

Boston University School of Law
Scholarly Commons at Boston University School of Law

Faculty Scholarship

9-2018

A Poor Mother's Right to Privacy: A Review

Danielle K. Citron

Boston University School of Law

Follow this and additional works at: https://scholarship.law.bu.edu/faculty_scholarship



Part of the [Privacy Law Commons](#)

Recommended Citation

Danielle K. Citron, *A Poor Mother's Right to Privacy: A Review*, 98 Boston University Law Review 1139 (2018).

Available at: https://scholarship.law.bu.edu/faculty_scholarship/634

This Book Review is brought to you for free and open access by Scholarly Commons at Boston University School of Law. It has been accepted for inclusion in Faculty Scholarship by an authorized administrator of Scholarly Commons at Boston University School of Law. For more information, please contact lawlessa@bu.edu.



COMMENT

A POOR MOTHER’S RIGHT TO PRIVACY: A REVIEW

DANIELLE KEATS CITRON*

INTRODUCTION	1140
I. PRIVACY RIGHTS AND POOR MOTHERS	1143
A. <i>Dispossession</i>	1144
B. <i>Due Process Turn</i>	1148
II. A NEW PRIVACY	1152
A. <i>The Scholarship of Charles Reich</i>	1152
B. <i>Due Process Rights for the Poor</i>	1155
C. <i>Beyond the Constitution</i>	1157
III. LAW, CONTEXT, AND RECIPROCITY	1161
A. <i>Technologies of Perfect Surveillance</i>	1161
B. <i>Reciprocity</i>	1166
CONCLUSION	1167

Collecting personal data is a feature of daily life. Businesses, advertisers, agencies, and law enforcement officers amass massive reservoirs of our personal data. This state of affairs—what I am calling the “collection imperative”—is justified in the name of efficiency, convenience, and security. The unbridled collection of personal data, however, leads to abuses. Public and private entities have disproportionate power over individuals and groups whose information they have amassed. Nowhere is that power disparity more evident than the State’s surveillance of the indigent. Poor mothers in particular have vanishingly little privacy. Whether or not poor mothers receive subsidized prenatal care, the existential state of poor mothers is persistent and indiscriminate State surveillance.

Professor Khiara Bridges’s book, The Poverty of Privacy Rights, advances the project of securing privacy for the most vulnerable among us. It argues

* Morton & Sophia Macht Professor of Law, University of Maryland Francis King Carey School of Law; Affiliate Scholar, Stanford Center on Internet & Society; Affiliated Fellow, Yale Information Society Project. Deep thanks to Khiara Bridges and James Fleming for including me in Boston University Law School’s celebration of *The Privacy of Poverty Rights* and to Michele Goodwin, Ryan Calo, David Gray, Woodrow Hartzog, Neil Richards, Marc Rotenberg, David Super, and Peter Swire for excellent comments. Dena Robinson, Emily Bryant, Susan McCarty, and Elyshia Menkin provided helpful research assistance. I am grateful to Roy Fan and the editors of the *Boston University Law Review* for their insightful edits and comments.

that poor mothers have a constitutional right not to be known if the State's data collection efforts demean and humiliate them for no legitimate purpose. This Book Review situates the book's contributions in light of another era's due process revolution. Fifty years ago, Professor Charles Reich's scholarship provided a theory for why government entitlements for the poor deserved the same protection as those provided the wealthy. His scholarship fundamentally changed the way the Supreme Court understood the procedural due process rights of the poor. Now, as then, Professor Bridges's scholarship has the potential to transform our conception of substantive due process protections for indigent mothers.

The Poverty of Privacy Rights provides an important lens for rethinking the data collection imperative more generally. It supplies a theory not only on which a constitutional right to information privacy can be built but also on which positive law and norms can develop. Concepts of reciprocity may provide another analytical tool to understand a potential right to be as unknown to government as it is to us.

INTRODUCTION

Collecting personal data is a feature of daily life.¹ Businesses collect massive amounts of information about consumers' likes and dislikes, strengths and weaknesses.² Online behavioral advertisers have copious records of individuals' searches, purchases, musings, and wish lists.³ Law enforcement aggregates video streams from public and private security cameras, images from license-plate readers, and data from government and private databases.⁴ Federal and state agencies amass dossiers on individuals in connection with decisions about employment, licenses, contracts, public benefits, travel, and taxes.⁵

¹ See JULIE E. COHEN, CONFIGURING THE NETWORKED SELF: LAW, CODE, AND THE PLAY OF EVERYDAY LIFE 1 (2012) ("Over the last two decades, the rapid evolution of networked information and communication technologies has catalyzed equally rapid change in the organization of economic and social activity."); Danielle Keats Citron, *Reservoirs of Danger: The Evolution of Public and Private Law at the Dawn of the Information Age*, 80 S. CAL. L. REV. 241, 244 (2007) ("Today, databases of personal identifying information in the private sector ensure the seamless flow of commerce.").

² See JOSEPH TUROW, THE AISLES HAVE EYES: HOW RETAILERS TRACK YOUR SHOPPING, STRIP YOUR PRIVACY, AND DEFINE YOUR POWER 1-3 (2017); Ryan M. Calo, *Digital Manipulation*, 82 GEO. WASH. L. REV. 995, 995 (2014) ("Today's companies fastidiously study consumers and, increasingly, personalize every aspect of the consumer experience.").

³ See JOSEPH TUROW, THE DAILY YOU: HOW THE NEW ADVERTISING INDUSTRY IS DEFINING YOUR IDENTITY AND YOUR WORLD 1 (2011).

⁴ See David Gray & Danielle Keats Citron, *The Right to Quantitative Privacy*, 98 MINN. L. REV. 62, 66 (2013) (explaining that law enforcement aggregates and analyzes video streams to create 24/7 surveillance systems).

⁵ DANIEL J. SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE 2-3 (2004) ("[A]n ever-growing series of records is created about almost

This state of affairs—what I am calling the “collection imperative”—is justified in the name of efficiency, convenience, and security.⁶ Retailers recommend gifts based on the recipients’ online activities.⁷ Startups promise to use our genetic data to personalize dining options and family planning.⁸ Law enforcement tracks individuals who have been flagged as likely to commit crimes.⁹ Federal agencies assign “risk assessment scores” to travelers.¹⁰

American law has largely tolerated this approach. In the United States, information privacy law generally focuses on the transparency, security, and disclosure of personal data.¹¹ The general assumption is that the collection of personal data is optimal for social welfare.¹² Everyone is better off if gifts are enjoyed, diseases are prevented, and criminals are caught, terrorists are stopped from flying, and citizens are provided with appropriate services. At most, the law addresses downstream problems associated with databases of personal data.¹³

every facet of a person’s life. As businesses and the government increasingly share personal information, digital dossiers about nearly every individual are being assembled.”).

⁶ VIKTOR MAYER-SCHONBERGER & KENNETH CUKIER, *BIG DATA: A REVOLUTION THAT WILL TRANSFORM HOW WE LIVE, WORK, AND THINK* 19 (2014) (arguing that big data developments are allowing problems to be viewed in new light); Jonathan Shaw, *Why Big Data Is a Big Deal*, HARV. MAG. (Mar.–Apr. 2014), <https://harvardmagazine.com/2014/03/why-big-data-is-a-big-deal> [<https://perma.cc/7XPW-KB5T>] (arguing that big data is justified on grounds that it creates innovative solutions to societal problems).

⁷ See, e.g., Shaw, *supra* note 6 (explaining that companies “make purchase suggestions based on the prior interests of one customer as compared to millions of others”).

⁸ Alexandra Ossola, *These DNA Diet Apps Want to Rule Your Health*, WIRED, (May 1, 2017, 12:00 AM) <https://www.wired.com/2017/05/these-dna-diet-apps-want-to-rule-your-health/>.

⁹ See ANDREW G. FERGUSON, *THE RISE OF BIG DATA POLICING: SURVEILLANCE, RACE, AND THE FUTURE OF LAW ENFORCEMENT* 8-9 (2017).

¹⁰ *EPIC v. CBP (Analytical Framework for Intelligence)*, ELEC. PRIVACY INFO. CTR., <https://epic.org/foia/dhs/cbp/afi/#documents> [<https://perma.cc/9S22-4SAK>] (explaining that U.S. Customs and Border Protection’s Analytical Framework for Intelligence uses personally identifiable information from government and private data sources to identify threats to security); see U.S. CUSTOMS AND BORDER PROT., U.S. DEP’T OF HOMELAND SEC., *PRIVACY IMPACT ASSESSMENT FOR THE ANALYTICAL FRAMEWORK FOR INTELLIGENCE 1-2* (2012), https://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_cbp_afi_june_2012.pdf [<https://perma.cc/6EV8-ND5Y>] (explaining methods used by Customs and Border Protection to assess individuals for risk).

¹¹ See Danielle Keats Citron, *The Privacy Policymaking of State Attorneys General*, 92 NOTRE DAME L. REV. 747, 763 (2016).

¹² See WILLIAM MCGEVERAN, *PRIVACY AND DATA PROTECTION LAW* 382-83 (2016) (“[I]ncreased processing and use of personal data is inevitable and offers enormous value to society.”).

¹³ Cf. *id.* at 383 (“Ideally, privacy law seeks to maximize [benefits of data collection] and reduce risks of harm, of course. When it comes to governing data processing and use, this balance is not always so easy to achieve.”).

The unbridled collection of personal data, however, can and does lead to abuses. Government and businesses obtain disproportionate power over individuals and groups whose information they have amassed.¹⁴ As Neil Richards and Woodrow Hartzog explain, individuals are “vastly less powerful than the government and corporate institutions that create and control digital technologies and the personal data on which those technologies run.”¹⁵

Nowhere is that power disparity more evident than the State’s surveillance of society’s most vulnerable members. The poor, unlike the affluent, are subject to unlimited state surveillance.¹⁶ The merger of big data and law enforcement results in persistent, indiscriminate surveillance of poor communities.¹⁷ Public benefits programs subject the poor to ever more intrusive and demeaning interrogations and inspections.¹⁸ A recent example is Wisconsin’s mandatory drug testing of food-stamp recipients.¹⁹

When it comes to poor mothers specifically, the State’s data collection efforts are boundless and inescapable.²⁰ If poor mothers obtain government assistance for medical care, every aspect of their life is interrogated, and every data point is collected.²¹ On the other hand, if poor mothers decline to pursue Medicaid benefits to protect their privacy, the State’s child protective services train their eyes on them.²² As a result, poor mothers find themselves under state surveillance whether or not they receive government-funded prenatal care.²³

¹⁴ See Neil M. Richards, *The Dangers of Surveillance*, 126 HARV. L. REV. 1934, 1936-37 (2013) (explaining how government and business obtain data for “purposes of influence, management, protection or direction.” (internal quotation omitted)).

¹⁵ Neil Richards & Woodrow Hartzog, *Privacy’s Trust Gap: A Review*, 126 YALE L.J. 1180, 1183 (2017).

¹⁶ See JOHN GILLIOM, *OVERSEERS OF THE POOR* 2-3 (2001).

¹⁷ Michele Estrin Gilman, *The Class Differential in Privacy Law*, 77 BROOK. L. REV. 1389, 1389-90 (2012) (“[The poor] endure a barrage of information-collection practices that are far more invasive and degrading than those experienced by their wealthier neighbors.”); see also FERGUSON, *supra* note 9, at 47, 73-76 (explaining that “predictive policing” methods use criteria that adversely affect poor communities).

¹⁸ See GILLIOM, *supra* note 16, at 1-5 (describing how monitoring systems associated with welfare programs allow welfare and law enforcement authorities to routinely conduct surveillance of poor individuals).

¹⁹ Jim Cole, *Scott Walker Moves Forward with Plan to Drug Test Food Stamp Users*, CBS NEWS (Dec. 9, 2017, 4:58 PM), <https://www.cbsnews.com/news/scott-walker-moves-forward-with-plan-drug-test-food-stamp-users/> [https://perma.cc/3T3B=7DJB].

²⁰ See KHIARA M. BRIDGES, *THE POVERTY OF PRIVACY RIGHTS* 1-5 (2017).

²¹ See *id.*

²² See *id.* at 1-2, 115-116 (explaining that criteria for what constitutes child abuse defines many attributes that are essentially synonymous with being poor, thereby forcing pregnant mothers to either accept state aid or run risk of committing child neglect).

²³ See *id.* at 148-49.

Professor Khiara Bridges's book, *The Poverty of Privacy Rights*, is an important step in developing "a bill of rights for the disinherited."²⁴ Building on her findings in *Reproducing Race: An Ethnography of Pregnancy as a Site of Racialization*,²⁵ Professor Bridges explains that state surveillance of poor mothers is premised on the moral construction of poverty rather than on legitimate concerns about prenatal care or successful parenting. Poor mothers are subjected to invasive state surveillance because their character is seen as defective and norm-breaking.²⁶ *The Poverty of Privacy Rights* contends that the constitutional right to information privacy should be understood to limit the State's collection of personal data from poor mothers.²⁷ Recognizing a zone of privacy is essential for a poor mother's dignity, autonomy, and capacity for self-governance.²⁸

This Book Review proceeds in three Parts. Part I discusses the central arguments and contributions of *The Poverty of Privacy Rights*. Part II situates the book's contributions in light of another era's due process revolution. Fifty years ago, Professor Charles Reich's scholarship provided a theory for why government entitlements for the poor and the wealthy equally deserved protection.²⁹ His scholarship fundamentally changed the way the Supreme Court understood the procedural due process rights of the poor.³⁰ Professor Bridges's scholarship has the potential to transform our conception of substantive due process protections for indigent mothers. Part II also sketches out a reform agenda that reaches beyond the Constitution. Part III frames the book's contributions in light of broader concerns about technologies of perfect surveillance. It extends the conversation to concepts of reciprocity and a potential right to be as unknown to government as it is to us.

I. PRIVACY RIGHTS AND POOR MOTHERS

Poor mothers have vanishingly little privacy. In exchange for government assistance with prenatal care, the State demands information about every detail of poor mothers' lives. It collects information about poor mothers' life experi-

²⁴ Charles A. Reich, *Individual Rights and Social Welfare: The Emerging Legal Issues*, 74 YALE L.J. 1245, 1257 (1965).

²⁵ See generally KHIARA M. BRIDGES, *REPRODUCING RACE: AN ETHNOGRAPHY OF PREGNANCY AS A SITE OF RACIALIZATION* (2011).

²⁶ See *infra* Section I.A (describing invasive assessments that State requires poor mothers to undergo when seeking healthcare).

²⁷ See *infra* Section I.B (considering State's surveillance of poor mothers in light of Supreme Court's recognition of right to privacy).

²⁸ See *infra* notes 108-109, 164 and accompanying text (explaining that privacy fosters autonomy, dignity, and self-governance).

²⁹ See *infra* Section II.A (describing influence of Professor Charles Reich's *The New Property*).

³⁰ See *infra* note 151 and accompanying text (noting that Supreme Court cited Reich's work in deciding scope of due process property rights).

ences, bodies, and homes.³¹ *The Poverty of Privacy Rights* explores the harm of such surveillance and why the Constitution should be understood to limit the State's data collection practices. This Part highlights the book's contribution to our understanding of the moral foundation and legal significance of the State's surveillance of poor mothers.

A. *Dispossession*

When pregnant women seek government assistance for medical care, the State demands a dizzying array of personal information.³² In addition to the expected health exams to determine pregnant women's physical health, state Medicaid rules require assessments of their "nutritional status, health education status, and psychosocial status."³³ Data is collected about poor pregnant women's "formal education and reading level," "religious and cultural influences," "history of previous pregnancies," "general emotional status and history," "wanted or unwanted pregnancy," "personal adjustment to pregnancy," "substance use and abuse," "housing/household," and "education/employment."³⁴

Poor mothers are interrogated about topics that have little to no connection with their physical health, the well-being of the fetus, or their ability to parent.³⁵ The State's questions vary from the quotidian to the highly sensitive. Was the pregnancy planned?³⁶ How many sexual partners has she had?³⁷ What are her strategies for preventing future pregnancies?³⁸ Has she ever had any marital or family problems?³⁹ Has she ever experienced sexual assault or domestic violence?⁴⁰ Has she ever been homeless?⁴¹ Has she ever struggled with mental illness?⁴² Has she ever used drugs or alcohol?⁴³ Has she ever ex-

³¹ See *infra* notes 37-48- and accompanying text (describing inquiries State poses to poor mothers during medical assessments).

³² See BRIDGES, *supra* note 20, at 1-2 (listing numerous assessments required before pregnant women receive medical care under California's Medicaid regulations).

³³ *Id.* (internal quotation marks omitted) (quoting CAL. CODE REGS. tit. 22, § 51348(e)(1)(A) (2012)).

³⁴ *Id.* at 2, 111 (quoting CAL. CODE REGS. tit. 22, § 51348(e)(1)(A) (2012)).

³⁵ See *id.* at 111-12, 164-66 (characterizing interrogations as social interventions rather than physical assessments).

³⁶ *Id.* at 111 ("Poor pregnant women in New York must . . . undergo[] a screening that asks about the unplanned-ness and/or unwantedness of the current pregnancy . . .").

³⁷ See *id.* at 166 (discussing poor pregnant women being forced to answer questions about "sexual adventurous[ness]").

³⁸ *Id.* at 7 (discussing "inquiries about women's . . . strategies for preventing the conception and birth of more children").

³⁹ *Id.* at 111.

⁴⁰ *Id.*

⁴¹ *Id.*

⁴² *Id.* ("Poor pregnant women in New York must . . . undergo[] a screening that asks about . . . [their] history of psychiatric treatment or emotional disturbance . . .").

changed sex for money or gifts?⁴⁴ What is her highest level of education?⁴⁵ Was she ever expelled from high school?⁴⁶ Has she ever been arrested or convicted of a crime?⁴⁷ Has she ever been found guilty of possessing contraband?⁴⁸

As Professor Bridges explains, the State's interrogations are rooted in the moral construction of poverty.⁴⁹ Under that construction, the pregnant mother's defective character is the cause of her indigence.⁵⁰ Race contributes to this construction—racial minorities are disproportionately represented among the poor.⁵¹ As President Ronald Reagan made famous with his description of the “welfare queen,” indigent black motherhood is caricatured as sexually irresponsible, lazy, and deviant.⁵²

The State's interrogations reflect the moral construction of poverty by attaching “pathology . . . to poor bodies.”⁵³ Why would the State demand information about a poor mother's history with abortion, prostitution, school expulsion, criminality, sexual abuse, mental illness, and homelessness if not for the State's belief that she is a person of defective character? The State's questions say that poor mothers are the *type* of people who abuse drugs, sell sex, commit crimes, and engage in behavior that would warrant suspension from school.⁵⁴ Because a poor mother's poverty is taken to suggest a flawed character that may cause her to mistreat her child, the State “*always* has the authority to infringe” her privacy.⁵⁵

⁴³ *Id.* at 166 (noting that poor pregnant women are often asked whether they have “been addicted to drugs” or “abused alcohol”).

⁴⁴ *Id.* at 174 (“She may have to reveal that she has broken moral norms dictating that sexual intercourse . . . should never be exchanged for money or gifts.”).

⁴⁵ *Id.* at 167.

⁴⁶ *Id.* at 166.

⁴⁷ *See id.* at 167 (arguing that poor mothers should not have to answer questions regarding “punishment by the criminal justice system”).

⁴⁸ *Id.* at 166.

⁴⁹ *See id.* at 113 (“[The State's interrogations] reveal that poor women are less valuable members of the body politic.”).

⁵⁰ *See id.* at 7 (discussing how moral construction of poverty leads to “idea that people are poor because something is wrong with them”).

⁵¹ *See id.* at 33 (“It is easy to moralize poverty when those who are disproportionately impoverished are racial Others.”).

⁵² *See id.* at 54 (discussing how President Reagan's stories of “welfare queen” reflected “a culture wherein black people have been constructed as sexually lascivious[,] . . . intractably indolent” and “apotheosis of immorality”).

⁵³ *Id.* at 113.

⁵⁴ *See id.* at 149 (noting that “the pursuit of full information about an individual poor mother would not even be attempted without the baseline supposition about the group to which she belongs”).

⁵⁵ *Id.* at 114 (emphasis in original).

Evidence that the State's surveillance of poor mothers has fulfilled its stated goal to protect children is scant. State surveillance has, however, resulted in grave harm to children. In a recent case, state workers placed a newborn into foster care based on concerns that the mother's poverty would prevent her from providing basic necessities for her child.⁵⁶ The infant died roughly three months later while in foster care.⁵⁷ The foster parents could have prevented the baby's death with a firm mattress.⁵⁸

As *The Poverty of Privacy Rights* illuminates, the State's interrogations strike a powerful blow to poor mothers' sense of self-worth. The State's message is that poor mothers "do not have equal standing in the nation's cultural imagination."⁵⁹ Rather than equal citizens of the state, they are subjects of a state that sees them as a social problem.⁶⁰ The State's interrogations suggest that uninsured mothers are diseased, broken, and incompetent, whereas insured mothers are told no such thing.⁶¹ They say that poor mothers' destructive tendencies must be tracked to prevent harm to their children.⁶² The state's "dignity-harming interrogations . . . insult poor pregnant women" and construct them as "second-class citizens."⁶³

The State's collection imperative carries downstream risks. Information stored in government databases is notoriously insecure.⁶⁴ The State's digital

⁵⁶ Mark Douglas, *Pinellas Parents Bury Newborn Who Died in Pasco Foster Care*, WFLA (Nov. 7, 2017, 6:21 PM), <http://wfla.com/2017/11/07/pinellas-parents-bury-newborn-who-died-in-pasco-foster-care/> [perma.cc/C4GJ-LHBX].

⁵⁷ *Id.* (reporting that baby was placed in foster care after July 29, 2017, and died on October 24, 2017).

⁵⁸ *See id.* (noting that foster parents "failed to follow [foster care agency's] baby safety checklist that says all infants should sleep in a crib with a firm mattress and tight-fitting sheets without other materials that might suffocate a baby" and instead put baby to sleep in adult bed).

⁵⁹ BRIDGES, *supra* note 20, at 113.

⁶⁰ *Id.* at 7-8 ("If personal failures are the presumptive cause of poverty, then poor *mothers* ought to be supervised closely, as their personal failures necessarily implicate children." (emphasis in original)).

⁶¹ *Id.* at 149 (noting different ways that mothers are treated based on financial conditions).

⁶² *See id.* at 12 (arguing that "if poor mothers have not been given privacy rights . . . because their behavioral or ethical flaws necessarily implicate children, these flaws would also explain why have [sic] been given ineffective privacy rights").

⁶³ *Id.* at 121.

⁶⁴ The breach of the federal Office of Personnel Management ("OPM") is a prominent example of the vulnerability of government databases. *See* Maria Korolov, *The OPM Data Breach 2 Years On: What Government Agencies Must Do Now*, CSO (June 20, 2017, 3:00 AM), <https://www.csoonline.com/article/3201041/data-breach/the-opm-data-breach-2-years-on-what-government-agencies-must-do-now.html> [perma.cc/SQZ2-K2U4] (discussing aftermath of OPM breach, which left vulnerable nearly twenty-two million Social Security numbers, over one million fingerprints, and individuals' criminal and financial histories).

dossiers about poor mothers may be subject to data leaks and hacks.⁶⁵ A common source of data breaches involves public hospitals where the personal data of poor mothers is collected and stored.⁶⁶ Personal data extracted from poor pregnant women could be used to create risk profiles that could justify searches of their homes in the name of child protection. Government-generated risk profiles, in turn, can result in what Professor Margaret Hu has aptly called “Big Data Blacklisting.”⁶⁷ Risk profiles can be shared with a host of federal and state agencies, impacting poor mothers’ opportunities, from government employment to immigration.⁶⁸

Poor mothers cannot avoid state surveillance by declining to seek government-assisted prenatal care. When the State learns that uninsured pregnant women are not getting prenatal care, it commences surveillance.⁶⁹ If a poor woman comes to a hospital for delivery and she has not been receiving prenatal care, then the hospital will likely hold the infant until the state inspects the mother’s home.⁷⁰ Child protective services will interrogate the mother to determine her competence to raise children absent the State’s intervention and

⁶⁵ Cf. Daniel J. Solove & Danielle Keats Citron, *Risk and Anxiety: A Theory of Data Breach Harms*, 96 TEX. L. REV. 737, 747-73 (2018) (discussing prevalence of data breaches today and judicial system’s difficulty in identifying their harm).

⁶⁶ See KAMALA D. HARRIS, CAL. DEP’T OF JUSTICE, CALIFORNIA DATA BREACH REPORT iv (2016) (noting that in California sixteen percent of breaches were within healthcare sector and involving medical information, including patient records and Social Security numbers); Citron, *supra* note 11, at 786-88 (discussing state attorney general’s offices’ responses to consumer privacy issues and noting that health privacy and data security are areas of focus for Massachusetts and Connecticut attorney general’s offices given “outgrowth of the high concentration of hospitals and insurance companies within their borders”).

⁶⁷ Margaret Hu, *Big Data Blacklisting*, 67 FLA. L. REV. 1735, 1735 (2016) (“‘Big data blacklisting’ is the process of categorizing individuals as administratively ‘guilty until proven innocent’ by virtue of suspicious digital data and database screening results.”).

⁶⁸ See Danielle Keats Citron & Frank Pasquale, *Network Accountability for the Domestic Intelligence Apparatus*, 62 HASTINGS L.J. 1441, 1443 (2011); Gray & Citron, *supra* note 4, at 80-81 (“Governmental data-mining systems have flagged innocent individuals as persons of interest, leading to their erroneous classifications as terrorists or security threats, intense scrutiny at airports, denial of travel, false arrest, and loss of public benefits.”).

⁶⁹ See, e.g., Khiara M. Bridges, *Privacy Rights and Public Families*, 34 HARV. J.L. & GENDER 113, 124-133 (2011) (discussing New York State Prenatal Care Assistance Program and noting that to receive benefits, women are required to divulge information regarding recent nutritional intake and undergo examinations including psychological assessments).

⁷⁰ See BRIDGES, *supra* note 20, at 9; see also *id.* at 131 (“The failure to receive prenatal care is a form of ‘neglect,’ and that justifies the state’s intervention into the family to ‘protect’ the child.”).

regulation.⁷¹ The State presumes that if poor mothers lack insurance, they cannot provide basic necessities for their children.⁷²

In short, the existential state of poor mothers is one of unavoidable state surveillance. If poor mothers accept government assistance for medical care, they lose their privacy. If poor mothers do not obtain Medicaid, they lose their privacy.⁷³ The “legal and social condition of poor mothers is one that is devoid of privacy—one in which state power surrounds them at all times, without regard to whether they receive public benefits.”⁷⁴

Poor mothers are denied privacy because the State assumes nothing valuable will come from their freedom from surveillance.⁷⁵ The State subjects poor mothers to surveillance because it views their character as suspicious.⁷⁶ Poor mothers are denied the “right to an inviolate personality,” as Samuel Warren and Louis Brandeis articulated the concept of privacy in their famous law review article *The Right to Privacy*.⁷⁷ State surveillance is designed to bring poor mothers “away from the margins of thought and behavior and toward the mainstream.”⁷⁸ As Professor Bridges explains, the poor mother’s lack of privacy is “not a function of [her] dependence on state aid; it is a function of [her] poverty.”⁷⁹

B. *Due Process Turn*

The Poverty of Privacy Rights considers the State’s surveillance of poor mothers in light of a series of cases in which the Supreme Court has tentatively recognized a constitutional right to information privacy.⁸⁰ In *Whalen v. Roe*,⁸¹ the Court raised the possibility that the Fourteenth Amendment’s Due Process Clause protects individuals against the improper collection, aggregation, or disclosure of their private information.⁸² In *Whalen*, a group of patients and

⁷¹ *See id.* at 10 (noting that if poor mothers refuse government assistance, they will still lose their privacy “because they will be unable to provide their children with basic necessities, thus making them vulnerable to a privacy-invading investigation”).

⁷² *See id.* at 9-10.

⁷³ *Id.* at 131.

⁷⁴ *Id.* at 10.

⁷⁵ *Id.* at 153 (“We want to prevent [poor mothers] from experimenting with behaviors that are unpopular or countercultural, as we do not trust that anything valuable will result from their experimentation.”).

⁷⁶ *See id.* at 154 (“[D]enying poor mothers privacy is a mechanism for bringing a problematized segment of society into conformity.”).

⁷⁷ Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 211 (1890).

⁷⁸ BRIDGES, *supra* note 20, at 154.

⁷⁹ *Id.* at 132.

⁸⁰ *See id.* at 157-58.

⁸¹ 429 U.S. 589 (1977).

⁸² *Id.* at 598-600.

doctors challenged a New York statute requiring the centralized collection of the names and addresses of individuals taking "Schedule II" drugs, for which there were legal and illegal markets.⁸³ The goal of the database was to help the State detect the diversion of drugs into illegal markets.⁸⁴ Plaintiffs argued the law illegitimately burdened their "individual interest in avoiding disclosure of personal matters."⁸⁵

In *Whalen*, the Court set the stage for the recognition of a right to information privacy: "The cases sometimes characterized as protecting 'privacy' have in fact involved at least two different kinds of interests. One is the individual interest in avoiding disclosure of personal matters, and another is the interest in independence in making certain kinds of important decisions."⁸⁶ The Court acknowledged: "the threat to privacy implicit in the accumulation of vast amounts of personal information in computerized data banks or other massive government files" arising from the "collection of taxes, the distribution of welfare and social security benefits, the supervision of public health, the direction of our Armed Forces, and the enforcement of the criminal laws."⁸⁷

The Court began by noting that the State's collection of prescription data was an "essential part of modern medical practice" though it did risk stigmatizing patients.⁸⁸ The Court upheld the statute, finding the State's interest in detecting drug crimes outweighed the Plaintiffs' privacy interest, because the Plaintiffs' data was adequately secured.⁸⁹ According to Justice Brennan's concurrence, had there been a real risk of disclosure to unauthorized individuals, the State's amassing of Plaintiffs' health data might have raised constitutional concerns.⁹⁰ The Court also noted the absence of evidence suggesting that the State's data collection chilled Plaintiffs from taking medicine.⁹¹

Since *Whalen*, the Supreme Court has suggested twice that a substantive due process right to informational privacy exists, but the law challenged in each case did not violate this right because safeguards prevented the unwarranted disclosure of personal information.⁹² In *National Aeronautics and Space Ad-*

⁸³ *Id.* at 595.

⁸⁴ *Id.* at 591-92.

⁸⁵ *Id.* at 599.

⁸⁶ *Id.* at 599-600.

⁸⁷ *Id.* at 605. In his concurrence, Justice Brennan similarly warned that "central storage and easy accessibility of computerized data vastly increase the potential for abuse of that information . . ." *Id.* at 607 (Brennan, J., concurring).

⁸⁸ *Id.* at 602 (majority opinion).

⁸⁹ *Id.* at 601-02 (noting that there is only "remote possibility" that the information will be inadequately protected, which is "not a sufficient reason for invalidating the entire patient-identification program").

⁹⁰ *Id.* at 606 (Brennan, J., concurring).

⁹¹ *Id.* at 604 (majority opinion).

⁹² BRIDGES, *supra* note 20, at 157-58 (discussing *Nixon v. GSA* and *NASA v. Nelson*).

ministration v. Nelson,⁹³ low risk contract employees at a government laboratory challenged background checks that required them to answer questions about their emotional health, drug treatment, and psychological counseling.⁹⁴ In *Nelson*, the Court held that the government's interests in managing its operations, combined with protections to secure the information, satisfied plaintiffs' "interest in avoiding disclosure' that may 'arguably ha[ve] its roots in the Constitution.'"⁹⁵ The Court underscored that the Privacy Act of 1974 adequately protected plaintiffs' information by requiring their written consent before disclosing it to third parties and by imposing criminal penalties for the unauthorized disclosure of their information.⁹⁶

Beyond the Supreme Court, lower courts have recognized a constitutional right to information privacy where the State has inappropriately disclosed individuals' personal data.⁹⁷ Some circuits have protected information implicating fundamental rights like family relationships, procreation, and contraception.⁹⁸ Others have protected information about which individuals enjoy a reasonable expectation of privacy.⁹⁹

For the most part, courts have refused to acknowledge—let alone balance—the harm caused by the State's collection of personal information.¹⁰⁰ Consider a due process challenge to a state law that required parents receiving government funding for childcare to submit finger scans when dropping off and picking up their children.¹⁰¹ In that case, the Plaintiff argued that submitting her finger scan in front of other parents and teachers was humiliating because it marked her as a welfare recipient.¹⁰² The Court refused to consider the stigma

⁹³ 562 U.S. 134 (2011).

⁹⁴ *Id.* at 138.

⁹⁵ *Id.* at 138 (quoting *Whalen*, 429 U.S. at 599).

⁹⁶ *Id.* at 147.

⁹⁷ BRIDGES, *supra* note 20, at 158 ("Although the Supreme Court has never announced definitively that a right to information privacy exists, the circuits have trudged ahead and recognized the right."). Courts generally engage in a balancing of interests to determine whether the government's interest is sufficiently important and narrowly tailored to compel the collection of personal data. *Id.* There is some variance among the circuits, however, as to whether burdens on this right are reviewed on the intermediate scrutiny or strict scrutiny standard. *See id.*

⁹⁸ *Id.* ("Some circuits only protect the privacy of information that implicates fundamental rights . . .").

⁹⁹ *Id.*

¹⁰⁰ *Id.* at 158 (arguing that current culture of blaming poor mothers for their situation has led to failure by courts to properly balance between privacy interest of individual and interest of government).

¹⁰¹ *Id.* at 159-60 (discussing how *Williams v. Berry*, 977 F. Supp. 2d 621 (S.D. Miss. 2013) failed to appreciate mother's interest in privacy).

¹⁰² *Id.* at 159 ("[B]ecause only beneficiaries of the Mississippi Child Care Payment Program were required to use the finger scanning technology, her status as a program beneficiary was disclosed to all those around her whenever she used the technology . . .").

caused by the State's collection efforts as implicating the constitutional right to information privacy.¹⁰³ For the Court, only the State's disclosure of the Plaintiff's finger scans to unauthorized third parties would implicate the right to information privacy.¹⁰⁴

Professor Bridges offers a thicker, more contextual conception of the constitutional right to information privacy than courts have recognized.¹⁰⁵ As Professor Bridges argues, courts should assess the State's collection of individuals' personal data, not just the subsequent disclosure of that personal data.¹⁰⁶ The State can infringe on a person's "right to be let alone" through its collection, aggregation, use, or disclosure of information.¹⁰⁷

Indeed, there are some aspects of a person's life in which the government has no legitimate interest and whose collection undermines self-respect and autonomy. Individuals have the right *not to be known* if the State's questions would demean and humiliate them for no good reason.¹⁰⁸ Privacy honors human dignity by conferring "respect for individual choice" and "respect for individuals because they have the capacity for choice."¹⁰⁹ "What makes a pursuit of information degrading does not turn on whether the information being pursued can be linked back to a specific individual or whether it is sensitive; rather, the degrading character of the pursuit turns on the assumptions made about the person that are motivating the interrogation."¹¹⁰

In the case of government-funded prenatal programs, crucial aspects of the State's interrogations have little to do with healthy parenting and much to do with the State's ability to control and demean poor mothers.¹¹¹ When the State demands to know a poor mother's history of abortion, sexual abuse, school ex-

¹⁰³ *Id.*

¹⁰⁴ *Id.*

¹⁰⁵ *Id.* at 154 (arguing that society gives privacy rights to practices that it values and that by not giving poor mothers more privacy protection, society implicitly suggests that their lives are not socially valuable).

¹⁰⁶ *See id.* at 162 (describing how courts frame issue as whether government can protect information from being released to unauthorized individuals).

¹⁰⁷ *Id.* (arguing that "it is degrading when the government asks the question and collects the information in the first instance"). As Justice Brandeis noted in a dissent, "the right to be let alone [is] the most comprehensive of rights and the right most valued by civilized men." *Olmstead v. United States*, 277 U.S. 438, 478 (1927) (Brandeis, J., dissenting).

¹⁰⁸ *Cf. BRIDGES, supra note 20* at 166 (describing how courts have not recognized "interest that individuals . . . have in avoiding these harms to dignity").

¹⁰⁹ Leslie Meltzer Henry, *The Jurisprudence of Dignity*, 160 U. PA. L. REV. 169, 208 (2011); *cf. Warren & Brandeis, supra note 77*, at 195, 198 ("The common law secures to each individual the right of determining, ordinarily, to what extent his thoughts, sentiments, and emotions shall be communicated to others. Under our system of government, he can never be compelled to express them (except when upon the witness-stand) . . .").

¹¹⁰ *BRIDGES, supra note 20*, at 162.

¹¹¹ *See id.* at 166 (displaying set of questions that women must answer for Medicaid that have little or nothing to do with health or parenting).

pulsions, and criminal convictions, it forces her to admit to a stigmatized social position.¹¹²

Even if poor mothers have nothing embarrassing to reveal, the State's interrogations are corrosive. They tell poor mothers that they are the *type* of people who are likely to have stigmatizing information to reveal. The poor mother "may experience the interrogation as doubly painful both because it facilitates social control while at the same time revealing her as the type of person that society wants to control."¹¹³

II. A NEW PRIVACY

The Poverty of Privacy Rights has the potential to shape the Supreme Court's understanding of substantive due process protections owed to vulnerable members of society. In an earlier age, the legal scholarship of Professor Charles Reich revolutionized our thinking about procedural due process protections afforded the indigent. Reich's *The New Property* and related work published in the 1960s called for a "Bill of Rights for the disenfranchised."¹¹⁴ In *Goldberg v. Kelly*,¹¹⁵ the Court embraced Reich's vision, recognizing procedural due process protections for the indigent whose public benefits were in jeopardy of termination.¹¹⁶ Though the Court has not taken up Reich's call for a constitutional right that would carve out a zone of privacy for the indigent,¹¹⁷ *The Poverty of Privacy Rights* charts a theory for such a right.

This Part explores the book's parallels to Reich's *The New Property*. It highlights the contributions that Professor Bridges makes to our understanding of the constitutional right to information privacy. *The Poverty of Privacy Rights* lays the groundwork for a "new privacy" by offering a more robust and contextual understanding of the privacy rights at stake. This Part ends with suggestions for the agenda at the heart of *The Poverty of Privacy Rights*, and urges us to look beyond the U.S. Constitution to address the erosion of privacy rights.

A. *The Scholarship of Charles Reich*

In 1964, Professor Charles Reich published *The New Property*, which poverty law scholar David Super has described as "one of the most influential arti-

¹¹² See *id.* at 167 (explaining how collecting private information from poor mothers can harm them even if they have nothing embarrassing to reveal).

¹¹³ *Id.* at 168.

¹¹⁴ Charles A. Reich, *The New Property*, 73 YALE L.J. 733, 760 (1964) (describing how oppressive government impairs individual's enjoyment of rights).

¹¹⁵ 397 U.S. 254 (1970).

¹¹⁶ *Id.* at 271 (requiring that decision-maker's conclusion as to welfare recipient's eligibility complies with certain procedural guidelines); see also Reich, *supra* note 114, at 783 (describing how procedure provides strong safeguard against arbitrary government action).

¹¹⁷ See Reich, *supra* note 114, at 785 ("[T]here must be a zone of privacy for each individual beyond which neither government nor private power can push—a hiding from the all-pervasive system of regulation and control.").

cles of the last century.”¹¹⁸ *The New Property* explored the power of the administrative state over individuals’ freedom.¹¹⁹ The State was a “gigantic siphon,” dispensing entitlements that often took the “form of rights or status rather than of tangible goods.”¹²⁰ As Reich explained, almost everyone received government entitlements, such as licenses, employment, contracts, tax breaks, and public benefits.¹²¹ The importance of those entitlements often exceeded that of traditional forms of wealth like homes or bank accounts.¹²²

Reich warned that the State acquired troubling power over citizens’ lives with the expansion of government entitlements.¹²³ The more government “hands out something of value, whether a relief check or a television license,” the more power it has to supervise that aspect of people’s lives.¹²⁴ The government investigated, monitored, and harassed recipients of its “largess[e].”¹²⁵ State interrogations were often expensive, embarrassing, and invasive.¹²⁶ The state could affix a “black mark” on recipients that would haunt them far into the future.¹²⁷ When subject to the State’s control, individuals had “no hiding place.”¹²⁸ Not even the home was sacred—agencies frequently conducted midnight raids of benefits recipients’ residences.¹²⁹ State surveillance and control impaired “individualism and independence.”¹³⁰

Individuals who defied the State’s conditions—no matter how arbitrary or invasive—could be punished with the suspension or revocation of government entitlements.¹³¹ Individuals could do little in response because entitlements

¹¹⁸ *Id.* at 744; see David A. Super, *The New New Property*, 113 COLUM. L. REV. 1773, 1779 (2013).

¹¹⁹ See Reich, *supra* note 114, at 733.

¹²⁰ *Id.* at 733, 737-38.

¹²¹ *Id.* at 739-46.

¹²² See *id.* at 738-39 (describing that sources of income or rights to receive income are primary form of wealth dispensed by government and how this can be most meaningful distinctive wealth that individuals possess).

¹²³ See *id.* at 746 (noting that when government offers entitlements, it begins to supervise entitlement recipients).

¹²⁴ *Id.*

¹²⁵ *Id.* at 749-50 (providing examples of agencies using their powers arbitrarily with constituents).

¹²⁶ See *id.* at 750 (explaining that use of surveillance alone would be enough to make people uncomfortable).

¹²⁷ *Id.* at 759-60.

¹²⁸ *Id.* at 760.

¹²⁹ See *id.* at 761 (explaining that Sunday mornings and after midnight were best for detecting fraud through unannounced visits).

¹³⁰ *Id.* at 733.

¹³¹ See *id.* at 747 (explaining that recipient’s moral character could be punished with denial of government largesse). For example, licenses were denied longshoremen because they had criminal records and mothers were denied aid for their children because of their alleged bad character. *Id.*

were treated like gifts or privileges that were conditional and subject to the state's discretion.¹³² For Reich, an antidote to the abuses of the "public interest state" would include the recognition of property rights in government entitlements.¹³³ Individuals needed to "possess, in whatever form, a small but sovereign island of his own" to protect their liberty.¹³⁴

Reich prescribed procedural and substantive protections of individuals' property interests in government entitlements. He argued that scrupulous observance of fair procedures was essential to restrain arbitrary government action.¹³⁵ Then too, government should be prevented from using its largesse to "buy up" rights guaranteed by the Constitution.¹³⁶ There should be "a zone of privacy for each individual beyond which neither government nor private power can push—a hiding place from the all-pervasive system of regulation and control."¹³⁷ Lastly, legislatures should ensure that the "regulation of largess[e]" does not "become a handle for regulating everything else."¹³⁸

Reich argued that vulnerable members of society warranted particular attention.¹³⁹ His scholarship argued that state power impacted groups differently, to the rich's benefit and the poor's disadvantage.¹⁴⁰ Welfare regulation "impose[d] a standard of moral behavior" that existed in no other area of government entitlement.¹⁴¹ It subjected the poor to surveillance amounting to a "deep invasion of [their] freedom."¹⁴² "It [was] only the poor whose entitlements, alt-

¹³² *Cf. id.* at 749 (noting that government could very easily rationalize increase in regulation to accompany new entitlements).

¹³³ *Id.* at 778.

¹³⁴ *Id.* at 774.

¹³⁵ *See id.* at 783 ("Action should be open to hearing and contest, and based upon a record subject to judicial review."). David Super explains that "[a]lthough Reich advocated developing [procedural] rules for governments' administration of largesse, he expressed great skepticism that they could rein in arbitrary power." Super, *supra* note 118, at 1780.

¹³⁶ Reich, *supra* note 114, at 779.

¹³⁷ *Id.* at 785.

¹³⁸ *Id.* at 782.

¹³⁹ *See id.* at 777 (arguing that abrogating rights of poor for "the public interest is no justification for the erosion of freedom that has resulted from the present system of government largess").

¹⁴⁰ *See id.* at 773 (discussing reforms in which corporations passed some power to government, creating system of "combined power" that "presses against the individual"). As Sarah Seo explains, Reich did not pay particular attention to how race or class "aggravated the problem of police discretion" in automobile stops. Sarah A. Seo, *The New Public*, 125 *YALE L.J.* 1616, 1645 (2016). However, he did acknowledge that "the police are far more likely to stop a Negro than a white man; far more likely to question a shabbily dressed man than one in an expensive suit." *Id.* (internal quotation marks omitted) (quoting Charles A. Reich, *Police Questioning of Law Abiding Citizens*, 75 *YALE L.J.* 1161, 1164 (1966)).

¹⁴¹ Reich, *supra* note 24, at 1247.

¹⁴² Reich, *supra* note 114, at 758.

though recognized by public policy, have not been effectively enforced.”¹⁴³ Too often, government entitlements for the poor were treated as “charity” rather than as “essentials, fully deserved.”¹⁴⁴

In *The New Property*, a companion piece to *Individual Rights and Social Welfare: The Emerging Legal Issues*, Reich argued that the recognition of property rights in public benefits was “urgently needed” to secure a “minimum basis for individual well-being and dignity.”¹⁴⁵ Public benefits were no different from government entitlements granted to wealthier segments of society.¹⁴⁶ They “aid security and independence” in the same way that professional licenses, farmers’ subsidies, and social security pensions do.¹⁴⁷ Eligibility safeguards for welfare benefits and limits on the “visitorial powers of the state” were essential to ensure the poor’s liberty and self-respect.¹⁴⁸

B. *Due Process Rights for the Poor*

Reich’s scholarship was profoundly influential. In *Goldberg v. Kelly*, decided in 1970, the Court addressed the procedures owed individuals before the State could terminate welfare benefits.¹⁴⁹ Justice Brennan, writing for the Court, made clear that low-income people had the same procedural rights as the affluent.¹⁵⁰ Citing Reich’s scholarship, the Court found that welfare benefits were property interests protected by the Due Process Clause.¹⁵¹ Low-income individuals had a right to notice and a meaningful opportunity to be heard before the termination of welfare benefits, the same as any other government entitlement.¹⁵² The Court held that public benefits were not charity or

¹⁴³ Reich, *supra* note 24, at 1255.

¹⁴⁴ *Id.*

¹⁴⁵ Reich, *supra* note 114, at 785-86.

¹⁴⁶ *See id.* at 785 (“The presumption should be that the professional man will keep his license, and the welfare recipient his pension.”).

¹⁴⁷ Reich, *supra* note 24, at 1255.

¹⁴⁸ *Id.* at 1256.

¹⁴⁹ *Goldberg v. Kelly*, 397 U.S. 254, 260 (1970).

¹⁵⁰ *Id.* at 262 (citing Reich’s articles).

¹⁵¹ *See id.* at 262-64 (noting importance of welfare to indigent persons that are qualified recipients). This is not to suggest that, following *Goldberg*, courts have been expansive in their understanding of the poor’s property rights, as Reich had hoped. As David Super explains, “[e]ven in procedural due process, defining which property rights are protected has proven continuously problematic.” Super, *supra* note 118, at 1828. The Court has had difficulty shedding “the distinction between rights and privileges.” *Id.* Then too, courts have struggled with “how much of the legal, social, and economic context that gives rights their meaning should be included in the definitions of rights.” *Id.* at 1829. Also, courts have “allowed legislatures to avoid creating property rights in public benefit programs with limitations that are substantive in name only.” *Id.*

¹⁵² *Goldberg*, 397 U.S. at 264 (requiring pre-termination evidentiary hearing to fulfill procedural due process requirements before welfare is terminated).

a “privilege,” but rather were a person’s property, such as state licenses, farmer subsidies, or corporate tax exemptions.¹⁵³

Reich’s call for procedural due process protections for the indigent was answered in *Goldberg*. The question remained as to whether substantive due process set limits on the State’s “all-pervasive” surveillance of the poor, as Reich had urged.¹⁵⁴ In *Whalen*, decided six years after *Goldberg*, the Court alluded to a right to information privacy.¹⁵⁵ *Whalen* and its progeny did not articulate a robust constitutional theory capable of addressing the pervasive surveillance of welfare recipients.¹⁵⁶

The Poverty of Privacy Rights is an important step towards a “bill of rights for the disinherited.”¹⁵⁷ It provides a theory on which a right to information privacy for the vulnerable can be built. It imagines a substantive due process right that would limit or prohibit a state’s collection of personal data that serves no justifiable purpose and erodes individual dignity and liberty.¹⁵⁸ It would “override the government’s interest in asking demeaning questions” if the answers would not advance the state’s legitimate interests.¹⁵⁹

A substantive right to information privacy, as developed in *The Poverty of Privacy Rights*, would have a structural impact. It would provide a “systemic-type remedy to address system-wide harms.”¹⁶⁰ It would say that poor mothers are citizens of the state, worthy of privacy and respect, rather than subjects of the State, deserving suspicion.¹⁶¹ Shielded from demeaning state interrogations, uninsured, poor mothers would be put on equal footing to insured,

¹⁵³ *Id.* at 262 n.8.

¹⁵⁴ Reich, *supra* note 114, at 785 (calling for “zone of privacy” to protect individuals from government’s control).

¹⁵⁵ See *Whalen v. Roe*, 429 U.S. 589, 605-06 (1977) (highlighting how duty to “avoid unwarranted disclosures” of certain personal information may have “its roots in the Constitution” but not deciding whether such disclosure would be unconstitutional).

¹⁵⁶ See Reich, *supra* note 24, at 1254 (“[T]he law has not yet developed a constitutional theory of privacy fully adequate to the present-day interdependent world.”).

¹⁵⁷ *Id.* at 1257.

¹⁵⁸ See BRIDGES, *supra* note 20, at 167 (“[I]f our courts were concerned about protecting the dignity of *all* individuals in the polity, then the Constitution might be interpreted to require that the state only collect information that is necessary to determine the level of benefits a person should receive and that facilitates her connection to other social services *only if she desires that connection*.”).

¹⁵⁹ *Id.* at 165.

¹⁶⁰ Hu, *supra* note 67, at 1797. Professor Margaret Hu argues that national security Big Data programs, such as the Terrorist Watch List and No Fly List, invade privacy on a mass, systemic scale and thus should be addressed with the systemic approach of substantive due process. See *id.* Her future scholarship will tackle the analytical framework of substantive due process for government’s big data scoring, ranking, and rating programs. See *id.* at 1798.

¹⁶¹ *Cf.* BRIDGES, *supra* note 20, at 166 (highlighting shame associated with forcing poor mothers to reveal personal information).

wealthier mothers who are not similarly interrogated.¹⁶² Preserving a poor mother's right to privacy would "produce an equality of treatment between poor and non-poor mothers, even when the narratives that are told about the two sets of mothers are far from equal."¹⁶³

A constitutional right to information privacy has the potential to impact democratic participation. Respecting privacy would further individual autonomy and democratic participation by ensuring that people see themselves as capable of self-governance.¹⁶⁴ The State would be precluded from engaging in interrogations that disenfranchise poor mothers more than they already are.

C. *Beyond the Constitution*

The Constitution is a crucial tool to address the erosion of the poor's privacy rights, but it is not the only tool. The tendency to reify the Constitution can prevent the pursuit of other fruitful avenues for reform.¹⁶⁵ Positive law, state constitutions, and corporate practices can help protect poor mothers' privacy and freedom as well.¹⁶⁶

A reform agenda should include the offices of state attorneys general. State enforcers have been active privacy norm entrepreneurs since the late 1990s.¹⁶⁷ They have pioneered baseline privacy norms to protect their citizens, relying on unfair and deceptive acts and practice ("UDAP") laws.¹⁶⁸ Several offices have devoted resources to investigating Big Data efforts that disadvantage the poor.¹⁶⁹ In my scholarship, I have called on state enforcers to "investigate unfair and deceptive uses of scoring algorithms given their potential to further marginalize vulnerable populations."¹⁷⁰

¹⁶² *Cf. id.* (calling attention to fact that wealthy mothers do not face same questioning and regulation as poor mothers).

¹⁶³ *Id.* at 169.

¹⁶⁴ See Brief for Elec. Privacy Info. Ctr. et al. as Amici Curiae Supporting Respondents, *Nat'l Aeronautics and Space Admin. v. Nelson*, 562 U.S. 134 (2011) (No. 09-530) (explaining that right to informational self-determination "prevents any processing of personal data that leads to an inspection of or an influence upon a person that is capable of destroying an individual capacity for self-governance").

¹⁶⁵ See, e.g., Danielle Keats Citron & Neil M. Richards, *Essential Preconditions to Digital Expression (You Won't Believe #3!)*, 95 WASH. U. L. REV. 1353, 1375-85 (2018) (discussing other avenues for reform).

¹⁶⁶ *Id.*

¹⁶⁷ See Citron, *supra* note 11, at 749 (outlining involvement of state attorneys general with privacy enforcement since the 1990s).

¹⁶⁸ *Id.* at 750-54 (giving overview of efforts of state attorneys general to enforce privacy norms).

¹⁶⁹ See *id.* at 809-10 (noting certain uses of big data that should be on agendas of state attorneys general, such as unfair and deceptive uses of scoring algorithms and cell phone apps for stalking).

¹⁷⁰ *Id.* at 810.

Although state attorney general (“AG”) privacy policymaking tends to focus on private uses of personal data, it can address the state’s aggregation of unnecessary and embarrassing personal data. State AG offices could look to state constitutions to challenge state regulations requiring the collection of extraneous—and stigmatizing—personal data from indigent mothers.

California’s AG office would have strong support for such a challenge.¹⁷¹ Article I of the California Constitution guarantees to all people the inalienable right to privacy.¹⁷² The privacy provision was added to the state constitution pursuant to a ballot initiative aimed to curtail overbroad and unnecessary collections of personal data.¹⁷³ The provision addressed the “accelerating encroachment on personal freedom and security caused by increased surveillance and data collection activity in contemporary society.”¹⁷⁴ As the California Supreme Court has held, the state needs to show a compelling interest to justify invading “autonomy-based privacy rights, particularly in the areas of free expression and association, procreation, or government-provided benefits in areas of basic human need.”¹⁷⁵ The California Supreme Court held that a law requiring public employees to submit to polygraph testing to investigate specific crimes violated employees’ privacy rights under the state constitution.¹⁷⁶

¹⁷¹ So too would private litigants. *See Soroka v. Dayton Hudson Corp.*, 1 Cal. Rptr. 2d 77, 86 (Ct. App. 1991) (finding that Target’s use of psychological profiling device that required job applicants to answer questions about religious beliefs and sexual orientation violated applicants’ privacy rights under state constitution).

¹⁷² CAL. CONST. art. I, § 1; *see also Sheehan v. San Francisco 49ers, Ltd.*, 201 P.3d 472, 479 (Cal. 2009) (holding that right to privacy applies to state actors and private parties).

¹⁷³ *See CAL. BALLOT PROPOSITIONS AND INITIATIVES, PROPOSITION 11: RIGHT OF PRIVACY 27* (UC Hastings Scholarship Repository 1972). California state senator James E. Whitmore opposed the initiative because he believed it would make it more difficult for the government to investigate welfare fraud. *Id.* at 27-28. The ballot’s key legislative proponents argued that “[p]roposition 11 will not prevent the government from collecting any information it legitimately needs. It will only prevent misuse of this information for unauthorized purposes and *preclude the collection of extraneous or frivolous information.*” *Id.* at 28 (emphasis added).

¹⁷⁴ *White v. Davis*, 533 P.2d 222, 233 (Cal. 1975).

¹⁷⁵ *Hill v. Nat’l Collegiate Athletic Ass’n*, 865 P.2d 633, 663 (Cal. 1994). The California Supreme Court has employed a balancing test, rather than strict scrutiny, when the privacy interest does not infringe on autonomy or when the data collection does not concern public benefits in areas of basic need. *Id.* at 678. For example, in *Lewis v. Superior Court*, 397 P.3d 1011 (Cal. 2017), the court upheld the state medical board’s access to a patients’ prescription records in an investigation of a doctor. The court held that even assuming the board’s actions constituted a serious intrusion on a legally protected privacy interest, the State’s access to the doctor’s prescription records was justified by their interest in protecting the public from the unlawful sale of dangerous drugs and protecting patients from negligent physicians. *Id.* at 1014.

¹⁷⁶ *Long Beach City Emps. Ass’n v. City of Long Beach*, 719 P.2d 660, 672 (Cal. 1986).

State attorneys general also can influence government data collection practices through the legislative process.¹⁷⁷ They could call for state legislation curtailing the collection of personal information from poor mothers. State legislatures should amend laws requiring poor mothers to answer demeaning questions that have nothing to do with prenatal care or successful parenting.¹⁷⁸

State legislation limiting the collection of personal data from poor mothers would be crucial for expressive reasons. Law is our teacher and guide.¹⁷⁹ It shapes social norms and behavior.¹⁸⁰ Revisions of state regulations would inform providers of state Medicaid programs that poor mothers should neither be suspected of, nor interrogated about, stigmatizing behavior. Changes in state laws could transform culture, which in turn could influence courts to interpret due process “to bestow equal privacy rights to poor and wealthier mothers.”¹⁸¹ As Professor Bridges explains, “if history is a teacher, poor mothers will only be granted privacy rights when cultural discourses around poverty shift as well.”¹⁸² State lawmakers can help root out the moral construction of poverty.

Another avenue of reform involves front line workers responsible for welfare surveillance. Social workers and medical staff are entrusted with the task of interrogating poor mothers.¹⁸³ Due to the moral construction of poverty, they may end up collecting far more personal data than the law requires.¹⁸⁴ Their interrogations of poor mothers can be deeply humiliating.¹⁸⁵ Bridges recalls an interview with a pregnant, poor woman who had several tattoos.¹⁸⁶ The first thing the doctor asked the woman was if her tattoo provider used clean needles.¹⁸⁷ The patient was devastated—the doctor’s question implied she was the type of person who would go to an unlicensed, back alley tattoo provider.¹⁸⁸

¹⁷⁷ Citron, *supra* note 11, at 758.

¹⁷⁸ See BRIDGES, *supra* note 20, at 2-6.

¹⁷⁹ See DANIELLE KEATS CITRON, HATE CRIMES IN CYBERSPACE 22-26 (2014) (arguing that legal reforms spearheaded by civil rights activists have resulted in societal change); Danielle Keats Citron, *Law's Expressive Value in Combating Cyber Gender Harassment*, 108 MICH. L. REV. 373, 407 (2009) [hereinafter Citron, *Law's Expressive Value*] (“Law creates a public set of meanings and shared understandings between the state and the public. It clarifies, and draws attention to, the behavior it prohibits. . . . Law educates the public about what is socially harmful.”).

¹⁸⁰ Citron, *supra* note 179, at 407.

¹⁸¹ BRIDGES, *supra* note 20, at 209-11.

¹⁸² *Id.* at 209.

¹⁸³ See *id.* at 163-65 (describing experience of interrogation and data collection of one pregnant black patient).

¹⁸⁴ See *id.* at 166-67 (describing wide range of information that would be gathered from such interrogations).

¹⁸⁵ See *id.* at 163-65.

¹⁸⁶ *Id.*

¹⁸⁷ *Id.* at 163.

¹⁸⁸ *Id.*

Hospitals should include the moral construction of poverty in its training of personnel. Staff should be taught about poverty bias and its corrosive impact on patient care. Had the doctor been aware of the tendency to impute bad character to poor mothers, the doctor might not have asked the needless and embarrassing questions about the woman's tattoo provider.

Progress is more likely if executives, lawmakers, and law enforcers view the protection of poor mothers' privacy rights as serving their interests. As Professor Derrick Bell has counseled, civil rights progress is most likely to occur when the interests of vulnerable people can be aligned with those in the dominant group.¹⁸⁹ Addressing poverty bias is in hospitals' interest because humiliating questions shake a patient's trust in medical providers.¹⁹⁰ Without trust, patients will be less inclined to share personal information essential for effective care. This lack of information can lead to bad medical outcomes and lawsuits, which hospitals and medical providers want to avoid.

Just as hospitals have some incentive to combat the moral construction of poverty, so too might state lawmakers and law enforcers. Data privacy is a pressing concern for constituents.¹⁹¹ The unraveling of privacy is underway in the health arena.¹⁹² Employers provide incentives to employees who agree to submit health data as part of wellness programs.¹⁹³ Employees who refuse to permit the collection of their health data are penalized because they are assumed to be withholding negative information, like a smoking habit.¹⁹⁴ Viewed

¹⁸⁹ See DERRICK BELL, AND WE ARE NOT SAVED: THE ELUSIVE QUEST FOR RACIAL JUSTICE 63-74 (1987) (explaining that progress on racial issues depends on ability to convince whites that they will benefit from social justice agenda); Danielle Keats Citron, *Cyber Civil Rights*, 89 B.U. L. REV. 61, 84-85 (2009) (heeding Professor Bell's advice and arguing that society suffers when law is brought to bear against online attacks that disproportionately impact women, people of color, and sexual minorities). Mary Anne Franks's important work has leveraged Professor Bell's interest convergence theory to argue that the emerging anti-surveillance sentiment should be transformed into what she calls "enlightened interest convergence" that would seek to protect the privacy interests of the vulnerable. Mary Anne Franks, *Democratic Surveillance*, 30 HARV. J.L. & TECH. 425, 430 (2016). As Professor Franks notes, 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." *Id.*

¹⁹⁰ See BRIDGES, *supra* note 20, at 163-65 (describing one woman's reluctance to go to doctor because of humiliation related to interrogation procedures).

¹⁹¹ See, e.g., Citron, *supra* note 11, at 786-90 (exploring how constituents have serious concerns about data breaches, identity theft, children's privacy, unwanted telephone calls, and other privacy and security issues).

¹⁹² Scott R. Peppet, *Unraveling Piracy: The Personal Prospectus and the Threat of a Full-Disclosure Future*, 105 NW. U. L. REV. 1153, 1155 (2011) ("The [healthcare] field has had the luxury of ignoring unraveling because technologies did not exist to make a signaling economy possible. Those days are over.").

¹⁹³ See *id.* at 1167-69 (discussing phenomenon of digital monitoring and employer programs to incentivize employees to participate by providing health information).

¹⁹⁴ See *id.* at 1156. Health insurance companies may insist upon the adoption of health monitoring technologies to pass on the costs of nonconforming behavior like smoking. See

in this way, everyone—from the poor to the affluent—may come to see that they could be subject to invasive data collection.

Ultimately, the protection of poor mothers' privacy rights could serve as a step towards the protection of everyone's privacy. It could force broader conversations about the data collection imperative, to which we now turn.

III. LAW, CONTEXT, AND RECIPROCITY

Rather than adopting technologies and techniques of perfect surveillance and asking questions later, a systematic review of the data collection imperative is in order. *The Poverty of Privacy Rights* brings into view several threshold questions. Should the data collection imperative be permitted to continue without end? What data collection efforts deserve careful study because they risk abuse and exact costs to dignity, liberty, and democracy?

This Part briefly considers these broader questions in light of the government's collection of personal data to protect against crimes, hazards, and terrorism. It discusses the role of the Fourth Amendment in limiting state surveillance designed to prevent and punish crimes and terrorism. Then, it considers the role of reciprocity in evaluating the data collection imperative.

A. *Technologies of Perfect Surveillance*

Since 9/11, government has significantly expanded surveillance over individuals' everyday lives. As Professor David Gray astutely observed in *The Fourth Amendment in the Age of Surveillance*, the goal “seems to be complete, pervasive surveillance of everywhere we go in virtual and physical space, everything we do, everything we say, and everything we think.”¹⁹⁵ Everyone is at risk of state surveillance given the detailed data trail continuously created about all of us.¹⁹⁶ The “National Surveillance State”—as Jack Balkin calls it—is “statistically oriented, *ex ante* and preventative, rather than focused on deterrence and *ex post* prosecution of individual wrongdoing.”¹⁹⁷

To illustrate domestic-surveillance techniques, government agents and private-sector partners collect and share information and intelligence through a network of fusion centers.¹⁹⁸ With an “all hazards, all crimes, all threats” man-

id. at 1168-69 (“Some employers have tracked employees' smoking habits even when the employees are away from their place of work. Some have fired employees who engage in behavior likely to raise the employer's health insurance costs.”).

¹⁹⁵ DAVID GRAY, *THE FOURTH AMENDMENT IN AN AGE OF SURVEILLANCE* 5 (2017).

¹⁹⁶ See FERGUSON, *supra* note 9, at 5 (warning that everyone is under surveillance and at risk of big data policing).

¹⁹⁷ Jack M. Balkin, *The Constitution in the National Surveillance State*, 93 MINN. L. REV. 1, 11 (2008).

¹⁹⁸ See Citron & Pasquale, *supra* note 68, at 1448 (defining “fusion centers” as “novel sites of intergovernmental collaboration that generate and share intelligence and information”).

date, “fusion centers cast a wide and indiscriminate net.”¹⁹⁹ Fusion centers utilize private entities to gather personal information for them.²⁰⁰ Data brokers specially design databases containing dossiers on hundreds of millions of Americans for “fusion centers.”²⁰¹ Data-mining tools analyze personal data culled from public and private databases, biometric data, social media posts, and public and private cameras.²⁰²

Governments employ technologies that continuously and indiscriminately collect personal data. For instance, cell site simulators, known as “stingrays,” “impersonate the cellular base stations that form the backbone of provider networks. . . . [T]hese devices can gather information from every cellular phone within their ranges of operation—often hundreds or thousands of phones at a time.”²⁰³ Cell site simulators enable law enforcement to “learn the unique identification numbers associated with each of these phones, their locations, and basic information about communications and callers.”²⁰⁴ For most city dwellers, being tracked by a cell site simulator is routine.²⁰⁵

The more power the State acquires with surveillance technologies and techniques, the more Americans need protections that check that power.²⁰⁶ State surveillance can lead to incorrect predictions about individuals that have a profound negative impact on their lives.²⁰⁷ As Reich warned fifty years ago, state surveillance can create a “black mark” on someone’s record from which one can never escape.²⁰⁸ It can demean and stigmatize, as *The Poverty of Privacy Rights* illustrated.²⁰⁹ It can interfere with projects of personal exploration, self-

¹⁹⁹ Danielle Keats Citron & David Gray, *Addressing the Harm of Total Surveillance: A Reply to Professor Neil Richards*, 126 HARV. L. REV. F. 262, 264 (2013) (citation omitted).

²⁰⁰ *See id.*

²⁰¹ *Id.*

²⁰² *See id.*

²⁰³ GRAY, *supra* note 195, at 4.

²⁰⁴ *Id.* at 5.

²⁰⁵ *Id.* (noting that neighborhoods designated as “high crime” areas are routinely monitored).

²⁰⁶ *Cf.* Citron & Pasquale, *supra* note 68, at 1444-55 (discussing how lack of oversight in domestic intelligence information sharing hubs erodes civil liberties); Richards, *supra* note 14, at 1952-58 (discussing potential injuries suffered by public as result of intellectual privacy infringement).

²⁰⁷ *See* Hu, *supra* note 68, at 1777-88 (discussing, for example, poor reliability of databases that inform screening protocols).

²⁰⁸ *See* Reich, *supra* note 114, at 759-80 (discussing consequences of criminal conviction). For thoughtful explorations of privacy harms in the digital age, see SOLOVE, *supra* note 5; DANIEL J. SOLOVE, *THE FUTURE OF REPUTATION: GOSSIP, RUMOR, AND PRIVACY ON THE INTERNET* (2007).

²⁰⁹ *See supra* notes 59-63 and accompanying text.

development, and democratic culture.²¹⁰ Government databases are subject to data breaches that risk considerable financial harm and cause anxiety.²¹¹ Massive state collections of personal data can metastasize to countless other databases run by federal, state, and local agencies.²¹²

A defining question is whether government will “protect[] individual dignity and conform[] both public and private surveillance to the rule of law.”²¹³ The Fourth Amendment stands as a “critical bulwark[]” against abusive state surveillance.²¹⁴ But legal doctrines have undermined the Fourth Amendment’s efficacy by allowing law enforcement to track individuals in public and to obtain third-party records without a warrant.²¹⁵ In *Carpenter v. United States*,²¹⁶ the Supreme Court reinvigorated the Fourth Amendment’s protections in finding that the government needed a warrant to obtain cell site location data from the defendant’s wireless carrier. For the Court, there was a qualitative difference between analog records and digital technologies. The Court underscored that cell phone location information generated by wireless carriers are “detailed, encyclopedic, and effortlessly compiled.”²¹⁷ The Court thus declined to extend the third-party doctrine to the case due to the “unique nature of cell phone location records.”²¹⁸ According to the Court, when the government “leverages the technology of a wireless carrier,” individuals have a legitimate expectation of privacy in the record of their physical movements in public.²¹⁹ The government conducted a search when it accessed cell site location data because the tracking technology enabled perfect surveillance of a person’s whereabouts far back in time.²²⁰ In concluding its findings, the Court harkened back to Justice

²¹⁰ See, e.g., Citron & Gray, *supra* note 199, at 269-70 (illustrating how technological information gathering “facilitates the sort of broad and indiscriminate surveillance that is characteristic of a surveillance state”).

²¹¹ See Solove & Citron, *supra* note 65, at 738 (outlining various types of harm that result from data breach).

²¹² See Citron & Pasquale, *supra* note 68, at 1484-87 (explaining scope of “network accountability” problem).

²¹³ Balkin, *supra* note 197, at 4.

²¹⁴ GRAY, *supra* note 195, at 69.

²¹⁵ See Balkin, *supra* note 197, at 19-20 (outlining various instances of government surveillance that were held to fall outside Fourth Amendment protection). A case decided by the Supreme Court this Term called into question the presumption that information collected by private parties can be provided to the government without Fourth Amendment restrictions. Brief of Scholars of the History and Original Meaning of the Fourth Amendment as Amici Curiae in Support of Petitioner, *Carpenter v. United States*, 138 S. Ct. 2206 (2018) (No. 16-402).

²¹⁶ 138 S. Ct. 2206 (2018).

²¹⁷ *Id.* at 2216.

²¹⁸ *Id.* at 2217.

²¹⁹ *Id.*

²²⁰ See *id.* at 2219-20.

Brandeis's prescient dissent in *Olmstead v. United States*,²²¹ which called for vigilance to ensure that the "progress of science" did not erode Fourth Amendment protections.²²²

Crucial to the Court's decision was the *method* of surveillance—whether digital technology permits "perfect surveillance" tantamount to the general warrant and writs of assistance that the Framers of the Fourth Amendment abhorred.²²³ In a series of articles, David Gray and I argued that the Fourth Amendment's protections are implicated when the government uses technologies or investigative techniques that facilitate a broad, continuous, and indiscriminate collection of personal data that intrudes upon reasonable expectations of quantitative privacy.²²⁴ The government's use of such technologies or techniques would amount to a "search," subject to the crucible of Fourth Amendment reasonableness, including judicially enforced constraints on law enforcement's discretion.²²⁵ The Supreme Court's decision in *Carpenter* affirmed the substance of our argument and found that the Fourth Amendment stands as a bulwark against technologies of perfect surveillance.

Might the constitutional right to *information privacy* serve as a check on surveillance technologies or techniques that facilitate broad, indiscriminate, and continuous *collection* of personal data? Due process would limit or block surveillance programs that serve no legitimate state purpose beyond the State's exertion of control over people's lives.²²⁶ Challenges to surveillance programs would face the classic argument that needles cannot be found without the haystack.²²⁷ Some surveillance programs, however, have been shown to produce

²²¹ 277 U.S. 438 (1928).

²²² *Carpenter*, 138 S. Ct. at 2223 (citing *Olmstead*, 277 U.S. at 473-474 (Brandeis, J., dissenting)).

²²³ See *id.* at 2218.

²²⁴ See Citron & Gray, *supra* note 199, at 270 (discussing history and significance of the term "reasonable expectation of privacy"); David Gray & Danielle Keats Citron, *A Shattered Looking Glass: The Pitfalls and Potential of the Mosaic Theory of Fourth Amendment Privacy*, 14 N.C. J.L. & TECH. 381, 404-05 (2013) (discussing effect of mosaic theory on traditional human surveillance); David Gray, Danielle Keats Citron & Liz Clark Rinehart, *Fighting Cybercrime After United States v. Jones*, 103 J. CRIM. L. & CRIMINOLOGY 745 (2013); Gray & Citron, *supra* note 4, at 71-72 ("Rather than asking how much information is gathered in a particular case, we argue here that Fourth Amendment interests in quantitative privacy demand that we focus on how information is gathered.").

²²⁵ See Gray & Citron, *supra* note 4, at 71-72.

²²⁶ See BRIDGES, *supra* note 20, at 156 (citing Supreme Court's openness to possibility that informational privacy is protected by due process).

²²⁷ See Citron & Pasquale, *supra* note 68, at 1450 (describing purpose of "fusion centers" devoted to detecting and preventing crimes and threats through analyzing information, which requires significant intelligence gathering).

little value, as the Privacy and Civil Liberties Oversight Board found of the NSA's bulk telephone records program.²²⁸

Professor Hu has argued that substantive due process should serve as a check on government's *use* of Big Data programs that deprive people of important rights.²²⁹ As Hu carefully documents, classified and non-classified government programs categorize individuals as "administratively 'guilty until proven innocent' by virtue of suspicious digital data and database screening results."²³⁰ As a result of "big data blacklisting," people are deemed ineligible to work, vote, and travel.²³¹ Hu contends that substantive due process should interrogate the "propriety of the mediation of a fundamental right in the first instance."²³² Hu's future work will explore whether a compelling state purpose justifies "big data blacklisting" programs that imperil liberty.²³³

The constitutional right to information privacy could serve as a check on government's collection and use of personal data in the national surveillance state.²³⁴ It raises important questions about the data collection imperative, which underlies government's use of technologies of perfect surveillance to investigate crimes, hazards, and terrorism. The data collection imperative is behind countless other surveillance projects in the private and public sector.²³⁵ Careful thought must be given to the benefits and costs of these projects and the need, if any, for judicial, legislative, or administrative constraints before their adoption.

²²⁸ PRIVACY & CIVIL LIBERTIES OVERSIGHT BD., REP. ON THE TEL. RECORDS PROGRAM 16 (2014) ("The Section 215 bulk telephone records program . . . has shown only limited value.").

²²⁹ See Hu, *supra* note 67, at 1797 (arguing that big data surveillance programs should be subject to strict scrutiny analysis and that "[t]he government must show that its reliance on big data is necessary and narrowly tailored to the use it is serving, and serves a compelling state interest").

²³⁰ *Id.* at 1747.

²³¹ *Id.* at 1735 (introducing concept of "big data blacklisting" and describing increasing use of databases to determine who can work, vote, and fly).

²³² *Id.*

²³³ See *id.* at 1798 ("[F]uture scholarship on this subject will explore the analytical framework of substantive due process in the context of the mass harms of big data blacklisting.").

²³⁴ See BRIDGES, *supra* note 20, at 133 (describing concept of "informational privacy" as possibly referring to individuals' ability to prevent government from disclosing information it has collected about citizens, and noting that informational privacy might enjoy constitutional protection).

²³⁵ See, e.g., PRIVACY AND CIVIL LIBERTIES OVERSIGHT BD., *supra* note 228, at 1 (describing NSA program designed to collect "millions of telephone records").

B. *Reciprocity*

Best practices and law often pair concerns about privacy with a commitment to transparency and accountability.²³⁶ That tradition is built on a commitment of reciprocity.²³⁷ When the State invades citizens' privacy, it owes citizens a reciprocal duty of transparency and accountability about its processes and decisions.²³⁸ The idea is to "watch the watchers."²³⁹ The Privacy Act of 1974²⁴⁰ and the Freedom of Information Act²⁴¹ embody the commitment of reciprocity for the administrative state.

There is a flip side to reciprocity. What happens as government shields its activities from view and loses any semblance of accountability? We have seen trends pointing in that direction. In some states, police disciplinary records are protected from public disclosure while criminal records plague citizens long after their time has been served.²⁴² Privatization often obscures what individual officials did or decided.²⁴³ State surveillance is certainly most troubling—and

²³⁶ See Citron & Pasquale, *supra* note 68, at 1471 ("America has a tradition of combining concerns about privacy with guarantees of government openness."). The Fair Information Practices are built on the idea that private and public entities handling personal information have reciprocal duties of transparency—that individuals have a right to know how their information is being handled; and accountability—that individuals can access personal records and correct inaccuracies. See Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1609, 1670-81 (1999).

²³⁷ The federal Privacy Act of 1974 is indeed "the most ambitious piece of federal legislation in the domain of information privacy[,] . . . the most comprehensive law that regulates processing and dissemination of information the government collects about individuals." Lior Strahelivitz, *Reunifying Privacy Law*, 98 CAL. L. REV. 2007, 2024 (2010).

²³⁸ This is a core commitment of procedural due process. See Danielle Keats Citron, *Technological Due Process*, 85 WASH. U. L. REV. 1249, 1258 (2008) (articulating new model of technological due process to guarantee transparency and accountability when automation threatens due process).

²³⁹ Citron & Pasquale, *supra* note 68, at 1471.

²⁴⁰ 5 U.S.C. § 552(a) (2012).

²⁴¹ 5 U.S.C. § 552(b)(6)-(7) (2012) (pairing transparency in government operations and processes with privacy protections for personnel and medical files and records compiled for law enforcement purposes).

²⁴² Kate Levine, *We Need to Talk About Police Disciplinary Records*, CITY SQUARE (Aug. 7, 2017), <http://urbanlawjournal.com/we-need-to-talk-about-police-disciplinary-records/> (noting, for example, that New York has statute protecting disciplinary records for individual police officers); see also Cynthia H. Conti-Cook, *Defending the Public: Public Accountability in the Courtroom*, 46 SETON HALL L. REV. 1063, 1074 (2016) (outlining heightened scrutiny that subpoenas for police records typically face when challenged in court); Stephen Rushin, *Police Union Contracts*, 66 DUKE L.J. 1191, 1228 (2017) (noting that handful of states have laws limiting public access to police disciplinary records and that police union contracts also limit even police chiefs' ability to view and use disciplinary records).

²⁴³ See JON D. MICHAELS, *CONSTITUTIONAL COUP: PRIVATIZATION'S THREAT TO THE AMERICAN REPUBLIC* 79-81 (2017) (summarizing effect of privatization on separation of

most hostile to the rule of law—when it amasses vast amounts of information about citizens while shrouding the State's operations in secrecy.²⁴⁴

As we take stock of the data collection imperative, concepts of reciprocity should inform our evaluation. Concepts of reciprocity force into consideration the disproportionate power acquired by government as it amasses reservoirs of personal data about each and every one of us.²⁴⁵ Might reciprocity demand that individuals have the right to be as unknown to government as it is to them?

Hints of a right not to be known have been recognized in some areas of the law. For instance, the Supreme Court supported the NAACP's efforts to keep its membership lists away from segregationist state and local officials, finding the right to avoid government scrutiny an integral part of the right of association.²⁴⁶

A right to be unknown would not be unlimited. Like other individual rights, it could be overcome by compelling, specific claims of public necessity or by an individual's deliberate waiver of her privacy. But requiring government to justify its surveillance or to show that individuals have surrendered their right to be unknown would have the effect of requiring more focused, and less intrusive, data gathering.²⁴⁷

CONCLUSION

The Poverty of Privacy Rights powerfully advances the project of securing privacy for the most vulnerable among us. It shows how the moral construction of poverty animates the State's surveillance of poor mothers, rather than legitimate concerns about prenatal care. State surveillance dispossesses poor mothers of their dignity and capacity for self-governance. Professor Bridges offers a

powers and noting that privatization can replace civil servants with for-profit contractors); Jon D. Michaels, *All the President's Spies: Private-Public Intelligence Partnerships in the War on Terror*, 96 CAL. L. REV. 901, 901 (2008) (highlighting novel nature of private-public partnership on intelligence gathering and informal nature of these relationships, which can help to evade oversight and law).

²⁴⁴ See Balkin, *supra* note 197, at 17 ("The more power the state amasses, the more Americans need constitutional guarantees to keep governments honest and devoted to the public good."). Frank Pasquale and I have suggested various ways to achieve accountability for the domestic intelligence apparatus. Technical standards should render the collection and sharing of personal data better subject to oversight and review. Citron & Pasquale, *supra* note 68, at 1471 (proposing "network accountability" technical standards to promote accountability in surveillance). Legal redress mechanisms ought to speed the correction of inaccurate information. See, e.g., *id.* An independent board of experts, such as a Civil Liberties Protection Board, should be charged with performing broad cost-benefit analysis of state surveillance, including a review of civil liberties and privacy protections.

²⁴⁵ See *supra* note 244 and accompanying text (discussing greater importance of accountability as governments gain more power).

²⁴⁶ NAACP v. Ala. ex. rel. Patterson, Attorney General, 357 U.S. 449, 466 (1958).

²⁴⁷ My current research is exploring the roles of reciprocity and fairness in data privacy law.

richer, contextual account of the constitutional right to information privacy that would limit the State's collection of personal data. Individuals have the right *not to be known* if the State's questions would demean and humiliate them for no good reason.

The Poverty of Privacy Rights provides an important lens for rethinking the data collection imperative more generally. It supplies a theory not only on which a right to information privacy can be built but also on which positive law and norms can develop. Concepts of reciprocity may provide another analytical tool to understand a potential right to be as unknown to government as it is to us.