, and whom to record,[296] and this discretion can easily be used in a discriminatory fashion. There is good reason to fear that the injustices that underpin the criminal justice system will only be replicated and amplified by technology.[297] There are also serious privacy questions to be considered regarding the consent of the civilians being recorded, who can access the footage, how the footage will be stored, and how the footage will be used.[298] One police chief in Washington, concerned that the state's public records law would force him to disclose footage from body cameras, decided not to purchase body cameras for his officers.[299] "Our view is we don't want to be part of violating people's privacy for commercial or voyeuristic reasons. Everyone's worst day is now going to be put on YouTube for eternity."[300]

The concern about voyeurism is underscored by the fact that at least some police officers are more than happy to use technology to boast of their racism, their use of force, or to simply express their contempt for civilians. In March 2015, the FBI opened an investigation into four Fort Lauderdale police officers who shared a mock movie trailer, created by one of the officers, that used racial slurs, "showed a dog attacking a black man[,] . . . depicted President Obama with gold

---

295. *Id.*

296. *See* Mateescu et al., *supra* note 288, at 9–11.

297. *See* Ludwig, *supra* note 290 ("Malkia Cyril, a prominent civil rights activist and director of the Center for Media Justice, said body cameras are no substitute for the kind of comprehensive reforms needed to curb police violence and hold cops accountable. 'Police body cameras are an unproven technology to collect evidence . . . . But this technology can't be relied upon to ensure police accountability that we, as a nation, have failed to implement.'").

298. *See* Mateescu et al., *supra* note 288, at 9–11.

299. Timothy Williams, *Downside of Police Body Cameras: Your Arrest Hits YouTube*, N.Y. TIMES (Apr. 26, 2015), http://www.nytimes.com/2015/04/27/us/downside-of-police-body-cameras-your-arrest-hits-youtube.html?_r=0 [https://perma.cc/EPM7-DXQ6].

300. *Id.*

teeth and included Ku Klux Klan imagery."[301] In May 2015, a photo surfaced of two rifle-bearing Chicago police officers posing with a black suspect on whose head they had placed deer antlers.[302] In August 2015, the *Washington Post* reported that the Sergeants Benevolent Association in New York had begun posting photographs of "signs of disorder" to Flickr, a photo-sharing site: "The cumulative effect makes it look a lot like the police, if they can't clean up the homeless, are mocking them instead. . . . The images, scrolling down for several pages, zoom in on New Yorkers at their worst moments and when they're most vulnerable."[303] One commentator, reflecting on the routine exposure to graphic footage of the deaths of black men at the hands of police, cautions:

> Yes, we should celebrate that even though an unarmed black man was killed, his killing was caught on film, so there's a better shot at justice and closure. But I'm trying desperately to make sense of why watching and sharing the video that tore his mother's heart to pieces is as normal as making your latest Instagram post. . . . In a world where we are inundated with explicit content, watching black men die on camera provides a thrill that America thought she lost when popular lynchings ended.[304]

Adding to the gravity of these concerns is the lack of attention paid to the prevalence of sexism and gendered violence in law enforcement. U.S. law enforcement is a hyper-masculine institution, heavily dominated by men and by rigid gender stereotypes.[305] Studies indicate that the families of police officers are two to four times more

---

301. Caitlin MacNeal, *FBI Looking into Florida Cops Tied to Racist Video Depiction of Obama*, TALKING POINTS MEMO (Mar. 23, 2015), http://talkingpointsmemo.com/livewire/fort-lauderdale-police-racist-messages [https://perma.cc/QXX6-WVNQ].

302. Travis Gettys, *Photo Shows Rifle-Toting Chicago Cops Posing with a Black Drug Suspect Like a Hunting Trophy*, RAW STORY (May 27, 2015), http://www.rawstory.com/2015/05/photo-shows-rifle-toting-chicago-cops-posing-with-a-black-drug-suspect-like-a-hunting-trophy/ [https://perma.cc/24UR-888G].

303. Emily Badger, *Police Are Posting Photos Online of New Yorkers at Their Most Vulnerable*, WASH. POST (Aug. 13, 2015), http://www.washingtonpost.com/news/wonkblog/wp/2015/08/13/police-are-posting-photos-online-of-new-yorkers-at-their-most-vulnerable/ [https://perma.cc/2CKQ-FLYS].

304. Jade E. Davis, *Black Men Being Killed is the New Girls Gone Wild*, MEDIUM (Apr. 10, 2015), https://medium.com/matter/black-men-being-killed-is-the-new-girls-gone-wild-da5c150b70c4 [https://perma.cc/8Z6M-LLKN].

305. *See* Mary Anne Case, *Police Mistakes in Ferguson Involve Gender as Well as Race*, HUFFINGTON POST (Sept. 11, 2014), http://www.huffingtonpost.com/mary-anne-case/police-mistakes-in-fergus_b_5793494.html [https://perma.cc/YBH9-6KQ6].

likely to experience domestic violence than the general population.[306] The second most-reported form of police misconduct, after the use of excessive force, is sexual assault: "[S]exual assault rates are significantly higher for police when compared to the general population."[307] There is good reason to be concerned about how misogynist law enforcement officers will use surveillance tools against women, especially for the purpose of sexual exploitation. One particularly horrific illustration of police sexual assault came to light in 2014, when Oklahoma City police officer Daniel Holtzclaw was charged with sexually assaulting 13 women while on duty.[308] Holtzclaw "forced women whom he had threatened to arrest or physically harm to perform various sex acts while he was on patrol. The females ranged in age from 17 to 58 and included a 57-year-old grandmother who was allegedly forced to perform oral sex on him."[309]

In January 2015, it was reported that Oklahoma City Police Department would begin a one-hundred-camera pilot program.[310] The mainstream media did not question whether the issue of sexual assault by police officers might complicate the endorsement of police body cameras as the solution to misconduct; in fact, the few outlets that even acknowledged the issue of police sexual assault seemed confident that body cameras were the solution to this problem as well.[311] This insouciance is alarming. What accounts for the confidence that if Daniel Holtzclaw had been wearing a body camera, it would have inhibited rather than emboldened him?[312] A police officer who sexual-

---

306. Zoë Carpenter, *The Police Violence We Aren't Talking About*, THE NATION (Aug. 27, 2014), http://www.thenation.com/article/police-violence-we-arent-talking-about/ [https://perma.cc/YR28-9S99].

307. *Id.*

308. *See* Marc Weinreich, *Oklahoma Police Lieutenant Faces Life Sentence as List of Alleged Victims Grows to 13*, N.Y. DAILY NEWS (Nov. 5, 2014), http://www.nydailynews.com/news/national/police-lieutenant-faces-life-sentence-victims-list-grows-article-1.2000120 [https://perma.cc/YUL8-C4LB].

309. In 2015, Holtzclaw was convicted of 18 of the 36 sexual assault charges levied against him and sentenced to 263 years. *See* Sarah Larimer, *Disgraced Ex-Cop Daniel Holtzclaw Sentenced to 263 Years for On-Duty Rapes, Sexual Assaults*, WASH. POST (Jan. 22, 2016), https://www.washingtonpost.com/news/post-nation/wp/2016/01/21/disgraced-ex-officer-daniel-holtzclaw-to-be-sentenced-after-sex-crimes-conviction/?utm_term=.739367b8fffe [https://perma.cc/C9FQ-82CD].

310. William Crum, *Oklahoma City Police to Test Body Cameras for Police Officers*, THE OKLAHOMAN (Jan. 12, 2015), http://newsok.com/article/5384108 [https://perma.cc/S98G-QAL5].

311. *See Arrest of OKC Officer Highlights the Benefits of Body Cameras*, NEWS9.COM (Aug. 22, 2014), http://www.news9.com/story/26345123/arrest-of-okc-officer-highlights-benefits-of-body-cameras [https://perma.cc/4ZVH-H8PA].

312. In 2015, the Associated Press concluded a yearlong investigation into law enforcement sexual abuse, uncovering more than 1000 officers who lost their licenses for rape and sexual misconduct. One of these men, Officer Sergio Alvarez, had been reprimanded for failing to use his audio-visual recording unit during detentions. After Alvarez was arrested for sexual assault, investigators discovered that he had worn a personal camera during some of the assaults. Martha Irvine & Scott Smith, *AP: Officer Sex Cases Plagued by Lax Super-*

ly assaults multiple women while on duty must feel confident that his victims will not report him; a police officer armed with a camera that he controls will have additional leverage. How many women will be willing to report a sexual assault by a police officer if they know the assault has been captured on film and could be exposed to family, co-workers, and the general public? The belief that the footage would show unambiguous evidence of assault and would therefore serve the victim's interests rather than the perpetrator's is naïve for at least two reasons. First, viewers' interpretations of wrongdoing in video footage can vary dramatically, especially when sexual, racial, or other stereotypes are at work. The appearance of consent can also be coerced, especially by someone with a gun and a badge. Second, even if a video shows clear evidence of assault, this would be small comfort to victims living in a society where sexual assault victims are routinely exposed, humiliated, and shamed. To report any crime, particularly a sexual crime, is to sacrifice intimate privacy in a way that cannot be undone and cannot be controlled.

Failing to consider the impact that any form of surveillance — even ostensibly benign surveillance — will have on marginalized individuals can result in disastrous consequences for those individuals, as well for society as a whole. Attentiveness to intersectionality, in both Crenshaw's sense of multiple forms of subordination and in the sense of multiple forms of surveillance, is crucial.

B. Revenge Porn

Civil liberties groups often hold themselves out as the watchdogs of privacy. The ACLU, for example, states that it is dedicated to "expand[ing] the right to privacy, increas[ing] the control that individuals have over their personal information, and ensur[ing] that civil liberties are enhanced rather than compromised by new advances in science and technology."[313] In many ways, the ACLU has made good on this claim. It has urged the Federal Trade Commission to pursue data brokers who buy and sell information about consumers,[314] written a letter of support for the Genetic Information Nondiscrimination Act as a

---

vision, Policies, Associated Press (Nov. 2, 2015), http://bigstory.ap.org/article/d6701aa27d894889b5c3c599d8d9f467/ap-officer-sex-cases-plagued-lax-supervision-policies [https://perma.cc/L6HB-8JNW].

313. *Privacy & Technology*, ACLU, https://www.aclu.org/issues/privacy-technology [https://perma.cc/T7R9-XNVH].

314. Chris Calabrese, *Federal Trade Commission Needs to Move Beyond Reports When It Comes to Data Brokers*, ACLU, https://www.aclu.org/blog/technology-and-liberty/federal-trade-commission-needs-move-beyond-reports-when-it-comes-data [https://perma.cc/YQ5W-5CXQ].

means of protecting "extremely personal sensitive information,"[315] and encouraged Congress to pass legislation that would require patient consent for the use of medical records for "secondary purposes."[316] However, the ACLU's approach to sexual privacy — an issue of ever-increasing urgency, particularly for women — has been the opposite of protective. The ACLU has taken a strangely hostile stance on the issue of sexual privacy by singling out revenge porn laws for attack.[317]

In 2012, the problem of nonconsensual pornography, often misleadingly referred to as "revenge porn," began to receive mainstream attention. Nonconsensual pornography refers to sexually explicit images disclosed without consent and for no legitimate purpose.[318] The term includes material obtained by hidden cameras, consensually exchanged images within a confidential relationship, stolen photos, and recordings of sexual assaults. Nonconsensual pornography often plays a role in intimate partner violence, with abusers using the threat of disclosure to keep their partners from leaving or reporting abuse to law enforcement.[319] Traffickers and pimps also use nonconsensual pornography to trap unwilling individuals in the sex trade.[320] It is becoming increasingly common for rapists to record their attacks not only to further humiliate their victims but also to discourage victims from reporting sexual assaults.[321]

Nonconsensual pornography can cause immediate and irreversible harm. Abusers, hackers, and traffickers can make an explicit image of a victim accessible to thousands, even millions of people merely by uploading it to a website. That image can go viral in

---

315. *ACLU Letter to the Senate Urging Support of S. 358, the "Genetic Information Nondiscrimination Act of 2007,"* ACLU, https://www.aclu.org/letter/aclu-letter-senate-urging-support-s-358-genetic-information-nondiscrimination-act-2007 [https://perma.cc/QV66-7W5W].

316. *ACLU Urges Congress to Define Medical Privacy as Patient Control of Electronic Health Records*, ACLU (July 23, 2008), https://www.aclu.org/news/aclu-urges-congress-define-medical-privacy-patient-control-electronic-health-records [https://perma.cc/Z8YR-W228].

317. *See* Franks, *supra* note 275.

318. *See* Citron & Franks, *supra* note 113, at 346.

319. *See* Annmarie Chiarini, *I Was a Victim of Revenge Porn*, THE GUARDIAN (Nov. 19, 2013), http://www.theguardian.com/commentisfree/2013/nov/19/revenge-porn-victim-maryland-law-change [https://perma.cc/H75C-KN3X]; Jack Simpson, *Revenge Porn: What Is It and How Widespread Is the Problem?*, THE INDEPENDENT (July 2, 2014), http://www.independent.co.uk/news/uk/home-news/what-is-revenge-porn-9580251.html [https://perma.cc/25AA-S54L].

320. *See* Ann Bartow, *Pornography, Coercion, and Copyright Law 2.0*, 10 VAND. J. ENT. & TECH. L. 799, 818 (2008); Marion Brooks, *The World of Human Trafficking: One Woman's Story*, NBC CHICAGO (Feb. 22, 2013), http://www.nbcchicago.com/investigations/human-trafficking-alex-campbell-192415731.html [https://perma.cc/8DPG-E8Y7].

321. Tara Culp-Ressler, *16-Year-Old's Rape Goes Viral on Twitter*, THINK PROGRESS (July 10, 2014), http://thinkprogress.org/health/2014/07/10/3458564/rape-viral-social-media-jada/ [https://perma.cc/U5F4-RTJV].

minutes or even seconds, at which point it can dominate the search engine results for the victim's name.[322] The image can also make its way to the victim's family, employer, co-workers, and peers. Victims suffer extreme psychological distress, depression, and anxiety. They frequently experience threats of sexual assault, stalking, and harassment and are often fired from jobs[323] or forced to change schools.[324] Some victims have committed suicide.[325] Nonconsensual pornography is not restricted to female victims, although available evidence to date indicates that the majority of victims are women and girls, and that women and girls face more serious fallout.[326]

While nonconsensual pornography is not a new phenomenon, technology has accelerated its occurrence and impact. Technology makes it possible for abusers to crowdsource their harassment and has helped create a market for voyeuristic content. The Internet makes it possible for dedicated revenge porn sites and other forums to openly solicit private, intimate images and expose them to millions of viewers, while allowing the posters themselves to hide in the shadows.[327] Thousands of websites feature revenge porn,[328] and intimate material is also widely distributed without consent through social media, blogs, emails, and texts.

Before 2013, almost no laws in the U.S. explicitly addressed this invasion of sexual privacy,[329] even as almost every other form of privacy — including financial, medical, and data privacy — have obtained legal and socially sanctioned protection. While some existing voyeurism, surveillance, and computer hacking laws prohibit the observation and recording of individuals in states of undress or engaged in sexual activity without consent, the nonconsensual *disclosure* of intimate images has been, until very recently, largely unregulated by the law.

By March 2017, due in large part to the efforts of the Cyber Civil Rights Initiative (for which I serve as Vice-President and Legislative and Tech Policy Director), the social and legal landscape of the issue

---

322. *See* Citron & Franks, *supra* note 113, at 350.

323. *See* Ariel Ronneburger, Note, *Sex, Privacy, and Webpages: Creating a Legal Remedy for Victims of Porn 2.0*, 21 SYRACUSE SCI. & TECH. L. REP. 1, 8–9 (2009).

324. *See* Citron & Franks, *supra* note 113, at 350.

325. Emily Bazelon, *Another Sexting Tragedy*, SLATE (Apr. 12, 2013), http://www.slate.com/articles/double_x/doublex/2013/04/audrie_pott_and_rehtaeh_parsons_how_should_the_legal_system_treat_nonconsensual.html [https://perma.cc/6UKH-LGBU].

326. *See* Citron & Franks, *supra* note 113, at 347–48.

327. Dylan Love, *It Will Be Hard to Stop the Rise of Revenge Porn*, BUS. INSIDER (Feb. 8, 2013), http://www.businessinsider.com/revenge-porn-2013-2 [https://perma.cc/8R7T-X6LM].

328. *Revenge Porn: Misery Merchants*, THE ECONOMIST (July 5, 2014), http://www.economist.com/news/international/21606307-how-should-online-publication-explicit-images-without-their-subjects-consent-be [https://perma.cc/K4TB-5NC7].

329. *See* Mary Anne Franks, *Revenge Porn Reform: A View From the Front Lines*, 69 FLA. L. REV. (forthcoming Sept. 2017).

had been transformed.[330] As of this writing, several major social media platforms have banned nonconsensual pornography; furthermore, thirty-six states have passed laws directly aimed at the practice,[331] while several others are in the process of passing legislation; and finally, Congresswoman Jackie Speier (D-CA) introduced a bipartisan federal criminal bill against the practice, called the Intimate Privacy Protection Act, in July 2016.[332] But as support for victims and for legislative reform has grown, so has opposition to reform, most vociferously from the ACLU.

When the issue first began receiving extensive public attention, ACLU representatives implied that *no* criminal law aimed at prohibiting the nonconsensual distribution of sexually explicit images was compatible with the First Amendment.[333] While the organization abandoned this claim fairly quickly, it continued to attack legislative efforts to address the problem. The organization penned letters and gave testimony asserting that the definition of the crime as proposed by victim advocates, legal experts, and democratically elected state lawmakers should be set aside in favor of the ACLU's own definition, to wit:

> (1) [A] person who was or is in an intimate relationship with another person and who, (2) during and as a result of that relationship, obtained a recognizable image of such other person in a state of nudity, (3) where such other person had a reasonable expectation of privacy and an understanding that such image would remain private, (4) to display such image (5) without the consent of such other person, (6) with the intent to harass, humiliate, embarrass, or otherwise harm such other person, and (7) where there is no public or newsworthy purpose for the display.[334]

---

330. *Id.* at 15, 21–24.

331. *Id.* at 4, 22–23.

332. Mary Anne Franks, *How to Defeat 'Revenge Porn': First, Recognize it's About Privacy, not Revenge*, HUFFINGTON POST (June 22, 2015), http://www.huffingtonpost.com/mary-anne-franks/how-to-defeat-revenge-porn_b_7624900.html [https://perma.cc/6YB7-5FQF].

333. CALIFORNIA SENATE RULES COMMITTEE, BILL ANALYSIS SB 255, at 5 (2013), http://www.leginfo.ca.gov/pub/13-14/bill/sen/sb_0251-0300/sb_255_cfa_20130703_114233_sen_floor.html [https://perma.cc/WRB9-GH9F] ("The ACLU states, 'The posting of otherwise lawful speech or images even if offensive or emotionally distressing is constitutionally protected. The speech must constitute a true threat or violate another otherwise lawful criminal law, such as stalking or harassment statute, in order to be made illegal.'").

334. *See* Franks, *supra* note 275.

How the ACLU arrived at this particular definition or why this definition is superior to other definitions has never been made clear.

The ACLU's definition of the crime of nonconsensual pornography rests on an exceedingly narrow conception of privacy, one that is at odds with fairly uncontroversial criminal legislation regarding other forms of private information. Both state and federal criminal laws prohibit the unauthorized disclosure of materials such as medical records,[335] financial data,[336] and cell phone usage information.[337] None of these statutes require that perpetrators act with the intent to harass their victims, and certainly none require that the perpetrator and victim be intimate partners. The ACLU clearly recognizes that protecting privacy in these contexts, without "intent to harass" requirements, does not violate the First Amendment.[338] The privacy measures spearheaded by the ACLU itself emphasize the right of individuals not to have their private information disclosed without consent, without any reference to motive.[339] While the ACLU does not claim that people have a First Amendment right to disclose medical records, social security numbers, or geolocation data of others without consent, it does claim that there is a First Amendment right to disclose naked photos and sex videos without consent. It is difficult to understand why the ACLU treats a form of privacy violation that disproportionately affects women differently from other privacy violations.

It is an unfortunate reality that women are experts in surveillance. From street harassment to sexual assault, stalking to limitations on reproductive rights, surveillance is a part of most women's daily lives. Sexual surveillance has devastating consequences on victims' freedom of intimate association, their participation in political, social, and cultural life, their educational and professional opportunities, and the development of their personalities. Those who discount the gravity of the harms of intimate surveillance — who indeed refuse to even recognize it as such and attempt to downgrade it to harassing or distressing behavior — reveal that their allegiance is not to privacy, but to the interests of those who enjoy and profit from invading privacy. Given that men make up the majority of perpetrators of intimate surveillance and women make up the majority of victims, this also means allegiance to the interests of men over the interests of women.

---

335. 42 U.S.C. § 1320d-6 (2010).

336. TEX. PENAL CODE ANN. § 31.01 (West 2015).

337. 47 U.S.C. § 222 (2015).

338. The ACLU's position also rests on a deeply flawed understanding of the First Amendment. *See* Franks, *supra* note 275.

339. *See* Mary Anne Franks, *It's Time for Congress to Protect Intimate Privacy*, HUFFINGTON POST (July 18, 2016), http://www.huffingtonpost.com/mary-anne-franks/revenge-porn-intimate-privacy-protection-act_b_11034998.html [https://perma.cc/3KJB-GY33].

Failing to acknowledge the multiple ways in which women and girls experience and are burdened by surveillance promotes male sexual entitlement over female autonomy. Characterizing invasions of privacy as free speech and attempts to protect privacy as censorship are not neutral or principled positions. It discounts the privacy interests of women in favor of the entertainment and profit interests of men, and, as such, is a profoundly undemocratic approach to privacy.

C. A Tale of Two Cases: From Terry *to* Papachristou

It is possible to develop a sophisticated and consistent approach to privacy that does not devalue the experience of marginalized populations. The contrast between two Supreme Court cases, *Terry v. Ohio*[340] and *Papachristou v. Jacksonville*[341] can provide a blueprint for the move from privileged interests to democratic interests.

The Court in *Terry* famously established that the practice of "stop and frisk," while subject to Fourth Amendment analysis, did not require probable cause.[342] Officer McFadden, a white officer, stopped and searched three men, two of whom were black, after observing them walk past a store window and peer into it several times.[343] McFadden was not able to say why he first started monitoring Terry and Chilton except that "they just didn't look right to me."[344] The Court found that what would later be termed "reasonable suspicion" was a sufficient basis for a stop and frisk.[345] The Court's decision was delivered in the wake of riots that had followed the assassination of Martin Luther King, Jr. earlier that year.[346] The civil rights movement had unleashed a wave of sit-ins, protests, and demonstrations, and law enforcement often responded with brutal force. Chief Justice Earl Warren took note of the unrest, referring to the "wholesale harassment by certain elements of the police community, of which minority groups, particularly Negroes, complain."[347] While he invoked the reality of racial surveillance, in the next breath he seemed to ignore it, asserting that this harassment cannot be deterred by the primary remedy for Fourth Amendment violations: namely, the exclusionary rule.[348] The rule, Justice Warren found, "is powerless to deter invasions of constitutionally guaranteed rights where the police either

340. Terry v. Ohio, 392 U.S. 1 (1968).
341. Papachristou v. Jacksonville, 405 U.S. 156 (1972).
342. *See Terry*, 392 U.S. at 2–3.
343. *Id.* at 1.
344. *Id.* at 5.
345. *See id.* at 30–31; *id.* at 37 (Douglas, J., dissenting).
346. *See* David A. Harris, *Frisking Every Suspect: The Withering of Terry*, 28 U.C. DAVIS L. REV. 1, 7 (1994).
347. *Terry*, 392 U.S. at 14.
348. *Id.* at 14–15.

have no interest in prosecuting or are willing to forgo successful prosecution in the interest of serving some other goal."[349] This curious formulation suggests that the Court did not rule against law enforcement in this case in part because doing so would not deter police who are motivated by prejudice. While it may be true that suppressing the evidence would not, standing alone, discourage law enforcement officers from engaging in racist practices, it does not follow that the Court could not or should not have found the search and seizure unconstitutional.

The lone dissenter in *Terry*, Justice Douglas, condemned the majority opinion as "a long step down the totalitarian path."[350] Four years later, Justice Douglas authored the majority opinion in *Papachristou*, striking down a Florida anti-vagrancy statute as unconstitutional.[351] The ordinance criminalized an impressive range of conduct and persons, including "persons wandering or strolling around from place to place without any lawful purpose or object, habitual loafers, [and] disorderly persons . . . ."[352] In declaring the statute overly broad and vague, Justice Douglas took note of two points in particular. First, that the freedom to engage in the kinds of activities outlined in the statute is central to the development of the human personality: "[T]hese activities are historically part of the amenities of life as we have known them. . . . They have encouraged lives of high spirits rather than hushed, suffocating silence."[353] Second, he observed that the discretion granted to law enforcement through these vague terms would no doubt result in disproportionate targeting of the marginalized:

> Those generally implicated by the imprecise terms of the ordinance — poor people, nonconformists, dissenters, idlers — may be required to comport themselves according to the lifestyle deemed appropriate by the . . . police and the courts. . . . It results in a regime in which the poor and the unpopular are permitted to "stand on a public sidewalk" . . . only at the whim of any police officer.[354]

Justice Douglas's opinion in *Papachristou* is in many ways the inverse of Chief Justice Warren's in *Terry*. *Terry* gave the green light for vague intuitions of law enforcement officers to serve as justifica-

---

349. *Id.* at 14.
350. *Id.* at 38 (Douglas, J., dissenting).
351. *See* Papachristou v. Jacksonville, 405 U.S. 156, 156 (1972).
352. *Papachristou*, 405 U.S. at 156–57 n.1.
353. *Id.* at 164.
354. *Id.* at 170 (citation omitted).

tion for invasive surveillance and invoked the existence of prejudice against a marginalized group only to ignore its constitutional significance. *Papachristou* rejected the attempt of law enforcement to broadly criminalize the freedom of movement and invoked prejudice against marginalized groups as a matter of deep constitutional significance. The contrast between these two cases offers important lessons about how we can ensure that our most fiercely defended rights are grounded in the experience of those who have the most to lose.

VI. THE POSSIBILITY OF DEMOCRATIC PRIVACY

A 2014 *New York Times* article on facial recognition technology focused on the concerns of one of the technology's pioneers, Joseph J. Atick, that face-matching could have disastrous consequences for privacy:

> Online, we are all tracked. But to Dr. Atick, the street remains a haven, and he frets that he may have abetted a technology that could upend the social order. Face-matching today could enable mass surveillance, "basically robbing everyone of their anonymity," he says, and inhibit people's normal behavior outside their homes. Pointing to the intelligence documents made public by Edward J. Snowden, he adds that once companies amass consumers' facial data, government agencies might obtain access to it, too.[355]

The obliviousness to race, gender, and class in this passage is remarkable. "Online, we are all tracked" of course assumes that "we" are all online, despite the fact that online access is a privilege not accessible to many people.[356] "[T]he street remains a haven" — for whom? Not to women, young minority men, or homeless individuals, for whom "the street" offers daily harassment, threats, and unwanted scrutiny. Face-matching technology deployed on the street might rob "everyone" of their anonymity — that would be people who are not already effectively deprived of anonymity due to databases tracking criminal records, welfare rolls, or child support delinquency, or deprived ano-

---

355. Natasha Singer, *Never Forgetting a Face*, N.Y. TIMES (May 17, 2014), http://www.nytimes.com/2014/05/18/technology/never-forgetting-a-face.html?_r=0 [https://perma.cc/WPU7-DM2K].

356. *See* Astra Taylor, *The Internet's Destructive Gender Gap: Why the Web Can't Abandon Its Misogyny*, SALON (April 10, 2014), https://www.salon.com/2014/04/10/the_internets_destructive_gender_gap_why_the_web_cant_abandon_its_misogyny_partner/ [https://perma.cc/97RZ-TSFM].

nymity through pretextual policing, or through stalking and harassment. This new technology will "inhibit people's normal behavior outside of their homes" — that is, those of us with homes and who are not already adapting our clothes, routes to work, facial expressions, or gait.[357] And finally, Atick says that "government agencies might obtain access" to our facial data, as if the government indisputably posed the greatest threat to citizens, a presumption that thousands of victims of racist aggression, public harassment, and domestic violence likely would not share.

This passage is a striking example of how the dominant privacy narrative, in focusing on fairly recent historical developments mostly involving state-sponsored threats to the informational privacy interests of mainstream and elite society, ignores the very long and destructive history of the surveillance of marginalized bodies, in particular black bodies, poor bodies, and female bodies. This focus not only erases the very real harms inflicted on these groups, but also warps the conception of surveillance itself and jeopardizes the privacy rights of all. If left unaddressed, these distortions will undermine any true progress on the question of privacy and how to protect it.

The foregoing is not intended to establish a hierarchy of the surveillance harms of one group over another, or to suggest that violations of informational privacy are trivial compared to violations of physical and decisional privacy. Rather, it is meant to encourage the potential for empathy and reflection presented by the democratization of surveillance. Mainstream society's relatively recent and, in many cases, relatively superficial encounter with the chilling effects of surveillance provides an opportunity to throw off historical complacency regarding the regulation of marginalized groups and to develop truly inclusive privacy protections. If society fails to do so, and responds only to the threat that a constrained view of surveillance poses to those with power and privilege, then there will be no real development or real progress with regard to privacy. Such an interest-convergence approach to privacy will parallel the limitations of an interest-convergence approach to racial equality.[358] We will be left with an anemic defense of anemic privacy rights that will have little chance of weathering the next great threat to expression and autonomy.

Kimberle Crenshaw's intersectional approach can function as a counter to the limitations of interest convergence described by Bell. Intersectionality is not only a way of understanding oppression and focusing on the needs of the most vulnerable, but also a way to im-

---

357. *See* Stacey Patton, *Is Looking Black a Crime?*, DAME MAGAZINE (Jan. 12, 2015), http://www.damemagazine.com/2015/01/12/looking-black-crime [https://perma.cc/P8LN-KNEW].

358. *See* Bell, *supra* note 7, at 528.

prove society as a whole. When we address "the needs and problems of those who are most disadvantaged . . . , then others who are singularly disadvantaged would also benefit."[359] When we build our systems around the experiences of the most vulnerable, we improve the outcomes for everyone. As Crenshaw eloquently expressed it, "When they enter, we all enter."[360] We can respond to the democratization of surveillance by democratizing privacy, by structuring it around the needs and interests of those who suffer the most. When they have privacy, we all have privacy.

359. Crenshaw, *supra* note 121, at 167.
360. *Id.*