

PRIVACY LAW'S ROLE IN AN INFORMATION ECONOMY

Sari Mazzurco[†]

What do we lose when we lose our privacy? A slew of recently enacted state laws suggest that the loss of privacy is merely a loss of individual choice in the market exchange of services for personal information. This Article argues that a loss of privacy risks something greater: the collapse of complex and fluid social identity. Without privacy, individuals cannot nurture their own senses of self because they are no longer free to try on different social roles across diverse relationships. Pervasive, private data collection threatens multifaceted selfhood by eliminating the boundaries that make social roles distinct and hindering the possibility of withdrawal from view.

If a loss of privacy entails a loss of our selves, how do we gain ourselves back? This Article argues the answer is in the “role” of privacy law in two senses. Normatively, it asserts online privacy law should work towards restoring the roleplay that underwrites social selfhood. Methodologically, it contends online privacy law should pursue that end through thoughtful “legal role-scripting.” Privacy lawmakers should be attentive to the social roles they ascribe to the data collectors and internet users law regulates. Legal role-scripts orient and pre-commit law in multiple ways. They establish a set of evaluative criteria that justify or undermine particular rights or responsibilities. They also direct courts to particular lines of legal precedent.

Following this understanding of privacy law's role, this Article uncovers a better way it can safeguard dynamic identity formation. It argues privacy governance law—an original legislative proposal—is better suited than alternative reforms to

[†] Assistant Professor of Law, SMU Dedman School of Law. The author thanks for their years of advice and guidance Robert Post, Jack Balkin, and Amy Kapczynski; and Dan Solove, Paul Schwartz, and Salomé Viljoen for their generous commentary. This Article has also benefitted from helpful feedback from participants in the Legitimacy in an Online World Conference at Yale Law School, the 2023 Lewis & Clark Fall Forum, Texas Junior Faculty Scholars Workshop, and the Yale Information Society Project community. The author also thanks the Glenn A. Portman Faculty Research Fund for its financial support. The views expressed in this Article are the author's own.

empower internet users to engage in self-constructive roleplay. It characterizes private, online data collection in terms of a governance relationship, with data collectors hegemonically deciding how they will collect and use internet users' personal information. Privacy law, in this formulation, works to afford internet users countervailing power to participate in collective decision-making about the privacy practices appropriate to their relationships with diverse data collectors. This offers internet users the greatest possibility of reclaiming emergent selfhood in an information economy.

TABLE OF CONTENTS

INTRODUCTION	125
I. PRIVACY AND THE SOCIAL SELF	129
A. <i>Social Roles in Everyday Life</i>	130
B. <i>Privacy, Identity, and Social Roles</i>	132
C. <i>Role-Relationships and Privacy Norms</i>	137
II. PRIVACY LAW'S ROLE-SCRIPTING FUNCTION	140
A. <i>Legal Role-Scripting</i>	141
B. <i>Privacy Law's Traditional Role-Scripting</i>	145
1. <i>Spousal Privacy</i>	146
2. <i>Healthcare Privacy</i>	148
3. <i>Postal Privacy</i>	149
4. <i>Privacy Torts</i>	151
C. <i>The Emergence of the Internet and the Business-Consumer Relationship</i>	153
III. REWRITING PRIVACY LAW'S ROLE-SCRIPTS	160
A. <i>Lessons for Reform from a Social Role Lens</i>	160
B. <i>Privacy Law Reform as Legal Role-Scripting</i>	162
1. <i>Data Protection</i>	163
2. <i>Information Fiduciaries</i>	169
C. <i>A Proposal for Privacy Governance</i>	175
CONCLUSION	181

INTRODUCTION

Since 2018, nineteen states have passed privacy laws aimed at protecting their residents' interests in an information economy.¹ Four states have active bills to do the same.² Though privacy reform at the federal level continues to exhibit its characteristic stagnation, state privacy law is in a period of ferment.

California ushered in the wave of state privacy law with its 2018 California Consumer Privacy Act. The states that have since passed their own privacy laws tended to follow California's lead, with substantive differences at the margins.³ All of these recent laws afford state residents "consumer rights" enforceable against the "businesses" that collect and use their information.⁴ They characterize personal information as a thing of value in an economic exchange.⁵ The role of privacy law, in this formulation, is to correct "market failures" that impede information transactions. The substance of legal protections is limited along those lines.

¹ See generally California Privacy Rights Act, CAL. CIV. CODE §§ 1798.100–199.100 (2020); Colorado Privacy Act, COLO. REV. STAT. §§ 6-1-1301 to -1313 (2021), amended by H.B. 24-1130, 74th Gen. Assemb., Reg. Sess. (Colo. 2024) (effective July 1, 2025), S.B. 24-41, 74th Gen. Assemb., Reg. Sess. (Colo. 2024) (effective Oct. 1, 2025); Connecticut Data Privacy Act, CONN. GEN. STAT. §§ 42-515 to -525 (2022); Delaware Personal Data Privacy Act, DEL. CODE ANN. tit. 6, §§ 12D-101 to -111 (2023) (effective Jan. 1, 2025); Kentucky Consumer Data Protection Act, H.B. 15, 2024 Gen. Assemb., Reg. Sess. §§ 1–9 (Ky. 2024) (effective Jan. 1, 2026); Indiana Consumer Data Protection Act, IND. CODE §§ 24-15-1-1 to -11-2 (2023) (effective Jan. 1, 2026); Iowa Consumer Data Protection Act, IOWA CODE §§ 715D.1–9 (2023) (effective Jan. 1, 2025); Maryland Online Data Privacy Act of 2024, S.B. 541, 432d Gen. Assemb., Reg. Sess. (Md. 2024) (effective Oct. 1, 2025); Minnesota Consumer Data Privacy Act, H.F. 4757, 93d Leg., Reg. Sess. (Minn. 2024) (effective July 31, 2025); Montana Consumer Data Privacy Act, MONT. CODE ANN. §§ 30-14-2801 to -2817 (2024); Nebraska Data Privacy Act, L.B. 1294, 108th Leg., 2d Sess. §§ 1–37 (Neb. 2024) (effective Jan. 1, 2025); New Hampshire Privacy Act, S.B. 255, 2024 Gen. Ct., Reg. Sess. (N.H. 2024) (effective Jan. 1, 2025); New Jersey Data Privacy Act, S.B. 332, 220th Leg., Reg. Sess. (N.J. 2024) (effective Jan. 15, 2025); Oregon Consumer Privacy Act, S.B. 619, 82d Gen. Assemb., Reg. Sess. §§ 1–15 (Or. 2023); Rhode Island Data Transparency and Privacy Protection Act, S. 2500, 2024 Gen. Assemb., Jan. Sess. (R.I. 2024) (effective Jan. 1, 2026); Tennessee Information Protection Act, TENN. CODE ANN. §§ 47-18-3301 to -3315 (2023) (effective July 1, 2025); Texas Data Privacy and Security Act, TEX. BUS. & COM. CODE ANN. §§ 541.001–541.205 (West 2023); Utah Consumer Privacy Act, UTAH CODE ANN. §§ 13-61-101 to -404 (West 2022); Virginia Consumer Data Protection Act, VA. CODE ANN. §§ 59.1-575 to -584 (2022).

² S.D. 745, 2023–2024 Leg., 193d Sess. (Mass. 2023); S.D. 1971, 2023–2024 Leg., 193d Sess. (Mass. 2023); Mass. H.D. 3245, 2023–2024 Leg., 193d Sess. (Mass. 2023); S.B. 659, 2023–2024 Leg., 102d Sess. (Mich. 2023); H.B. 345, 2023–2024, 135th Sess. (Ohio 2023); H.B. 1201, 2023–2024 Gen. Assemb., Reg. Sess. (Pa. 2023); H.B. 708, 2023–2024 Gen. Assemb., Reg. Sess. (Pa. 2023).

³ See *supra* note 1.

⁴ See *id.*

⁵ See *id.*

No state legislatures seem to have questioned whether this is the best role of privacy law—safeguarding individual choice by correcting “market failures” in an information economy. This Article asserts neglecting privacy law’s role—and the *social roles* privacy law scripts—are grievous oversights because they miss a core harm of the pervasive, private surveillance that sustains today’s information economy: the collapse of complex and fluid social identity.

The link between privacy, social roles, and identity formation is well-documented in sociological and legal scholarship. In 1934, George Herbert Mead argued people get to know who they are by playing a variety of social roles; privacy allows people, acting collectively, to set boundaries between different roles.⁶ Being a teacher, policymaker, father, and parishioner all entail different standards of personal revelation and restraint. Surveillance threatens multifaceted selfhood by eliminating the boundaries that make social roles distinct and hindering the possibility of withdrawal from view.⁷ Numerous legal scholars have since urged the importance of legal privacy protections because they “shelter [the] dynamic, emergent subjectivity” of selfhood.⁸ Yet, online privacy discourse so far has neglected to consider whether proposed legal reforms support the kind of roleplay that animates identity formation.

How do we gain our *selves* back in an information economy? This Article argues the answer lies in the “role” of privacy law in two senses. Normatively, it asserts online privacy law should work towards restoring the roleplay that underwrites social selfhood—that is, the role privacy law should play in rectifying a problematic social structure. Methodologically, it contends online privacy law should pursue that end through thoughtful “legal role-scripting.” This Article proposes a new legislative proposal for “privacy governance law” to satisfy these criteria.

“Legal role-scripting” refers to the way law contributes to the norms society attaches to different social roles. It is an overlooked but incredibly common expressive function of law. Law often assigns characteristics, rights, and responsibilities to the entities it regulates when they occupy particular roles (e.g., doctor, hospital, patient). For privacy law, legal role-scripting is so deep-rooted that it might be regarded as one of privacy law’s customary functions. Consider the evidentiary privileges for attorney-client relationships,⁹ psychotherapist-patient relationships,¹⁰

⁶ GEORGE HERBERT MEAD, *MIND, SELF & SOCIETY* xxii (U. Chi. Press 2015) (1934).

⁷ See *infra* notes 65–71 and accompanying text.

⁸ See, e.g., JULIE E. COHEN, *CONFIGURING THE NETWORKED SELF* 149 (2012); Anita L. Allen, *Coercing Privacy*, 40 *WM. & MARY L. REV.* 723, 754 (1999).

⁹ See FED. R. EVID. 502.

¹⁰ See FED. R. EVID. 501.

and spousal relationships,¹¹ and sectoral laws like the Health Insurance Portability and Accessibility Act¹² and the Family Educational Rights and Privacy Act.¹³ And, as Daniel Solove and Neil Richards have shown, the law of confidentiality historically protected expectations of trust and secrecy associated with particular relationships.¹⁴

The social role lens presents a functional vision of how privacy law operates—privacy rights and responsibilities as flowing from, and simultaneously shaping, societal expectations about particular social roles' appropriate information practices. Legal role-scripts orient and pre-commit law in multiple ways. They establish evaluative criteria that justify or undermine particular rights or responsibilities. They also direct courts to particular lines of legal precedent. For instance, the Supreme Court formerly refused to afford wives the right to volunteer adverse testimony against husbands, relying on a characterization of wives' subordinate marital role.¹⁵ In the process of assigning privacy rights and responsibilities to particular social roles, law also shapes *what it means to be* a spouse, patient, or student, and, by extension, those facets of individuals' identities.¹⁶

Turning to the information economy, the social role lens reveals the legal decision to orient online privacy protections around a “business-consumer” relationship as a key predicate to widespread private surveillance and stifled roleplay. When commercial use of the internet was still in its infancy, policymakers adopted a neoclassical “business-consumer” relationship to frame online privacy protections. Legal reliance on these roles has since spread to Federal Trade Commission (FTC) enforcement under Section 5 of the FTC Act and jurisprudence on generalist privacy laws like the Wiretap Act and state torts.¹⁷ In this view,

¹¹ See *Trammel v. United States*, 445 U.S. 40, 53 (1980) (holding confidential communications between petitioner and wife were privileged and inadmissible in a criminal case against petitioner).

¹² Health Insurance Portability and Accountability Act (HIPAA) of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (1996) (codified as amended in scattered sections of 18, 26, 29, and 42 U.S.C.).

¹³ Family Educational Rights and Privacy Act of 1974, Pub. L. No. 90-247, 88 Stat. 571 (codified as amended at 20 U.S.C. § 1232g).

¹⁴ Neil M. Richards & Daniel J. Solove, *Privacy's Other Path: Recovering the Law of Confidentiality*, 96 GEO. L.J. 123, 134–40 (2007).

¹⁵ *Hawkins v. United States*, 358 U.S. 74, 78–81 (1958).

¹⁶ See *supra* notes 9–15 and accompanying text.

¹⁷ Christopher W. Savage, *Managing the Ambient Trust Commons: The Economics of Online Consumer Information Privacy*, 22 STAN. TECH. L. REV. 95, 106, 126 (2019); Steven Hetcher, *Changing the Social Meaning of Privacy in Cyberspace*, 15 HARV. J.L. & TECH. 149, 162 (2001) [hereinafter Hetcher, *Social Meaning*]; Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 587, 596–97 (2014); Jessica Litman, *Information Privacy/Information Property*, 52 STAN. L. REV. 1283, 1288 (2000); James P. Nehf, *Recognizing the Societal Value in Information Privacy*, 78 WASH. L. REV. 1, 6, 46, 58 (2003); Allyson

consumers have idiosyncratic “preferences” about online privacy and they need information about businesses’ profit-driven information practices so that they can make informed self-interested decisions about the personal information they share.¹⁸ These roles justify the much-decried “notice-and-consent” approach that dominates online privacy law.¹⁹

The choice to orient online privacy around a business-consumer relationship set into motion a dynamic in which online intermediaries (including platforms like Facebook and Google, but also data brokers like Akamai, CoreLogic, and Epsilon) are empowered to make unilateral decisions about personal data collection and use. As Shoshana Zuboff documented, the freedom to make these sorts of decisions, coupled with the expectation that businesses rightfully pursue their profit interests, spurred a data collection and monetization imperative.²⁰ The possibility of privacy norms (i.e., notions of appropriate information practices) wither because “consumers” have no rightful claim to participate in businesses’ decision-making. And, as Julie Cohen explains, “surveillance . . . seeks to constitute individuals as fixed texts.”²¹ It thwarts the roleplay that fuels dynamic identity formation.

Regaining our selves in an information economy will require lawmakers to re-envision the *role* of privacy law, both in terms of the social roles privacy law chooses as its frame and how those role choices enable individuals to engage in roleplay across their diverse data collection relationships. There are multiple role-relationships other than a “business-consumer” relationship that could frame privacy rights and obligations. Not all are equally equipped to nurture identity formation. This Article argues “privacy governance law”—an original legislative proposal—is better suited than alternative reforms to empower internet users to engage in self-constructive roleplay. Privacy governance law characterizes private, online surveillance in terms of a governance relationship. It casts data collectors as “private governors” that hegemonically decide how they will collect and use internet users’ personal information, and internet users as “citizens” interested in collective autonomy—the ability to participate in governance that affects

W. Haynes, *Online Privacy Policies: Contracting Away Control Over Personal Information?*, 111 PENN. ST. L. REV. 587, 597–99, 607 (2007); 18 U.S.C. §§ 2510–2523.

¹⁸ See *infra* notes 205–212 and accompanying text.

¹⁹ See, e.g., Daniel J. Solove, *Introduction: Privacy Self-Management and the Consent Dilemma*, 126 HARV. L. REV. 1879, 1881–82 (2013). See generally Neil Richards & Woodrow Hartzog, *The Pathologies of Digital Consent*, 96 WASH. U. L. REV. 1461 (2019).

²⁰ See generally SHOSHANA ZUBOFF, *THE AGE OF SURVEILLANCE CAPITALISM* (2019).

²¹ Julie E. Cohen, *Privacy, Visibility, Transparency, and Exposure*, 75 U. CHI. L. REV. 181, 187 (2008).

their daily lives. Privacy law, in this formulation, works to afford internet users “countervailing power” to participate in collective decision-making about the privacy practices appropriate to their relationships with diverse data collectors.

Privacy governance law is a procedural remedy that targets a problematic social structure. It does not fully specify in advance the privacy obligations owed in any particular relationship between a data collector and internet users—deliberately so. It anticipates that these substantive obligations will be as heterogenous as the data collection relationships they bind, and they will emerge and change over the course of any given relationship. Privacy governance law’s capacious, power-conscious legal role-scripts nurture the sort of roleplay that invigorates a dynamic, emergent identity.

This Article proceeds in three Parts. Part I draws insights from social theory on privacy, roles, and identity formation to set the stakes of privacy law in an information economy. Part II introduces “legal role-scripting” as one of law’s expressive functions before describing privacy law’s longstanding role-scripting practices. It also traces the early legal decisions to adopt “business” and “consumer” roles to frame online privacy and critically examines how they fueled the erosion of privacy online to this day. Part III then turns to privacy law reforms. It presents the lessons policymakers and scholars can learn by viewing privacy law through a social role lens. It then scrutinizes two reform proposals—data protection and information fiduciary laws—in terms of the social roles they script and how they support roleplay in data collection relationships. Part III ends with an original legislative proposal for privacy law oriented around a privacy governance relationship. It asserts that “privacy governance law”—privacy law that serves a governance relationship—is better suited to reinvigorate identity-constructive roleplay in an information economy.

I. PRIVACY AND THE SOCIAL SELF

A robust literature recognizes the social value of privacy; that is to say how privacy supports relationships, communities, and individuals’ social personalities.²² Privacy serves these valuable social ends, in large

²² Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 STAN. L. REV. 1373, 1423–28 (2000); Daniel J. Solove, *Conceptualizing Privacy*, 90 CALIF. L. REV. 1087, 1116–18 (2002); Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 STAN. L. REV. 1193, 1212–20 (1998); Danielle Keats Citron & Frank Pasquale, *The Scored Society: Due Process for Automated Predictions*, 89 WASH. L. REV. 1, 10–18 (2014); Paul M. Schwartz, *Property, Privacy, and Personal Data*, 117 HARV. L. REV. 2055, 2087 (2004) [hereinafter Schwartz, *Property, Privacy*]; Julie E. Cohen, *What Privacy Is For*, 126 HARV. L. REV. 1904, 1908–10 (2013) [hereinafter Cohen,

part, by creating boundaries around and distance between the multiple social roles individuals play in everyday life. It allows people to develop multifaceted, complex identities by enabling them to play in and with different behavioral scripts. This Part presents social theory on privacy, roles, and identity formation to set the stakes of the work privacy law does when it scripts social roles. Privacy contributes to individuals' ongoing identity formation not only by allowing withdrawal from social interactions or absolute secrecy. Its role-based scripts of appropriate information practices also help constitute the multiple relationships that shape individuals' senses of self.

A. *Social Roles in Everyday Life*

Social roles, simply put, are the lenses through which individuals see others in the world.²³ As individuals go about their daily lives, they encounter others in particular social roles. These might include the mechanics who repair their cars, the protestors outside a business, or the friend who asks to meet for coffee. Social roles are not just "labels": they stand for the expectations society holds for actors' appropriate behavior, values, interests, and attributes in various contexts.²⁴ As Peter Berger and Thomas Luckmann put it, social roles are an "essential ingredient" of social reality because they give social interactions meaning and establish routine.²⁵

Individuals often perceive the meaning of others' actions based on whether they conform to or deviate from shared expectations, also called norms.²⁶ One might expect a car salesperson to ask a patron about their intended uses for a new car, and not their religious practices. And it is

What Privacy Is For]; Helen Nissenbaum, *Privacy as Contextual Integrity*, 79 WASH. L. REV. 119, 138–40 (2004); Neil M. Richards, *Intellectual Privacy*, 87 TEX. L. REV. 387, 407–09 (2008); PRISCILLA M. REGAN, LEGISLATING PRIVACY 213 (1995).

²³ GEORGE A. AKERLOF & RACHEL E. KRANTON, IDENTITY ECONOMICS 11 (2010).

²⁴ Frank Dobbin, *Economic Sociology*, in 21ST CENTURY SOCIOLOGY 319, 320 (Clifton D. Bryant & Dennis L. Peck eds., 2007); Ralf Dahrendorf, *Homo Sociologicus*, in ESSAYS IN THE THEORY OF SOCIETY 19, 35–37 (1968); NEAL GROSS, WARD S. MASON, & ALEXANDER W. MCEACHERN, EXPLORATIONS IN ROLE ANALYSIS: STUDIES OF THE SCHOOL SUPERINTENDENCY ROLE 59–60, 63 (1958); B.J. Biddle, *Recent Developments in Role Theory*, 12 ANN. REV. SOCIO. 67, 70–71 (1986); John Scott, *Status and Role: Structural Aspects*, in INTERNATIONAL ENCYCLOPEDIA OF THE SOCIAL & BEHAVIORAL SCIENCES 15095, 15095–96 (2001).

²⁵ PETER L. BERGER & THOMAS LUCKMANN, THE SOCIAL CONSTRUCTION OF REALITY 60–61, 74, 91 (Penguin Books 1991) (1966); Meir Dan-Cohen, *Between Selves and Collectivities: Toward a Jurisprudence of Identity*, 61 U. CHI. L. REV. 1213, 1218, 1228–29 (1994).

²⁶ Peter M. Hall, *A Symbolic Interactionist Analysis of Politics*, 42 SOCIO. INQUIRY 35, 38–40 (1972); Dahrendorf, *supra* note 24, at 44; Ralph H. Turner, *Role Theory*, in HANDBOOK OF SOCIOLOGICAL THEORY 233, 235 (Jonathan H. Turner ed. 2001).

reasonable to expect a car salesperson to know about different car models' distinguishing features, but it would be unreasonable to expect them to have a master's degree in Russian literature. If a salesperson does not meet these expectations, it is reasonable to regard their conduct as "unusual" and potentially consider them a "bad" salesperson.

Roles also help individuals figure out how to treat one another.²⁷ A salesperson should know, because of their social role and that of their patrons, that they should not probe their patrons' religious practices. If an individual internalizes a social role by embracing it as a benchmark for their conduct, they are more likely to comply with its norms and spread it in society.²⁸

All individuals occupy multiple social roles. Together, these roles help constitute a person's social identity.²⁹ Someone might be a mother, professor, tenant, sister, customer, and religious parishioner, among other things. Meir Dan-Cohen writes that as these roles interrelate within an individual, they "form[] together a relatively dense, cohesive, stable core" that helps shape who the individual considers herself to be.³⁰

Groups of individuals can also play social roles collectively, as a single organization. One might envision, for instance, the ways it is appropriate for the military to collect information (about citizens, non-citizens, and servicemembers), discipline officers, or regulate servicemembers' speech. And it would be reasonable to expect the military, a school, and a news organization to collect information quite differently on the basis of their different social roles.

Role-relationships also tend to contain a particular power structure. Though some relationships may invoke expectations of equality—like the relationship between friends—others involve asymmetry along various lines.³¹ Parent-child, teacher-student, employer-worker, and democratic government-citizen relationships involve power levers that are often specific to the role-relationship. An employer might have the power to

²⁷ Hall, *supra* note 26, at 39–40, 55; Turner, *supra* note 26, at 235.

²⁸ See Hall, *supra* note 26, at 38; BERGER & LUCKMANN, *supra* note 25, at 74; Dahrendorf, *supra* note 24, at 56.

²⁹ WILLIAM LITTLE, INTRODUCTION TO SOCIOLOGY 223 (2d Can. ed. 2016) (2013); Dahrendorf, *supra* note 24, at 43; Dan-Cohen, *supra* note 25, at 1219; Eric J. Mitnick, *Law, Cognition, and Identity*, 67 LA. L. REV. 823, 828, 865 (2007).

³⁰ Dan-Cohen, *supra* note 25, at 1219; see also Dan Solove, *The Virtues of Knowing Less: Justifying Privacy Protections Against Disclosures*, 53 DUKE L.J. 967, 1038 (2003) (describing complex multifaceted personality to dismantle distinction between "public" and "private" self [hereinafter Solove, *Virtues of Knowing Less*]).

³¹ Peter M. Hall, *Asymmetric Relationships and Processes of Power*, in FOUNDATIONS OF INTERPRETIVE SOCIOLOGY: ORIGINAL ESSAYS IN SYMBOLIC INTERACTION 309, 310 (1985); Dobbin, *supra* note 24, at 320; JEFFREY K. HASS, ECONOMIC SOCIOLOGY 9 (2d ed. 2020); NEIL FLIGSTEIN, THE ARCHITECTURE OF MARKETS 28 (2018); David Ardit, *Digital Hegemony*, in THE DIALECTIC OF DIGITAL CULTURE 13 (David Ardit & Jennifer Miller eds., 2019).

coerce workers' behavior by threatening termination, but workers may also have power over their employer by threatening to unionize or stop work.

Social roles typically arise through a process of continuous interaction in society, between and among individuals, organizations, governments, and others.³² The process is dialectic; individuals and groups persistently clash over what social roles are and the norms that should characterize them.³³ Even so, social roles and their associated norms are typically well-known and they serve as the assumed, background rules of individual behavior.³⁴ Forms of sanctions, including social shaming and ostracism, rewards, and legal penalties, help sustain current meanings.³⁵ For instance, someone can understand what it means to be a military servicemember even if they never interact with one because they have access to cultural knowledge about a servicemember's typical attributes and behaviors. With that knowledge, they can also push back against existing role-based norms. The decades-long effort to repeal Don't Ask Don't Tell (DADT) fought against discriminatory norms that it was unacceptable for servicemembers to be gay.

Overall, social roles are a core organizing feature of social life. They help actors navigate otherwise uncertain interactions, contribute to individuals' senses of self, and generate specific kinds of social order. And, as the next subparts explain, social roles both depend on privacy for their existence and enable important forms of privacy to exist.

B. *Privacy, Identity, and Social Roles*

The social practice of privacy, especially as it relates to roleplaying, is essential to individuals' identity formation and continual reformation. Privacy literature historically separated concepts of privacy and identity into "liberal" and "social" accounts.³⁶ But, since the 1990s, more complex

³² HASS, *supra* note 31, at 9; Mark Granovetter, *Economic Action and Social Structure: The Problem of Embeddedness*, 91 AM. J. SOCIO. 481, 486 (1985); FLIGSTEIN, *supra* note 31, at 27–28.

³³ BERGER & LUCKMANN, *supra* note 25, at 60–61. Ideas about social roles may also differ dramatically between different communities. One could imagine, for instance, Christian ideas of what it means to be a parent, father, or mother diverging from secular ideas about these roles.

³⁴ FLIGSTEIN, *supra* note 31, at 27.

³⁵ Dahrendorf, *supra* note 24, at 38, 42–43.

³⁶ Anuj Puri, *A Theory of Group Privacy*, 30 CORNELL J.L. & PUB. POL'Y 477, 498–505 (2021); Allen, *supra* note 8, at 739–40; Stuart Hargreaves, 'Relational Privacy' & Tort, 23 WM. & MARY J. WOMEN & L. 433, 444–60 (2017); Valerie Steeves, *Reclaiming the Social Value of Privacy*, in LESSONS FROM THE IDENTITY TRAIL: ANONYMITY, PRIVACY AND IDENTITY IN A NETWORKED SOCIETY 192–93 (Ian Kerr, Valerie Steeves & Carole Lucock eds., 2009); Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1609, 1648–54 (1999) [hereinafter Schwartz, *Privacy and Democracy*]; ALAN F. WESTIN, *PRIVACY AND FREEDOM* 24, 26 (1967); Mark Burdon,

accounts have demonstrated that “liberal” and “social” privacy together contribute to the emergence of the self.³⁷

Alan Westin's *Privacy and Freedom* encapsulates the liberal account. He defined privacy as “the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others.”³⁸ He identifies privacy with autonomy—the exercise of control over information as a form of self-determination. Individual exercises of privacy amount to removal from social gaze, with isolation as the pinnacle.³⁹ This account aligns with what Michael Sandel describes as the “new” privacy, which requires the government and others to let individuals alone to make important decisions.⁴⁰

By contrast, fully social accounts portray privacy within networks of social relationships.⁴¹ The self is an “ever-changing construct that is intersubjectively created and negotiated in the process of social interaction.”⁴² According to George Herbert Mead, the individual acquires their sense of self by taking others' points of view and recognizing themselves as the object of others' view.⁴³ Social theorist Valerie Steeves adds that “the social negotiation of a desired boundary between self and other” can only be achieved through interaction and

Contextualizing the Tensions and Weaknesses of Information Privacy and Data Breach Notification Laws, 27 SANTA CLARA COMPUT. & HIGH TECH. L.J. 63, 67–71 (2011); Robert H. Sloan & Richard Warner, “I'll See”: *How Surveillance Undermines Privacy by Eroding Trust*, 32 SANTA CLARA HIGH TECH. L.J. 221, 245–46 (2016) [hereinafter Sloan & Warner, “I'll See”]; Charlotte A. Tschider, *Meaningful Choice: A History of Consent and Alternatives to the Consent Myth*, 22 N.C. J.L. & TECH. 617, 664–67 (2020); Katrin Schatz Byford, *Privacy in Cyberspace: Constructing a Model of Privacy for the Electronic Communications Environment*, 24 RUTGERS COMPUT. & TECH. L.J. 1, 6–9 (1998); Mark MacCarthy, *Privacy Policy and Contextual Harm*, 13 I/S: J.L. & POL'Y INFO. SOC'Y 399, 405–08 (2017). “Liberal” in this application refers to liberal political philosophy that characterizes persons by their separateness. See JOHN RAWLS, *A THEORY OF JUSTICE* 33–34 (1971); ROBERT NOZICK, *ANARCHY, STATE, AND UTOPIA* 36, 38 (Blackwell Publishers 1999) (1974).

³⁷ Allen, *supra* note 8, at 754; Steeves, *supra* note 36, at 203–08; Robert C. Post, *The Social Foundations of Privacy: Community and Self in the Common Law Tort*, 77 CALIF. L. REV. 957, 969–74 (1989) [hereinafter Post, *Social Foundations*].

³⁸ WESTIN, *supra* note 36, at 7.

³⁹ *Id.* at 40–41.

⁴⁰ MICHAEL J. SANDEL, *DEMOCRACY'S DISCONTENT: AMERICA IN SEARCH OF A PUBLIC PHILOSOPHY* 97 (1996).

⁴¹ Puri, *supra* note 36, at 498–500; Hargreaves, *supra* note 36, at 460–63; see also Paul M. Schwartz, *Privacy and Participation: Personal Information and Public Sector Regulation in the United States*, 80 IOWA L. REV. 553, 559–60 (1995) (articulating a social vision of privacy that pursues individual capacity for decision-making requisite to a democratic society).

⁴² Byford, *supra* note 36, at 15.

⁴³ *Id.* at 15–16 (citing MEAD, *supra* note 6, at 138); Steeves, *supra* note 36, at 204 (citing Jürgen Habermas, *Individuation Through Socialization: On George Herbert Mead's Theory of Subjectivity*, in POSTMETAPHYSICAL THINKING: PHILOSOPHICAL ESSAYS 149, 176 (William Mark Hohengarten trans., MIT Press 1992) (1988)).

information-sharing.⁴⁴ Norms that emerge about what information one should share and how others may use it partly constitute each relationship by distinguishing it from others.⁴⁵ And, unlike the liberal account, when someone shares information in a manner that aligns with these norms, they do not surrender their privacy.⁴⁶ Instead, they practice privacy by demonstrating they trust their counterpart to use that information appropriately.

Social accounts recognize the importance of social roles to identity formation. Mead argues individuals “com[e] to know [them]selves [by] . . . play[ing] a variety of social roles.”⁴⁷ “By trying on [social] roles and seeing them reflected back at us through our social interactions with others, we come to know who we are.”⁴⁸ Privacy norms that vary between different role-relationships allow individuals to distinguish one role from the next.⁴⁹ They enable individuals to form multidimensional identities by performing multiple social roles.⁵⁰

The complex account of privacy’s contribution to identity formation embeds the autonomous individual in a dense social life. Anita Allen writes, “[P]ersons a[re] shaped partly and substantially by social forces not of their own choosing, but also and importantly by their own choices.”⁵¹ Networks of social relationships are a predicate to the exercise of autonomous choice. In a sense, this is obvious. Privacy as the choice to insulate oneself from others presumes there are relationships from which one may withdraw.

But, as Robert Post explains, the social norms that give a relationship its shape and individuals’ autonomous decisions to reveal or withhold information within a relationship together constitute community and individual identity.⁵² An individual’s decision to reveal information within a particular relationship is an act of intimacy; the counterpart’s decision to comply with a relationship’s privacy norms conveys respect for the person with whom they are dealing.⁵³ A child who comes out to their parent as transgender signals trust, closeness, and intimacy with the parent; the parent who decides not to reveal their child’s gender identity

⁴⁴ Steeves, *supra* note 36, at 207.

⁴⁵ MacCarthy, *supra* note 36, at 400–01; Steeves, *supra* note 36, at 208; Puri, *supra* note 36, at 503–04.

⁴⁶ Steeves, *supra* note 36, at 207.

⁴⁷ *Id.* at 205.

⁴⁸ *Id.*

⁴⁹ *Id.*; MacCarthy, *supra* note 36, at 400–01.

⁵⁰ Richard Warner & Robert H. Sloan, *Self, Privacy, and Power: Is It All Over?*, 7 TULANE J. TECH. & INTELL. PROP. 61, 67–69 (2014).

⁵¹ Allen, *supra* note 8, at 753–54.

⁵² Post, *Social Foundations*, *supra* note 37, at 959.

⁵³ *Id.* at 973.

to the child's school (without the child's approval) conveys respect for their child's autonomous personhood. The acts of voluntarily divulging information about oneself and complying with the relationship's social norms—living in the relationship—contribute to the formation of identities that are at once socially and individually constituted.

Privacy and roleplaying are closely connected when it comes to the practice of identity formation. As the earlier subpart explained,⁵⁴ social roles make interactions meaningful by communicating the norms relevant to a particular relationship. And when individuals perform social roles or rail against them, they express aspects of their identity.⁵⁵ Social roles are interdependent with “liberal” and “social” privacy. Privacy helps individuals move through different social roles by helping to distinguish one role from another based on their norms (social privacy) and enabling individuals to autonomously withdraw from a particular role and enter another (liberal privacy).⁵⁶ Liberal privacy allows individuals to modulate their exposure within a network of relationships so that they can move from one role to the next;⁵⁷ social privacy communicates what kinds of exposure are appropriate within each role.⁵⁸ Bruce Schneier writes: “Privacy isn't about hiding something. It's about being able to control how we present ourselves to the world.”⁵⁹ Choosing to perform social privacy in different role-relationships helps a social identity flourish.⁶⁰

The ability to autonomously modulate exposure also provides individuals some freedom to retreat from role-based obligations and expectations. Allen writes, “The formation of self-concept and intimate relationships . . . requires opportunities for privacy and private choice. Privacy is down time. . . . Privacy is also a matter of freedom to escape, reject, and modify [my] identities.”⁶¹ Privacy provides individuals with “breathing room” to not have to live up to particular social roles'

⁵⁴ See *supra* Section I.A.

⁵⁵ See Solove, *Virtues of Knowing Less*, *supra* note 30, at 1037.

⁵⁶ Puri, *supra* note 36, at 499–505; Allen, *supra* note 8, at 753–55; Byford, *supra* note 36, at 15–18; MacCarthy, *supra* note 36, at 407–09; Sloan & Warner, “I'll See,” *supra* note 36, at 245–46; Hargreaves, *supra* note 36, at 460–63.

⁵⁷ Hargreaves, *supra* note 36, at 476.

⁵⁸ See *supra* notes 41–50 and accompanying text.

⁵⁹ Bruce Schneier, *The Security Risks of Third-Party Data*, SCHNEIER ON SECURITY: CRYPTOGRAM (Sept. 15, 2015), <https://www.schneier.com/crypto-gram/archives/2015/0915.html> [<https://perma.cc/AN5T-YCST>]. Dan Solove has observed that privacy laws also aid role-switching and withdrawal. Solove, *Virtues of Knowing Less*, *supra* note 30, at 1037.

⁶⁰ MacCarthy, *supra* note 36, at 407–08, 419; Robert H. Sloan & Richard Warner, *Relational Privacy: Surveillance, Common Knowledge, and Coordination*, 11 U. ST. THOMAS J.L. & PUB. POL'Y 1, 9–10 (2017).

⁶¹ Allen, *supra* note 8, at 739, 754.

behavioral norms.⁶² And when individuals take this distance from their social roles, they have the opportunity to reflect on them and, potentially, figure out how to redefine them.⁶³ Privacy powers the dialectic that keeps social roles dynamic. Woven together, social privacy and liberal privacy help individuals construct a complex and multidimensional identity by performing, rejecting, or modifying the numerous roles they play as they go about their daily lives.⁶⁴

A key feature of this Article's complex account of privacy, role, and identity is that it maintains and nurtures the fluidity of identity. Individuals continually form and reform their identities as they interact in society. Some of these interactions take place in particular social roles and others in a state of withdrawal or opposition. All the while, social roles change along with actors' actual behaviors in particular relationships.

Surveillance undermines all of that. It erodes individuals' ability to engage in the play necessary to constitute their identities.⁶⁵ Erving Goffman's studies of total institutions, such as prisons and asylums, demonstrate that the deprivation of privacy destroys individuals' sense of self.⁶⁶ Not only do total institutions "mortif[y]" the self by exposing every aspect of one's life to others, they disrupt individuals' ability to keep their various roles separate.⁶⁷ Daniel Solove adds that excessive disclosures about people "can often be jarring, for they display people out of the particular context in which others may know them."⁶⁸ Actions in the context of one role are not separated from actions in the context of other roles, and so individuals are "constantly confronted with inconsistencies in their behavior and [a]re fully accountable to the same people for all aspects of behavior."⁶⁹ Jeffrey Reiman writes that data surveillance replicates total institutions' privacy deprivations by making individuals'

62 Bert-Jaap Koops, *Privacy Spaces*, 121 W. VA. L. REV. 611, 630 (2018) (quoting ROBERT SOMMER, *PERSONAL SPACE* 26 (1969)); Burdon, *supra* note 36, at 113; Byford, *supra* note 36, at 24–25; McCarthy, *supra* note 36, at 411.

63 Allen, *supra* note 8, at 740.

64 See Solove, *Virtues of Knowing Less*, *supra* note 30, at 1037 ("Selfhood is a process of growth and development, not a fixed state of being.").

65 Hargreaves, *supra* note 36, at 451; Sloan & Warner, "I'll See," *supra* note 36, at 225–29.

66 Erving Goffman, *On the Characteristics of Total Institutions*, in *ASYLUMS: ESSAYS ON THE SOCIAL SITUATION OF MENTAL PATIENTS AND OTHER INMATES* 1, 6, 23–32 (Routledge 2017) (1961).

67 *Id.* at 14–16. Paul Schwartz adds that surveillance undermines individuals' "capacity for free choice": "[T]he more that is known about an individual, the easier it is to force his obedience." Schwartz, *Privacy and Participation*, *supra* note 41, at 560.

68 Solove, *Virtues of Knowing Less*, *supra* note 30, at 1038.

69 IRWIN ALTMAN, *THE ENVIRONMENT AND SOCIAL BEHAVIOR* 40 (1975).

lives visible without the authority to withdraw from view.⁷⁰ Worse still, it replaces the complex dynamic of identity formation with a static concept of identity as a set of acontextual data about an individual.⁷¹

C. *Role-Relationships and Privacy Norms*

Privacy contributes to individuals' identity formation because of the social practice it entails. Privacy involves acts of intimacy and trust through revelations of personal information,⁷² acts of respect when someone fulfills social privacy expectations,⁷³ play in multiple social roles,⁷⁴ and withdrawal from particular roles.⁷⁵

Social roles are a central, organizing feature of privacy relationships. Beyond the connection between roleplay and identity formation, notions of what acts constitute intimacy or respect typically depend on the social roles participants play in any given interaction. As Erving Goffman writes, “[T]he very forms of behavior employed to celebrate and affirm relationships—rituals such as greetings, enquiries after health, and love-making... would be a violation... if performed between wrongly related individuals.”⁷⁶ Individuals typically navigate privacy expectations in terms of the social roles they and others happen to play. They also often perceive privacy violations based on their social role.

Helen Nissenbaum's influential work on privacy as a form of “contextual integrity” carefully lays out how context typically shapes the practice of privacy.⁷⁷ Contextual integrity refers to compliance with the informational norms that apply in a given context. Nissenbaum relies on a social account of privacy, viewing it as the right to the appropriate flow of personal information considering existing social norms.⁷⁸ There are “four key parameters” of “context-relative informational norms”: the “context” (or the social structure), the “actors” who participate in the exchange, the “attributes” of the information exchanged, and the

⁷⁰ Byford, *supra* note 36, at 52 (citing Jeffrey H. Reiman, *Driving to the Panopticon: A Philosophical Exploration of the Risks to Privacy Posed by the Highway Technology of the Future*, 11 SANTA CLARA COMPUT. & HIGH TECH. L.J. 27, 39 (1995)).

⁷¹ Puri, *supra* note 36, at 490–94; Steeves, *supra* note 36, at 206.

⁷² Ari Ezra Waldman, *Designing Without Privacy*, 55 HOUS. L. REV. 659, 704–05 (2018).

⁷³ Byford, *supra* note 36, at 12–15; Post, *Social Foundations*, *supra* note 37, at 967; MacCarthy, *supra* note 36, at 416.

⁷⁴ Steeves, *supra* note 36, at 205.

⁷⁵ See Allen, *supra* note 8, at 739; Steeves, *supra* note 36, at 193, 199–201.

⁷⁶ ERVING GOFFMAN, *RELATIONS IN PUBLIC: MICROSTUDIES OF THE PUBLIC ORDER* 57–58 (Harper Colophon Books 1972) (1971).

⁷⁷ HELEN NISSENBAUM, *PRIVACY IN CONTEXT* 84–85 (2010).

⁷⁸ *Id.*

“transmission principles” that stipulate the terms of the exchange.⁷⁹ A novel practice violates information privacy when it breaches a context-relative informational norm.⁸⁰ Social roles factor into Nissenbaum’s method as a component of “context.” She writes that “[c]ontexts incorporate assemblages of roles,” defined as “typical or paradigmatic capacities in which people act in contexts.”⁸¹ She adds that “it is crucial to identify the contextual roles of . . . actors to the extent possible” because they “are among those critical variables” that pertain to privacy.⁸²

A focus on role reveals that, in many cases, the details that populate Nissenbaum’s four parameters often flow from an understanding of the role-relationship. Other aspects of context, like time of day and place of an interaction, are likely shaped by the actors’ social roles. It would be reasonable to expect the information exchange between a car salesperson and a patron to occur during business hours at a dealership, rather than over a candlelit dinner. Roles are also likely to inform expectations about who the actors are, what information may be exchanged, and how it may be used and shared. In interactions among strangers, social role might be one of the only details participants know about one another.⁸³

Moreover, as this Article discusses more thoroughly in Section II.A, law often operates through the idiom of social role, rather than other aspects of context. That is to say, law often seeks to change the behaviors of entities acting in particular roles, rather than any entity at a car dealership during business hours.⁸⁴ It may be far more difficult to enact change within a social structure without assigning specific rights and responsibilities on the basis of a regulated entity’s role.

For an example of how social role informs other aspects of context, take the interaction between a university and an applicant—a relationship that involves quite a lot of information sharing and associated norms. Knowing only their social roles, one could specify a detailed account of appropriate and inappropriate interactions and encounters. It would be reasonable to expect applicants to divulge information about their grades, test scores, finances and, increasingly, hardships they have faced, and how they might contribute to a diverse student community. Universities require applicants to submit much of this information in their applications.⁸⁵ (One who does not divulge this information might not

⁷⁹ *Id.* at 132–34, 140–47.

⁸⁰ *Id.* at 140.

⁸¹ *Id.* at 133.

⁸² *Id.* at 141–42.

⁸³ Sloan & Warner, “*I’ll See*,” *supra* note 36, at 252.

⁸⁴ See Section II.A.

⁸⁵ See *Application Guide for First-Year Students*, COMMON APP, <https://www.commonapp.org/apply/first-year-students> [<https://perma.cc/9CTS-A38L>].

even be considered an “applicant.”) But even in free-form submissions, like personal statements, there are norms about what details applicants should include (e.g., demonstrations of leadership, perseverance, or talent) and should not include (e.g., descriptions of intimate sexual encounters, criminal activity, or fabrications).⁸⁶ Norms (and, to an extent, law) constrain what universities may do with this information.⁸⁷ Grades and test scores might factor into whether an applicant will be exempt from certain course requirements if admitted, but applicant finances likely should not. Universities also tailor the information they share about themselves to applicants, typically in the form of information sheets or lookbooks about courses, financial aid, or class composition,⁸⁸ but not about whether faculty interactions with one another tend to be cooperative or adversarial.

Robert Sloan and Richard Warner explain that strangers coordinate “through mutual voluntary restraint” based on their respective roles to abide by shared expectations of appropriate information sharing and use.⁸⁹ “You *trust another person to conform to a norm* if, based on the relevant role presentations, it is common knowledge between you that each of you will conform.”⁹⁰ Their focus is on cooperative endeavors, where people “voluntarily limit their knowledge of each other” out of respect for role-based privacy norms.⁹¹ But role-based privacy norms may also guide behavior—albeit differently—in antagonistic relationships.

Consider the relationship between an employer and a union. Each wants to know as much as possible about the other and reveal only selective and self-serving information about itself.⁹² The employer would want to know whether a union will actually strike when it threatens to do so, but if the union reveals that information, it loses its primary bargaining chip.⁹³ The union would be well-served to know the maximum an employer could pay workers while remaining profitable, but the

⁸⁶ Amy Allen, *How to Write a Personal Essay for Your College Application*, HARV. BUS. REV.: ASCEND (Dec. 14, 2021), <https://hbr.org/2021/12/how-to-a-personal-essay-for-your-college-application> [<https://perma.cc/W6KD-GGR4>]; Sawyer Earwood, *How Personal Is Too Personal in a College Essay?*, VIRTUAL COLL. COUNS. (July 19, 2023), <https://www.virtualcollegecounselors.com/post/how-personal-is-too-personal-in-a-college-essay> [<https://perma.cc/W4QB-39NZ>].

⁸⁷ See, e.g., 20 U.S.C. § 1232g.

⁸⁸ See, e.g., *Discover Why You Belong Here*, SMU: UNDERGRADUATE ADMISSION, <https://www.smu.edu/admission/you-belong-here> [<https://perma.cc/YB74-M5MP>].

⁸⁹ Sloan & Warner, “*I’ll See*,” *supra* note 36, at 248.

⁹⁰ *Id.* at 258.

⁹¹ *Id.* at 224.

⁹² Sari Mazzurco, *Democratizing Platform Privacy*, 31 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 792, 822–23 (2021).

⁹³ *Id.* at 839–40.

employer knows that revealing that detail would reduce its leverage.⁹⁴ That is all to say, one can form expectations about appropriate information sharing and use practices based on the roles parties are playing even when their relationship is characteristically antagonistic.

II. PRIVACY LAW'S ROLE-SCRIPTING FUNCTION

Law often contributes to the meaning society attaches to particular social roles through the statements it makes about the entities it regulates and the public it serves. When politics or markets are in periods of “formation or transformation,” social roles can be underdeveloped or altogether uncertain.⁹⁵ In this social context, law has a special influence over the initial meaning associated with developing roles.

Law can script social roles well or poorly. It can respond to the felt needs of society, empower the disenfranchised, and enable responsive future reform. Alternatively, it can fracture society, bolster hegemonic power structures, and cabin reform. That is because role-scripts orient and pre-commit laws in multiple ways. They establish a set of evaluative criteria that justify or undermine particular rights or responsibilities. For example, laws that serve the “consumer” are justified if they support individual “choice.” They also call up a particular set of legal precedents that bind court adjudications. If a court perceives individuals participating in a boycott as concerned citizens, their association and demonstration might be protected by the First Amendment; if they are consumers in an economic exchange, their association and demonstration might be an unlawful restraint of trade.⁹⁶ The role-scripts law authors carry consequences for individuals’ emergent selfhood as they identify with or distance themselves from the social roles law has helped define.

Section II.A introduces law’s role-scripting function. Section II.B then explores its traditional application in privacy law. It argues privacy law, by operating through the idiom of social role, often generates role-scripts to guide the privacy norms that constitute particular relationships. When it does so, it operates normatively, articulating an idealized vision of how one should handle certain information when acting in the regulated role. Section II.C describes and critiques U.S. privacy law’s reliance on a “business-consumer” role-relationship during a crucial period of transformation—the dawn of the commercial internet. When policymakers first attempted to protect privacy on the early internet, they

⁹⁴ *Id.* at 822–23.

⁹⁵ FLIGSTEIN, *supra* note 31, at 27.

⁹⁶ See *NAACP v. Claiborne Hardware Co.*, 458 U.S. 886, 894–96, 906–17 (1982).

framed the relationship between websites and internet users as a one-size-fits-all “business-consumer” relationship. The choice of this role relationship catalyzed the dysfunctional state of online privacy today—and the threat to individual identity formation—by undermining the development of online privacy norms and narrowing available legal reforms. Part III then looks to the future of privacy law’s role-scripting function. It examines whether current reform proposals serve emergent selfhood, and it ultimately presents a legislative proposal it argues is superior in that respect.

A. *Legal Role-Scripting*

Social roles take shape through continuous interactions in society. Law takes part in this dynamic too.⁹⁷ Modern liberal democracies typically govern entities based on a perception of their social roles.⁹⁸ There are some laws that regulate certain acts without reference to the actor’s social role. For instance, whether you are a broadcaster or a truck driver, state law personality rights would prohibit you from appropriating someone else’s name or likeness for your own benefit.⁹⁹ But, for the most part, law categorizes the entities it regulates by naming and describing its legal subject. The rights, responsibilities, behavioral constraints, and entitlements it gives that legal subject outline a social role.¹⁰⁰

Some commentators argue law may only reflect settled social roles (and imperfectly at that).¹⁰¹ But others recognize that law also sometimes creates new social roles or substantially redefines existing roles’ behavioral norms.¹⁰² Harlan Fiske Stone, for example, explained that from the time of the nation’s founding, family law helped define what it means to be a “husband” and “wife” by allocating to each role certain

⁹⁷ Cass R. Sunstein, *Social Norms and Social Roles*, 96 COLUM. L. REV. 903, 921, 923 (1996); Dan-Cohen, *supra* note 25, at 1228–29; Mitnick, *supra* note 29, at 824, 831; Bert I. Huang, *Law and Moral Dilemmas The Trolley Problem Mysteries*, 130 HARV. L. REV. 659, 678 (2016).

⁹⁸ Mitnick, *supra* note 29, at 824; Manfred Rehbinder, *Status, Contract, and the Welfare State*, 23 STAN. L. REV. 941, 955 (1971).

⁹⁹ See, e.g., RESTATEMENT (SECOND) OF TORTS § 652C (AM. L. INST. 1977); N.Y. CIV. RIGHTS LAW § 50-f(2) (McKinney 2022).

¹⁰⁰ Mitnick, *supra* note 29, at 824, 828, 831, 833, 868–69; Rehbinder, *supra* note 98, at 951–52; Dan-Cohen, *supra* note 25, at 1228–30; Huang, *supra* note 97, at 678.

¹⁰¹ See, e.g., HARLAN FISKE STONE, LAW AND ITS ADMINISTRATION 34 (1915); Paul Bohannon, *The Differing Realms of the Law*, 67 AM. ANTHROPOLOGIST, Dec. 1965, at 33, 35–37.

¹⁰² See, e.g., Sunstein, *supra* note 97, at 923; Dan-Cohen, *supra* note 25, at 1229–30; Mitnick, *supra* note 29, at 824, 865; STONE, *supra* note 101, at 78–79, 82; Neil Fligstein, *The Transformation of Corporate Control*, in THE NEW ECONOMIC SOCIOLOGY 407, 408–09 (Frank Dobbin ed., 2004); William G. Roy, *Socializing Capital: The Rise of the Large Industrial Corporation in America*, in THE NEW ECONOMIC SOCIOLOGY 433, 438–39, 450–51 (Frank Dobbin ed., 2004).

rights and responsibilities and periodically adjusting them.¹⁰³ At common law, the husband was the legal head of the family, liable for his wife's torts and contracts, and entitled to his wife's services and all of her personal property. When women became wives, on the other hand, they lost the power to contract, could not be sued apart from their husbands, and had an indefeasible right to dower. Statutes that gradually protected wives' legal independence supported new, progressive norms for the husband-wife relationship.¹⁰⁴

The corporation is an emblem of legally created social roles. The corporation and the suite of roles within it all originate as legal constructs.¹⁰⁵ Historically, when a government granted a corporate charter, a corporation emerged as a distinct legal and social entity, with a set of legally granted privileges and responsibilities to "shareholders" (another new social role) and the public.¹⁰⁶ Corporate law defined what it means to be a "corporation" and it created many roles *within* the corporation (e.g., shareholders, officers, directors, chairs, etc.), each with their own legally scripted behavioral obligations.¹⁰⁷ Antitrust law also contributed to the boundaries of appropriate corporate behavior.¹⁰⁸ And, in recent years, the Supreme Court has recognized a range of corporations' rights, such as the rights to speak, fund electioneering communications, and practice religion, suggesting these are all normal social behaviors for corporations.

The legal system itself contains well-recognized examples of legally scripted social roles. Juror, defendant, prosecutor, and judge, and the behavioral norms associated with those roles, derive from law.¹⁰⁹ Law supplied the initial social meaning of these roles, but they are continually redefined as actors interact *in* the roles and *with* the roles.¹¹⁰ Roberto Mangabeira Unger describes this dance between law and society more generally: "[O]bligations do arise primarily from relationships . . . that have been only incompletely shaped by government-imposed duties or

¹⁰³ STONE, *supra* note 101, at 78–79.

¹⁰⁴ *Id.* at 79.

¹⁰⁵ *Id.* at 82; Fligstein, *supra* note 102, at 408–09; Roy, *supra* note 102, at 438–39, 450–51.

¹⁰⁶ Fligstein, *supra* note 102, at 409; Roy, *supra* note 102, at 450–51.

¹⁰⁷ See, e.g., N.Y. BUS. CORP. LAW §§ 601–630, 701–727 (McKinney 2024).

¹⁰⁸ Fligstein, *supra* note 102, at 409.

¹⁰⁹ Dan-Cohen, *supra* note 25, at 1230.

¹¹⁰ One need only look, for example, at the syllabus of the Harvard Business School course "Corporate Governance and Boards of Directors." The legal rights and obligations that attach to the many social roles within the corporate structure are only a small component of the course. Rather, the course focuses on "the complex dynamics among boards, executives, and shareholders," and the "managerial[] and behavioral issues that directors must contend with." See *Corporate Governance and Boards of Directors*, HARV. BUS. SCH. COURSE CATALOG (2024), <https://www.hbs.edu/coursecatalog/2010.html> [<https://perma.cc/DZ89-KU67>].

explicit and perfected bargains.”¹¹¹ Society and law define social roles dialogically. Paul Bohannon describes this phenomenon as law being perpetually but constructively “out of phase with society.”¹¹² Societal conflict over social roles’ meaning and varied real-life social practices continuously alter the expectations associated with social roles and push law to keep up.

Regardless of whether law “makes” new social roles or “takes” existing roles, it presses individuals to adopt its chosen role scripts. In that sense, legal role-scripting is a normative endeavor. Individuals “readily internalize legally constructed” roles and norms to the point that they “are rarely . . . conscious of [law’s] influence on [thei]r perceptions.”¹¹³ For example, Bert Huang conducted an experimental study that examined participants’ reactions to different iterations of tort law’s classic trolley problem. Huang found that the legal duty the law assigned to each role influenced participants’ views of the roles’ moral obligations.¹¹⁴ His study suggests individuals often translate legal definitions into social norms on instinct, especially when norms are not settled.¹¹⁵

The possibility of legal sanctions for non-compliance augments the law’s ability to enforce social roles and norms.¹¹⁶ For instance, when the United States military enforced its DADT policy, it selected and enforced a discriminatory norm that servicemembers must not be homosexual (and, if they were, their homosexuality was shameful) or else face discharge.¹¹⁷

Law is also often situated to mediate between competing normative claims and back a particular role-script with its coercive power. The end of DADT in 2011 reflected the success of LGBTQ advocacy to normalize servicemembers’ sexual diversity, but the Trump Administration’s 2019

¹¹¹ ROBERTO MANGABEIRA UNGER, *THE CRITICAL LEGAL STUDIES MOVEMENT* 81 (1983).

¹¹² Bohannon, *supra* note 101, at 37.

¹¹³ Mitnick, *supra* note 29, at 826; see also Huang, *supra* note 97, at 694–95.

¹¹⁴ Huang, *supra* note 97, at 694–95. Elizabeth Anderson provides another example of a Swiss town that was offered compensation to serve as a potential site for a nuclear waste facility. She writes that the government’s offer of compensation treated residents as property owners rather than citizens. The residents were less likely to accept the facility when thinking as property owners instead of as citizens. Elizabeth Anderson, *Beyond Homo Economicus: New Developments in Theories of Social Norms*, 29 PHIL. & PUB. AFFS. 170, 197 (2000).

¹¹⁵ See Lawrence Lessig, *The Regulation of Social Meaning*, 62 U. CHI. L. REV. 943, 1030 (1995).

¹¹⁶ Dahrendorf, *supra* note 24, at 42–43; Rehbinder, *supra* note 98, at 953; Dan-Cohen, *supra* note 25, at 1233; Anderson, *supra* note 114, at 193.

¹¹⁷ See generally Daniel Ryan Koslosky, *Sexual Identity as Personhood: Towards an Expressive Liberty in the Military Context*, 84 N.D. L. REV. 175 (2008) (describing DADT policy and implications for expressions of homosexual identity).

ban of transgender persons in the military swung the pendulum the other way.¹¹⁸

Legal definitions of social roles also delineate the scope of possible legal reform and legal claims on a particular subject.¹¹⁹ For instance, when in vitro fertilization became more widely available in the 1990s, courts had to decide whether gestating women had any rights to nonbiological children they birthed. In *Johnson v. Calvert*, a California court found that a gestating woman who refused to turn over a child to the child's genetic parents had no parental right to the child—she was not a “mother” but a “gestational surrogate.”¹²⁰ By contrast, in *Perry-Rogers v. Fasano*, a New York court found that a woman mistakenly implanted with another couple's embryo would have been the child's “mother” (with associated parental rights) had she not voluntarily relinquished custody.¹²¹ Law that regards a gestating woman as a “mother” would confer parental rights such as custody or visitation, as well as parental responsibilities of care. Law that regards a gestating woman as a “gestational surrogate” would limit her rights to the terms of her surrogacy contract. A revision of gestating women's role predicates reform to surrogacy law and the precedent a court would consider when deciding a dispute. If the law treats gestating women as surrogates for hire, reforms to provide visitation rights would make little sense—they are not parents, but service providers. Surrogacy law would have to alter the role it envisions gestating women play in parentage to justify such a reform.

There also must be sufficient public buy-in and acceptance of law's role-scripts for legal definitions of social roles to drive future reform. A group of political scientists based out of the University of Zurich, writing about Trump's ban from Twitter, found that “[t]o rise to the political agenda, a given issue must first be construed as politically salient and specific arguments put forward as to how and why it might warrant policy intervention,” and “[h]ow political actors frame th[e] issue . . . may impact the kinds of solutions proposed.”¹²² The public's acceptance, rejection, or alteration of legal role-scripts foments support for or resistance to possible future reform.

¹¹⁸ Evan R. Seamone, *Beyond “Restoration of Honor”: Compensating Veterans for the Psychological Injuries of the Gay and Transgender Bans*, 28 WM. & MARY J. RACE, GENDER & SOC. JUST. 687, 688–90 (2022).

¹¹⁹ J.M. Balkin, *Understanding Legal Understanding: The Legal Subject and the Problem of Legal Coherence*, 103 YALE L.J. 105, 121–23 (1993).

¹²⁰ 851 P.2d 776, 785–87 (Cal. 1993).

¹²¹ 715 N.Y.S.2d 19, 24 (N.Y. App. Div. 2000).

¹²² Meysam Alizadeh et al., *Content Moderation as a Political Issue: The Twitter Discourse Around Trump's Ban*, J. QUANTITATIVE DESCRIPTION: DIGIT. MEDIA, Oct. 2022, at 1, 6.

Law's role-scripting function illuminates the stakes when privacy law operates through the idiom of social role. Privacy law guides human behaviors and contributes to individuals' senses of self in important part through the messages it sends about who it regulates and who it serves. Privacy law's role-scripts also tend to set law on particular paths. That is to say, once privacy law scripts a role to contain a particular set of norms, adjudication and reform efforts down the line will be limited by existing role constructions, along the lines of the surrogacy example above. That is because legal role-choices direct lawmakers and the public to evaluate reforms' desirability based on different criteria.

The idea of *law* constructing social roles may seem odd, considering social roles typically stem from everyday interactions.¹²³ Legal prescription might seem paternalistic. But this critique misses that law largely unavoidably shapes social roles because it must categorize entities, whether it redefines existing social roles or creates them anew.¹²⁴ Scripting roles well requires lawmakers to direct attention to the sorts of practices and legal pathways law's role-choices sustain. Neglecting privacy reforms' role-scripts misses an opportunity to evaluate these social and legal implications.

B. *Privacy Law's Traditional Role-Scripting*

Privacy law's engagement with social roles is so routine that it is difficult to imagine how privacy law might function without regarding the roles actors play in a particular relationship or legal dispute. This Section delves into privacy law's traditional role-scripting function by examining the many ways privacy law relies on and espouses the social roles of regulated entities and the public. It describes spousal privacy, healthcare privacy, postal privacy, and privacy torts as instructive examples.

A number of sectoral statutes, like the Health Insurance Portability and Accountability Act (HIPAA),¹²⁵ the Gramm-Leach-Bliley Act (GLBA),¹²⁶ the Video Privacy Protection Act (VPPA),¹²⁷ and the Family Educational Rights and Privacy Act (FERPA)¹²⁸ explicitly regulate privacy within specific role-relationships. Likewise, evidentiary privileges attach

¹²³ See *supra* note 32 and accompanying text.

¹²⁴ See *supra* notes 102–111 and accompanying text.

¹²⁵ 45 C.F.R. § 160 (2024); 45 C.F.R. § 164.102–.106, .500–.535 (2024).

¹²⁶ 15 U.S.C. § 6809.

¹²⁷ 18 U.S.C. § 2710.

¹²⁸ 20 U.S.C. § 1232g.

on the basis of one's role as a psychotherapist,¹²⁹ spouse,¹³⁰ or attorney.¹³¹ But even beyond these narrow forms, privacy law typically reflects and directs the social roles individuals and organizations play as they interact. For instance, the Fourth Amendment¹³² and a suite of federal statutes¹³³ regulate the privacy relationship between the government and citizens. In the process, they articulate a vision of what it means to be a government and a citizen, whether by crystallizing existing role-based norms or setting aspirational behavioral standards.

Even "generalist" privacy laws, like privacy torts,¹³⁴ often invoke social roles. The "reasonable person" who must be highly offended is rarely a bare outline of a person; they are more often the reasonable student, reasonable employee, reasonable country fair attendee, and so on. Privacy law is sometimes a role *taker*, reflecting prevailing role-based norms (and operating descriptively). But often (and largely unavoidably), it is a role *maker*, operating normatively. Privacy law's imprimatur on a set of norms helps shape societal understandings of particular social roles and direct future reform, for better or worse.

1. Spousal Privacy

Privacy law historically sheltered the spousal relationship based on the understanding women were subsumed under men's personhood once they entered into a marriage. In fact, in their earliest forms, protections of the spousal relationship from legal action had less to do with privacy between spouses and more to do with women's loss of social and legal status once they became wives. Far from autonomous persons in a relationship of trust and respect, wives were more like their husbands' wards or property.

This notion of wives' social and legal status animated both marital rape laws and the evidentiary privilege shielding marital communications. In the eighteenth century, British jurist Sir Matthew Hale stated that a "husband cannot be guilty of a rape committed by himself upon his lawful wife, for by their mutual matrimonial consent

¹²⁹ See FED. R. EVID. 501 advisory committee's note to 1974 amendment.

¹³⁰ See *Trammel v. United States*, 445 U.S. 40, 53 (1980).

¹³¹ See FED. R. EVID. 502.

¹³² U.S. CONST. amend. IV.

¹³³ See Privacy Act of 1974, Pub. L. No. 93-579, 88 Stat. 1896 (codified as amended at 5 U.S.C. § 552a); Freedom of Information Act of 1974, Pub. L. No. 93-502, 110 Stat. 3048 (codified as amended at 5 U.S.C. § 552); Right to Financial Privacy Act of 1978, Pub. L. No. 95-630, 92 Stat. 3641 (codified as amended at 12 U.S.C. §§ 3401-3423); Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (codified as amended at 18 U.S.C. §§ 2510-2523).

¹³⁴ RESTATEMENT (SECOND) OF TORTS § 652 (AM. L. INST. 1977).

and contract the wife hath given up herself in this kind unto her husband which she cannot retract.”¹³⁵ That is to say, a woman’s sexual autonomy terminated once she became a wife and was replaced with a norm of sexual submission or, potentially, violence. The spousal privilege against adverse testimony, on the other side of the coin, began as a spousal disqualification. A wife could not testify for or against her husband because she was considered the same legal person as her husband.

These laws relied on—and bolstered—oppressive characterizations of what it means to be a “wife” in a marital relationship under the guise of protecting spousal privacy from legal scrutiny. In *Hawkins v. United States*, the Supreme Court rejected a modification to the spousal privilege to allow voluntary adverse testimony stating “that the law should not force or encourage testimony which might alienate husband and wife, or further inflame existing domestic differences.”¹³⁶ Allen writes that this norm of wives’ “seclusion and subordination” rendered “women . . . unable to utilize their full capacities to participate in society. Maternal and social roles kept women[—]who might otherwise have distinguished themselves in the public sphere . . . [—]in the private sphere.”¹³⁷

The women’s liberation movement of the 1960s and 1970s galvanized legal reforms to replace prevailing, oppressive norms with expectations of wives’ sexual autonomy and social and political equality. In *Griswold v. Connecticut*, decided in 1965, the Supreme Court articulated an altogether different view of the marital relationship based on continued voluntary association and bilateral loyalty.¹³⁸ States began to outlaw marital rape in the 1970s and, by 1980, the Court modified *Hawkins* to allow voluntary adverse spousal testimony. It reasoned “[t]he ancient foundations” for the rule against adverse testimony “have long since disappeared,” and “[w]hen one spouse is willing to testify against the other . . . there is probably little in the way of marital harmony for the privilege to preserve.”¹³⁹ Though spousal privacy reforms purported to sync up with already changed societal understandings of the marital

¹³⁵ SIR MATTHEW HALE, *THE HISTORY OF THE PLEAS OF THE CROWN* 629 (London, E. Rider 1800) (1736).

¹³⁶ 358 U.S. 74, 79 (1958).

¹³⁷ Allen, *supra* note 8, at 724, 744.

¹³⁸ 381 U.S. 479, 486 (1965) (“We deal with a right of privacy older than the Bill of Rights—older than our political parties, older than our school system. Marriage is a coming together for better or for worse, hopefully enduring, and intimate to the degree of being sacred. It is an association that promotes a way of life, not causes; a harmony in living, not political faiths; a bilateral loyalty, not commercial or social projects. Yet it is an association for as noble a purpose as any involved in our prior decisions.”).

¹³⁹ *Trammel v. United States*, 445 U.S. 40, 52 (1980).

relationship, over time they helped drive new spousal norms from the margins to the mainstream.

2. Healthcare Privacy

Notions of privacy within a healthcare relationship date back to the Hippocratic Oath.¹⁴⁰ In the United States, state and federal laws developed over time to protect the privacy of doctor-patient relationships. At various junctures, healthcare-specific privacy laws expressly sought to usher in new role-based behavioral norms.

State law evidentiary privileges protecting patient information from compelled disclosure were among the earliest legal protections of healthcare privacy. Mark MacCarthy notes that “[b]eginning with New York in 1828, . . . the states passed [these] laws in an attempt to ensure that people sought treatment for diseases.”¹⁴¹ States afforded the doctor-patient relationship an evidentiary privilege to advance a new privacy norm that patients would candidly share their health information with doctors. These laws aimed to support concomitant norms of patients’ maximal disclosure of health information and doctors’ general non-disclosure of that information outside the context of care.¹⁴² Early breach of confidence tort cases that regarded hospital-patient and doctor-patient relationships as confidential reinforced those norms.¹⁴³

Since then, Congress passed a number of laws aimed at stimulating a number of different privacy norms on the part of doctors and patients. The HIPAA Privacy Rule (the “Privacy Rule”) protected the existing norm of doctor-patient confidentiality,¹⁴⁴ but it also confronted an unsettled norm: the extent and limits of patient autonomy. The U.S. Department of Health and Human Services (HHS), which drafted the Privacy Rule, wavered on whether to require patients’ consent to healthcare providers’ use of their medical information. Over the course of seven years, it received tens of thousands of public comments favoring consent. Ultimately, HHS took a mixed approach to consent, allowing providers to use patient health information for a set of specifically defined

¹⁴⁰ *Ancient Greek Medicine “I Swear by Apollo Physician...”: Greek Medicine from the Gods to Galen*, NIH NAT’L LIBR. MED., <https://www.nlm.nih.gov/hmd/topics/greek-medicine/index.html> [<https://perma.cc/7EE6-ETXZ>] (“Whatever I see or hear in the lives of my patients, whether in connection with my professional practice or not, which ought not to be spoken of outside, I will keep secret, as considering all such things to be private.”).

¹⁴¹ MacCarthy, *supra* note 36, at 434–35.

¹⁴² *Id.*

¹⁴³ Richards & Solove, *supra* note 14, at 151, n.198.

¹⁴⁴ MacCarthy, *supra* note 36, at 435 (“The rationale for the rule was the need to provide doctors with accurate information in order for patients to receive medical care.”).

purposes and requiring patient consent for any other uses.¹⁴⁵ The Privacy Rule ushered in a new, more fine-grained norm of patient trust and dependence on doctors for medical care and patient control over other uses of information about them.

More recently, Congress passed the Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009 to encourage a new norm for healthcare providers: “[T]o promote the adoption and meaningful use of health information technology.”¹⁴⁶ And, in 2016, Congress passed the 21st Century Cures Act to encourage greater information sharing between healthcare providers by prohibiting “information blocking.”¹⁴⁷ As information technology and medical practice have evolved, privacy laws have repeatedly waded in to direct new role-based privacy norms to meet current needs.

3. Postal Privacy

Early American postal privacy law helped constitute the role of the post, especially in terms of its relationship with the public. It responded to the needs of the time—secrecy from the crown—and it set law down a path to ultimately guard email relationships that are decidedly non-postal and non-public.

In 1775, before the Declaration of Independence was signed, the Continental Congress created the Post Office of the United States.¹⁴⁸ Even before the relationship between the government and its citizens took shape in the federal Constitution, this early government forged the relationship between the post office and the public. In his comprehensive account of the post office and early communications privacy, Anuj Desai explains that before the “constitutional post,” there was no settled expectation regarding postal privacy.¹⁴⁹ “The role of the British post office as an ‘intelligence organ,’ . . . remained crucial to the British government throughout the eighteenth century and well into the nineteenth.”¹⁵⁰ Via its “‘Secret Office,’ the British post office ‘created intelligence by opening,

¹⁴⁵ Tschider, *supra* note 36, at 645.

¹⁴⁶ *HITECH Act Enforcement Interim Final Rule*, U.S. DEP’T HEALTH & HUM. SERVS. (June 16, 2017), <https://www.hhs.gov/hipaa/for-professionals/special-topics/hitech-act-enforcement-interim-final-rule/index.html> [<https://perma.cc/7GYP-FLUQ>].

¹⁴⁷ Carleen M. Zubrzycki, *Privacy from Doctors*, 39 YALE L. & POL’Y REV. 526, 535 (2021).

¹⁴⁸ Winnifred Gallagher, *A Brief History of the United States Postal Service*, SMITHSONIAN MAG. (Oct. 2020), <https://www.smithsonianmag.com/smithsonian-institution/brief-history-united-states-postal-service-180975627> [<https://perma.cc/MFQ7-29NS>].

¹⁴⁹ Anuj C. Desai, *Wiretapping Before the Wires: The Post Office and the Birth of Communications Privacy*, 60 STAN. L. REV. 553, 562–63, 566 (2007).

¹⁵⁰ *Id.* at 560.

detaining, or copying correspondence, and sending “interceptions” to the Secretaries of State.”¹⁵¹ British law forbade tampering with the mail, but this was mostly a formality.¹⁵² And, practically, mail in the colonies was highly insecure. Overseas mail came in “a mailbag hung in a tavern, where anyone could rifle through,” and wax seals often broke down during transit.¹⁵³ For the rebels, who were likely engaged in treason, the privacy of their mailed communications was imperative to the possibility of independence from the crown. As Desai writes, “Confidentiality of correspondence was thus a significant factor motivating the establishment of the separate ‘constitutional post.’”¹⁵⁴

The Continental Congress infused the constitutional post with a norm of communications privacy early on. In 1782, it passed a law explicitly prohibiting postal workers from opening the mail without a warrant.¹⁵⁵ In the 1792 Post Office Act, Congress simultaneously founded the United States Post Office and guaranteed postal privacy.¹⁵⁶ It forged a new relationship between the post and the public based on confidentiality, trust, and responsibility. Desai points out that this norm of postal privacy became such a powerful custom that it ascended to constitutional status.¹⁵⁷ In *Ex parte Jackson*, the Supreme Court decided mailed letters qualify as the sender’s “papers” for Fourth Amendment purposes, such that the government could not open a sender’s mail without a warrant.¹⁵⁸ Indeed, early legal definitions of privacy norms in postal relationships proved so influential that they informed the privacy norms associated two hundred years later with *electronic* mail (email) providers. The Electronic Communications Privacy Act (ECPA) generally bars email providers from intercepting the emails they transmit and requires the government to satisfy legal process before it can engage in interception.¹⁵⁹

¹⁵¹ *Id.* (quoting KENNETH ELLIS, *THE POST OFFICE IN THE EIGHTEENTH CENTURY* 62 (1958)).

¹⁵² *Id.*

¹⁵³ *Id.* at 562.

¹⁵⁴ *Id.* at 564.

¹⁵⁵ *Id.* at 566.

¹⁵⁶ An Act to Establish the Post-Office and Post Roads Within the United States, ch. 7, § 16, 1 Stat. 232, 236 (1792).

¹⁵⁷ Desai, *supra* note 149, at 577.

¹⁵⁸ *Ex parte Jackson*, 96 U.S. 727, 733 (1878).

¹⁵⁹ 18 U.S.C. § 2511.

4. Privacy Torts

Legal scholars often characterize the privacy torts first espoused by Samuel Warren and Louis Brandeis and developed further by William Prosser as generalist privacy laws. Neil Richards and Daniel Solove assert that Warren and Brandeis, in their call for a tort to guard against “publication of embarrassing facts,” directed privacy law away from protecting particular relationships and “toward a more general protection of ‘inviolate personality’ against invasions by strangers.”¹⁶⁰ Richards and Solove write: “Warren and Brandeis sought a right against the world to protect hurt feelings.”¹⁶¹ Richards and Woodrow Hartzog argue Warren and Brandeis advocated for this sort of general right to privacy because the “aggressive press” that concerned Warren and Brandeis mostly “didn’t have a relationship with the subjects of its reportage.”¹⁶² They contend that, following in this tradition, “Today, with a few exceptions such as HIPAA and a handful of other confidentiality-based regimes, privacy . . . law is generally agnostic to . . . whether a relationship exists between people at all.”¹⁶³

The privacy torts at face value seem to support the view that they are not concerned with relationships. In practice, however, they too often reflect and direct social roles. As written in the Restatement (Second) of Torts, the privacy torts prohibit “unreasonable intrusion upon [another’s] seclusion,” the “appropriation of . . . [an]other’s name or likeness,” “unreasonable publicity . . . to [an]other’s private life,” and publicity that unreasonably places another publicly in a false light regardless of the invader and invadée’s roles.¹⁶⁴ But three of the four torts hinge liability on whether the act would be “highly offensive to a reasonable person.”¹⁶⁵ Robert Post explains that “the reasonable person” the torts consider “is a genuine instantiation of community norms.”¹⁶⁶ And, as explained in Section I.C, more often than not, privacy norms in any given interaction vary depending on participants’ social roles.

The privacy torts may have begun as “right[s] against the world,”¹⁶⁷ but, when applied, courts often evaluate whether the invasion would

¹⁶⁰ Richards & Solove, *supra* note 14, at 125, 132.

¹⁶¹ *Id.* at 132.

¹⁶² Neil Richards & Woodrow Hartzog, *A Relational Turn for Data Protection?*, 6 EUR. DATA PROT. L. REV. 492, 493 (2020) [hereinafter Richards & Hartzog, *Relational Turn*].

¹⁶³ Woodrow Hartzog & Neil Richards, *The Surprising Virtues of Data Loyalty*, 71 EMORY L.J. 985, 992–93 (2022) [hereinafter Hartzog & Richards, *Surprising Virtues*].

¹⁶⁴ RESTATEMENT (SECOND) OF TORTS § 652A(2) (AM. L. INST. 1977).

¹⁶⁵ *Id.* § 652B, D–E.

¹⁶⁶ Post, *Social Foundations*, *supra* note 37, at 961.

¹⁶⁷ Richards & Solove, *supra* note 14, at 132.

highly offend a reasonable person by looking to the plaintiff's and defendant's role-relationship. In the process, they articulate role-based privacy norms, perhaps informed by a view of existing societal expectations (i.e., role-taking), but importantly, bolstering a particular role-construction with the coercive power of law (i.e., role-making).¹⁶⁸

Employee privacy cases are an illuminating example. Pauline Kim explains that outside of a few, narrow statutory protections, employee privacy rights derive mainly from privacy torts.¹⁶⁹ For instance, "[L]iability for invasion of privacy may arise when an employer enters an employee's home without permission, searches an employee's locker and purse, or inquires into an employee's sexual relationship with her husband."¹⁷⁰ A look into the cases she cites reveals the courts attuned their concept of the purported invasion's reasonableness to the employment relationship specifically.

In *Love v. Southern Bell Telephone & Telegraph Company*, a Louisiana court found it was unreasonable for employees to enter a fellow employee's home without permission because they did so "in the furtherance of their employer's interest and designed to prove plaintiff's unworthiness as a supervisory employee."¹⁷¹ In *K-Mart Corp. Store No. 7441 v. Trotti*, a Texas court held that where an "employee purchases and uses his own lock on [employer-provided] lockers, with the employer's knowledge," one can reasonably conclude "the employee manifested, and the employer recognized, an expectation that the locker and its contents would be free from intrusion and interference."¹⁷² Query whether the *Love* court would have found an actionable invasion if a neighbor entered the plaintiff's house to prove him an unsavory community member, or whether the *Trotti* court would have held a school liable for breaking into a student's locker. When courts appeal to role-based community morals to evaluate the reasonableness of a potentially privacy-invading behavior, their opinions also pronounce certain privacy norms for society to ascribe to litigants' roles—or else risk legal penalty.¹⁷³

¹⁶⁸ See *infra* notes 169–173 and accompanying text.

¹⁶⁹ Pauline T. Kim, *Privacy Rights, Public Policy, and the Employment Relationship*, 57 OHIO ST. L.J. 671, 679 (1996).

¹⁷⁰ *Id.* at 675.

¹⁷¹ 263 So. 2d 460, 466 (La. Ct. App. 1972).

¹⁷² 677 S.W.2d 632, 637 (Tex. Ct. App. 1984). The court also explained the "highly offensive" requirement's necessity by calling upon different role-based interactions that should not face liability because they are benign. *Id.* ("A business executive, for example, could find himself liable for entering an associate's office without express permission; so could a beautician who opened a co-worker's drawer in order to find some supplies needed for a customer.").

¹⁷³ This is also the case when courts find no invasion occurred. For instance, in *McLain v. Boise Cascade Corp.*, an Oregon court held it was not unreasonable for an employer to film an employee's activities on his own property because he "could have been observed by his neighbors or passersby

C. *The Emergence of the Internet and the Business-Consumer Relationship*

Privacy law historically scripted social roles fairly granularly. It has enforced privacy norms within role-relationships (like an employer-employee relationship) or set new norms for emerging role-relationships (like the post-public relationship). Yet, during a phase of major transformation—the emergence of the commercial internet—privacy law's role-multiplicity collapsed. FTC enforcement actions and, later, generalist privacy laws like the ECPA and privacy torts, construed online privacy through the framework of a one-size-fits-all neoclassical business-consumer relationship.¹⁷⁴ The legal choice of this role-relationship catalyzed the erosion of privacy online, the threat to identity constituting roleplay, and privacy law's ineffectiveness when dealing with current data surveillance problems.

As Part III explores in greater depth, there is an opportunity for online privacy law to scrap the business-consumer relationship and author new roles for data collectors and internet users. Data protection and information fiduciary proposals offer limited improvement. Instead, this Article proposes and advocates for a “privacy governance” legislative proposal that prioritizes roleplay and complex identity formation.

It was not a given that online information privacy law would adopt “business” and “consumer” roles for the entities it regulates and the public it serves. Rather, these legal role choices trace their roots to 1970s-era policymaking focused on computerized databases.¹⁷⁵ The first government effort to consider private-sector information privacy was the Privacy Protection Study Commission (PPSC) established by the Privacy Act of 1974.¹⁷⁶ The PPSC's Report, released in 1977, marked a crucial but so far underappreciated step toward law's adoption of “business” and “consumer” as the relevant social roles in private-sector information privacy.¹⁷⁷

Though the PPSC did not explicitly state its analysis of privacy issues and recommendations were based on a business-consumer relationship,

on the road running in front of his property.” 533 P.2d 343, 346–47 (Or. 1975). In other words, it might be normatively acceptable for an employer to surveil an employee at home if the employee's behavior is visible beyond their property line.

¹⁷⁴ Electronic Communications Privacy Act of 1986, 18 U.S.C. §§ 2510–2523.

¹⁷⁵ Savage, *supra* note 17, at 100.

¹⁷⁶ John A. Rothchild, *Against Notice and Choice: The Manifest Failure of the Proceduralist Paradigm to Protect Privacy Online (or Anywhere Else)*, 66 CLEV. ST. L. REV. 559, 586 (2018); REGAN, *supra* note 22, at 83; Nehf, *supra* note 17, at 45.

¹⁷⁷ PRIV. PROT. STUDY COMM'N, PERSONAL PRIVACY IN AN INFORMATION SOCIETY (1977) [hereinafter PPSC REPORT].

its reasoning and ultimate suggestions respond to that type of relationship. The PPSC focused on three interests: individuals' personal privacy interests (i.e., information secrecy), organizations' interests in exchanging information with one another, and society's interest in "keep[ing] governmental intrusion into the flow of information to a minimum."¹⁷⁸ The PPSC reasoned two commercial speech Supreme Court opinions, *Lamont v. Postmaster General of the United States*¹⁷⁹ and *Virginia State Board of Pharmacy v. Virginia Citizens Consumer Council, Inc.*,¹⁸⁰ militated against statutory restrictions on information flows and for individual choice.¹⁸¹ Ultimately, it concluded Congress should rely on organizations' voluntary compliance with a stripped-down notice-and-consent regime.¹⁸²

The PPSC's orientation toward privacy as an individual, personal interest, information exchange as an equally important organizational interest, and small government as an overall societal interest reflect neoclassical economics-based business and consumer roles (as well as neoliberalism's contemporaneous rise in public policy). It imagines individuals and organizations in an unsocialized trade relationship: if individuals receive information about the organization's privacy practices, they will either proceed with the transaction or find an alternative based on their individual privacy preferences.¹⁸³

Though the PPSC Report's recommendations were never enacted into law,¹⁸⁴ its "business-consumer" orientation lingered and was overtly adopted in subsequent government policy on telecommunications information privacy. Whereas in the 1970s, concerns over information privacy focused on computerized databases, in the early 1990s, information privacy concerns centered on a new development: popular use of the internet.¹⁸⁵ In 1995, the Clinton Administration's National Telecommunications and Information Administration (NTIA) released a white paper addressing internet service providers' (ISPs) use of subscribers' personal information for marketing purposes.¹⁸⁶ Writing around that time, Paul Schwartz observed that "the Clinton

¹⁷⁸ *Id.* at 21–22; REGAN, *supra* note 22, at 84.

¹⁷⁹ 381 U.S. 301 (1965).

¹⁸⁰ 425 U.S. 748 (1976).

¹⁸¹ PPSC REPORT, *supra* note 177, at 23–24 (citing *Lamont*, 381 U.S. at 301; *Virginia Citizens*, 425 U.S. at 748).

¹⁸² *Id.* at 26–27, 34, 36.

¹⁸³ *See id.* at 26–27.

¹⁸⁴ REGAN, *supra* note 22, at 85.

¹⁸⁵ *See* U.S. DEP'T OF COM., PRIVACY AND THE NII: SAFEGUARDING TELECOMMUNICATIONS-RELATED PERSONAL INFORMATION 26–27 (1995).

¹⁸⁶ *Id.* at 23–24, 26–27.

[a]dministration and legal commentators increasingly view the role of the [i]nternet law of privacy as facilitating wealth-creating transmission of . . . personal data.”¹⁸⁷ The white paper overtly focused on consumers’ interest in information privacy, defined as an individual’s control over how information about them may be acquired, disclosed, and used, ISPs’ interest in marketing new services to consumers (which, the NTIA asserted, would “doubtless benefit consumers”), and a societal interest in “minim[al] government involvement.”¹⁸⁸ It concluded these interests would be served well by a notice-and-consent approach,¹⁸⁹ which, it imagined, would produce the following interaction:

Under this “contractual approach” to privacy protection, companies would inform their customers about what sorts of personal information the firms intend to collect and the uses to which that information would be put. Consumers could then either accept a company’s “offer,” or reject it and shop around for a better deal.¹⁹⁰

The NTIA’s adoption of a business-consumer paradigm for telecommunications information privacy thus made overt the PPSC’s initial construction of the relationship private-sector information privacy law governs *and* carried it over to a new context—the internet. These policy papers set the scene for the next stage of information privacy policy: the FTC’s regulation of *online* information privacy.

In the late 1990s and early 2000s, website privacy policies were a new phenomenon, brought on by the FTC’s influence over businesses’ commercial practices.¹⁹¹ When the internet was first opened up to commerce in the early 1990s,¹⁹² commercial websites proliferated and began to collect and use personal data—either by “requesting it or simply

¹⁸⁷ Schwartz, *Privacy and Democracy*, *supra* note 36, at 1611.

¹⁸⁸ U.S. DEP’T OF COM., *supra* note 185, at 7, 20.

¹⁸⁹ *Id.* at 8–9, 20, 27.

¹⁹⁰ *Id.* at 20. Schwartz also observed the Clinton Administration exhibited broad deference to industry self-development of online privacy standards. Schwartz, *Privacy and Democracy*, *supra* note 36, at 1639–40 (“Vice President Gore’s ambitiously titled proposal for an ‘Electronic Bill of Rights’ modestly responds to information privacy exigencies with a call for ‘industry self-regulation with enforcement mechanisms.’ In Gore’s view, the Administration’s role is to monitor the effectiveness of industry activity and of any enforcement mechanisms that industry provides against itself.” (footnote omitted)).

¹⁹¹ Steven A. Hetcher, *The Emergence of Website Privacy Norms*, 7 MICH. TELECOMM. & TECH. L. REV. 97, 131, 139 (2000) [hereinafter Hetcher, *Website Privacy Norms*]; Hetcher, *Social Meaning*, *supra* note 17, at 176 (2001).

¹⁹² STEPHEN SEGALLER, NERDS 2.0.1: A BRIEF HISTORY OF THE INTERNET 295, 297 (1998); Boucher Amendment to National Science Foundation Act, 42 U.S.C. § 1862(g) (1992) (expanding acceptable use of the internet beyond “research and education in science and engineering”); Hetcher, *Website Privacy Norms*, *supra* note 191, at 107.

taking it.”¹⁹³ With the development of web cookies, data collection skyrocketed, and Americans began to express distrust and an aversion to internet use.¹⁹⁴ Congress urged the FTC to get involved.¹⁹⁵

Beginning in 1998, the FTC released a series of reports to try to motivate websites to “*self-regulat[e] . . . to protect[] consumer privacy*” with the ultimate aim of “*increasing consumer confidence and . . . their participation in the online marketplace.*”¹⁹⁶ It was not until the FTC threatened to advocate for online privacy legislation¹⁹⁷ that websites began to self-regulate, adopting a notice-and-consent approach the FTC promoted in its 2000 report, *Privacy Online: Fair Information Practices in the Electronic Marketplace*.¹⁹⁸ Since that time, the FTC has regulated online privacy through enforcement actions against websites that fail to live up to their privacy disclosures (deemed “deceptive” under the FTC’s Section 5 authority)¹⁹⁹ and, occasionally, websites that collect and use individuals’ personal information without providing any privacy disclosures at all (deemed “unfair”).²⁰⁰

Unlike the earlier policy papers, the FTC’s decision to structure online privacy law around a business-consumer relationship had “teeth.” The FTC’s business-consumer framing was both expressive—in that the Commission stated outright that online privacy aimed to increase consumer confidence without placing limits on businesses’ use of consumers’ data—and enforceable. The prospect of FTC enforcement actions against websites that shirk its notice-and-consent guidelines make these roles mandatory for websites and internet users when it comes to online privacy issues.²⁰¹

Following the FTC’s effort to regulate “consumer privacy” through website-authored privacy notices, other privacy laws, such as the Wiretap Act and privacy torts, became tethered to the same relationship

¹⁹³ Steven A. Hetcher, *Norm Proselytizers Create a Privacy Entitlement in Cyberspace*, 16 BERKELEY TECH. L.J. 877, 888 (2001) [hereinafter Hetcher, *Norm Proselytizers*]; Hetcher, *Website Privacy Norms*, *supra* note 191, at 107–08.

¹⁹⁴ Hetcher, *Website Privacy Norms*, *supra* note 191, at 108; Hetcher, *Norm Proselytizers*, *supra* note 193, at 888, 895.

¹⁹⁵ Solove & Hartzog, *supra* note 17, at 598.

¹⁹⁶ Savage, *supra* note 17, at 126 (quoting Martha K. Landesberg & Laura Mazzarella, FED. TRADE COMM’N, SELF-REGULATION AND PRIVACY ONLINE: A REPORT TO CONGRESS 3 (1999)).

¹⁹⁷ KATIE MCINNIS, CONSUMER REPS.: DIGIT. LAB, THE EVOLUTION OF CONSUMER ATTITUDES TOWARD ONLINE TRACKING, 1995–2019, at 32 (2020); Hetcher, *Website Privacy Norms*, *supra* note 191, at 104–05, 139.

¹⁹⁸ BUREAU OF CONSUMER PROT., FED. TRADE COMM’N, PRIVACY ONLINE: FAIR INFORMATION PRACTICES IN THE ELECTRONIC MARKETPLACE: A REPORT TO CONGRESS (2000); Hetcher, *Website Privacy Norms*, *supra* note 191, at 129–31; Savage, *supra* note 17, at 105–06, 126–27.

¹⁹⁹ Solove & Hartzog, *supra* note 17, at 628.

²⁰⁰ *Id.* at 638–43.

²⁰¹ Savage, *supra* note 17, at 106.

framing.²⁰² Wiretap and tort suits against online data collectors, including the likes of Google, Apple, and Facebook, rise and fall on the privacy notices they provide to internet users (and users' consent implied from the fact they click "agree" or continue to use the service).²⁰³ In these cases, collectors also often assert (with mixed success) their information practices are "in the ordinary course of business" or "standard" within their industry, to suggest any contrary expectation would be "unreasonable."²⁰⁴

The business-consumer relationship is both a key predicate to privacy law's current ineffectual notice-and-consent regime and a catalyst of privacy's erosion online. Neoclassical economic descriptions of businesses and consumers support minimal legal intervention and undermine normativity because they are fundamentally unsocialized.²⁰⁵ Economics is not concerned with what businesses or consumers *should* do, in a normative sense. Instead, it makes predictions about what they *will* do, from the baseline assumption each acts instrumentally to pursue their self-interest. And these interests are limited. It assumes businesses (or "firms") pursue profits through their market behaviors, and consumers pursue self-interested preferences based on price and quality considerations.²⁰⁶ Online privacy that responds to this relationship regards private entities' information collection and use as a managerial prerogative. It makes sense that businesses should have the unilateral ability to decide *what* information they will collect and *how* they will use it because those decisions will be "checked" by consumers' choice. If consumers do not like a particular business's information practices, they will abstain or choose an alternative, and the business will be forced to change its practices to meet consumer preferences. This relationship framing justifies a good deal of government abstention—if individuals are merely neoclassical "consumers" and data collectors are "businesses," the only conditions that warrant government intervention are market

²⁰² Hetcher, *Social Meaning*, *supra* note 17, at 161–62; Solove & Hartzog, *supra* note 17, at 587, 596–97; Litman, *supra* note 17, at 1288; Nehf, *supra* note 17, at 6, 46, 58; Haynes, *supra* note 17, at 597–99, 607; Electronic Communications Privacy Act of 1986, 18 U.S.C. §§ 2510–11.

²⁰³ See, e.g., *Calhoun v. Google LLC*, 526 F. Supp. 3d 605, 615–16, 619–23 (N.D. Cal. 2021); Order Granting in Part & Denying in Part Motion to Dismiss, *Rodriguez v. Google LLC*, No. 20-cv-04688, 2021 WL 2026726, at *1 (N.D. Cal. May 21, 2021); *Brown v. Google LLC*, 525 F. Supp. 3d 1049, 1057–60, 1063–67 (N.D. Cal. 2021); *In re Facebook, Inc. Internet Tracking Litig.*, 956 F.3d 589, 602–03 (9th Cir. 2020); *Backhaut v. Apple, Inc.*, 74 F. Supp. 3d 1033, 1045–46 (N.D. Cal. 2014).

²⁰⁴ See, e.g., *Calhoun*, 526 F. Supp. 3d at 626; *Brown*, 525 F. Supp. 3d at 1071; *Dunbar v. Google, Inc.*, No. 10-cv-194, 2011 WL 12907501, at *1 (E.D. Tex. May 23, 2011).

²⁰⁵ There is also a link between privacy law's adoption of business and consumer social roles for information privacy and concepts of liberal personhood in political theory. See Allen, *supra* note 8, 723–24.

²⁰⁶ See LUCY BLACK CREIGHTON, *PRETENDERS TO THE THRONE: THE CONSUMER MOVEMENT IN THE UNITED STATES* 2, 4 (1976).

failures or externalities. And, when the government intervenes, it is limited to correcting those particular issues.²⁰⁷ Any other regulation would not serve “consumers’ interests” and, for that reason, it could not be justified.

Privacy law’s choice of a business-consumer role-relationship to frame the information economy is a structural problem. The business-consumer paradigm propagates and entrenches data collectors’ power over internet users’ normative expectations of online privacy.²⁰⁸ As Hartzog and Richards explain, “The current U.S. approach to privacy flattens the power dynamics within relationships with a giant *caveat emptor* sign.”²⁰⁹ Privacy norms rely on societal notions of what privacy expectations are “reasonable” for a relationship.²¹⁰ But within a neoclassical business-consumer relationship, social norms are inapposite; expectations are reduced to the business’s disclosures about its practices. Ari Ezra Waldman expounds that “[p]rivacy law’s performances are constructions of industry.”²¹¹ At a structural level, the business-consumer relationship places data collectors in a conceptually and legally legitimated position to determine the privacy internet users may reasonably expect. Privacy is in effect de-normalized and, instead, managed. The profit-driven data imperative Zuboff documents in *Surveillance Capitalism* flows from the legitimacy this role-relationship confers.

Online privacy law’s choice of a business-consumer relationship threatens the sort of privacy and roleplay on which identity formation depends. Numerous scholars, especially Julie Cohen, have identified how data surveillance mortifies emergent selfhood.²¹² It eviscerates the boundaries between behaviors in different contexts and relationships in service of rendering individuals as sets of acontextual data points. The business-consumer relationship both enables and legitimates this practice. After all, collecting and monetizing personal information is in data collectors’ profit interest, and how they go about that practice is a matter of business discretion. Placing internet users in a neoclassical “consumer” role when it comes to online privacy also collapses the mobility between social roles, through selective exposure, that makes individuals complex persons. Individuals typically explore facets of their

²⁰⁷ Joshua D. Wright, *The Antitrust/Consumer Protection Paradox: Two Policies at War with Each Other*, 121 YALE L.J. 2216, 2218 (2012).

²⁰⁸ See Mazzurco, *supra* note 92, at 807–15.

²⁰⁹ Hartzog & Richards, *Surprising Virtues*, *supra* note 163, at 993.

²¹⁰ Post, *Social Foundations*, *supra* note 37, at 960–61.

²¹¹ Ari Ezra Waldman, *Privacy, Practice, and Performance*, 110 CALIF. L. REV. 1221, 1226 (2022) [hereinafter Waldman, *Privacy, Practice*].

²¹² Cohen, *What Privacy Is For*, *supra* note 22, at 1905, 1925.

identity by interacting across multiple social roles, partly defined by differences in privacy norms. But privacy law that protects them solely as “consumers” online enables only a binary performance of identity—as consumers or not. And, given the pervasiveness of data surveillance, withdrawal from the consumer role might require withdrawal from social life altogether.

Finally, online privacy law’s current neoclassical “business” and “consumer” roles have become “sticky.” Legal reforms not bound by court precedent—like statutory lawmaking—have exhibited a tendency to adopt the same business and consumer roles. The path online privacy has taken, from policy to agency enforcement to the courts, bears that out. Newer laws, such as the California Consumer Privacy Act and the California Privacy Rights Act (which replaced the earlier Consumer Privacy Act), reflect the same tendency.²¹³ In name, the California laws aim to protect *consumer* privacy; in practice, they maintain the perspective that data collectors should be regulated as “businesses” but pivot toward regarding internet users as data property owners. On that basis, they assume much of the same logic of information privacy law to date.²¹⁴ The California laws depart from the existing notice-and-choice framework only partially—to specify what businesses must disclose about their information practices and to afford “consumers” additional control rights: to access, amend, correct, delete, and block the sale or disclosure of their personal information.²¹⁵ As for the business-consumer relationship, it is data collectors’ prerogative to decide what information they collect and how they will use it. Internet users are left to satisfy their privacy preferences through their individual decisions. Online privacy’s business-consumer orientation also bolsters political resistance to reforms that diverge. For example, “Since its introduction in June [2022], the American Data Privacy and Protection Act” (ADPPA), which would afford individuals rights to control and bind data collectors to loyalty duties, “has been one of the most lobbied [against] bills in Congress.”²¹⁶

²¹³ California Consumer Privacy Act of 2018, CAL. CIV. CODE § 1798.100 (2023); California Privacy Rights Act (CPRA) of 2020, 2020 Cal. Legis. Serv. Prop. 24 (ratified via referendum vote as Prop. 24 in general election of Nov. 3, 2020, codified as amended in CAL. CIV. CODE §§ 1798.100–.199.100 (2023)).

²¹⁴ CAL. CIV. CODE §§ 1798.100–.199.100; BRENT A. OLSON, CAL. BUS. LAW DESKBOOK § 17:38 (2023).

²¹⁵ CAL. CIV. CODE § 1798.110; CPRA §§ 5–11.

²¹⁶ Karl Evers-Hillstrom & Rebecca Klar, *Corporate Lobbying Could Imperil Sweeping Data Privacy Bill*, THE HILL (Aug. 3, 2022, 5:20 AM), <https://thehill.com/lobbying/3585322-corporate-lobbying-could-imperil-sweeping-data-privacy-bill> [<https://perma.cc/MJ38-5B3L>].

III. REWRITING PRIVACY LAW'S ROLE-SCRIPTS

If lawmakers are going to alleviate the threat of private surveillance to emergent selfhood, they will have to shift the paradigm through which they view the information economy. Part of that shift will require reimagining the social roles at play in the relationship between data collectors and internet users. This Part examines the new role-scripts that two current privacy reform proposals author: data protection and information fiduciary approaches. In doing so, it builds a methodology for lawmakers to approach conscientiously privacy law's role-scripts. It also highlights the limited extent to which either of these role-scripts supports complex identity formation.

This Part then proposes a different way to script privacy law's social roles. This alternative proposal—"privacy governance law"—scripts a privacy governance relationship between data collectors and internet users. A privacy governance relationship has the potential to guide data collectors to be responsive to internet users' will and empower users to participate in decision-making about information practices. It is not a perfect solution, but neither are data protection and information fiduciary reforms. Even so, a privacy governance relationship better equips law to support the kinds of privacy and roleplay fundamental to emergent selfhood.

A. *Lessons for Reform from a Social Role Lens*

Richards and Hartzog argue in favor of a "relational turn" for privacy law.²¹⁷ They assert lawmakers should "look[] at how the people who expose themselves and the people that are inviting that disclosure relate to each other" and ascribe duties and rights to the parties based on the qualities of that relationship, especially power asymmetries.²¹⁸ As Sections II.B and II.C set out, privacy law is repletely relational—even as it applies to online interactions. The problem is the particular relationship policymakers chose to frame internet users' interactions with online intermediaries: as a neoclassical business-consumer relationship. Waldman stresses it is time for privacy discourse to focus on what should be to "change baseline assumptions about what privacy is for."²¹⁹ In Solove's words, "By redefining relationships, the law would make a

²¹⁷ Richards & Hartzog, *Relational Turn*, *supra* note 162, at 493 (emphasis omitted).

²¹⁸ *Id.*

²¹⁹ Waldman, *Privacy, Practice*, *supra* note 211, at 1273.

significant change to the architecture of the information economy.”²²⁰ A core component of that pivot will be a change to the social roles online privacy law scripts for data collectors and internet users.

There are multiple reasons the neoclassical business-consumer relationship is an unfit frame for privacy law in an information economy. First, internet users’ interactions with data collectors are thoroughly heterogenous. As a matter of analogy, one might consider online relationships in terms of common advertising “verticals,”²²¹ like real estate (e.g., Zillow, StreetEasy), restaurants (e.g., Seamless, Uber Eats), travel (e.g., Expedia, Uber), and fitness (e.g., Peloton, ClassPass). The heterogeneity of internet users’ interests, values, and needs as they interact with these entities suggests there should be a number of relationships with different standards of appropriate information practices. But online privacy law’s business-consumer relationship eviscerates relationship diversity in favor of a singular social structure that empowers all of these entities to decide their information practices (however surveillant) unilaterally.

Second, in terms of social theory on privacy and identity, a universal business-consumer relationship enacts an empty form of autonomy because it protects individual choices as to compliance with norms data collectors decide heteronomously. A large part of autonomy’s value lies in the play it enables. Autonomous individuals choose to play certain social roles, withdraw from them, or oppose their established scripts, all the while participating in a complex social practice that keeps roles dynamic. Privacy, as a matter of consumers’ autonomous choice within businesses’ profit-driven normative framework, reduces multifaceted identity to a consumer-or-not binary.

Online privacy did not have to be this way. Writing contemporaneously with commercial internet’s emergence, Schwartz identified “the true promise of the Internet [is] not . . . as a place for electronic commerce, but as a forum for deliberative democracy.”²²² Schwartz presciently asserted:

Participants in cyberspace need access to public, quasi-public, and private spaces where they can engage in civic dialogue and the process of self-definition. Moreover, these information territories must be well-defined with enforceable rules that set different boundaries for different entities In the Information Age, one-size privacy will not

²²⁰ DANIEL J. SOLOVE, *THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE* 104 (2004) [hereinafter SOLOVE, *DIGITAL PERSON*].

²²¹ 7 *Advertising Verticals to Target in 2022*, BROADSTREET (Apr. 12, 2022), <https://broadstreetads.com/7-advertising-verticals-to-target-in-2022> [https://perma.cc/N9VR-CCH2].

²²² Schwartz, *Privacy and Democracy*, *supra* note 36, at 1649.

be adequate for all situations; our task is to develop nuanced concepts for use in charting and fixing the bounds of different privacy domains.²²³

A social role lens supplies some principles for privacy law reform that build off Schwartz's early insight. Different social relationships call for different role-based privacy norms. In fact, role-based privacy norms help constitute the multiple relationships that contribute to individuals' sense of self. Online privacy law must support and sustain varied relationships with online intermediaries, governed by differing privacy norms.²²⁴

The *role of privacy law* in an information economy should be to support the roleplay that fuels complex identity formation. In a sense, this affords support for "sectoral" privacy laws over omnibus laws that paper over the multiplicity of online privacy relationships. It also directs omnibus laws to be flexible enough to enable a variety of role-relationships to flourish. One key feature must be a legal limit on data surveillance. Otherwise, the prospect (and current reality) of internet users' total online exposure eliminates the boundaries between roles and potential for withdrawal requisite to a multifaceted, transformative identity.

The social roles privacy law chooses to characterize its legal subjects (privacy law's role-scripting function) are highly consequential in that regard. The rights and responsibilities privacy law affords will be judged against the precommitments manifest in privacy law's role choices; the precedents courts rely on to resolve disputes over data collectors' information practices will differ based on their perception of the parties' roles. And, as online privacy law's current business-consumer role-relationship demonstrates, privacy law's role-scripts structure the relationship between data collectors and internet users, for worse or for better.

B. *Privacy Law Reform as Legal Role-Scripting*

The following subparts draw out the roles envisioned by two prominent privacy reform proposals—data protection and information fiduciaries. They examine each reform's role constructions by

²²³ *Id.* at 1667, 1671.

²²⁴ *But see* Solove, *Virtues of Knowing Less*, *supra* note 30, at 1050 (arguing law should not necessarily "actively promote role-playing" because "people would be uncomfortable around those who . . . radically chang[e] their personalities in every situation"). *Compare id.*, with *supra* Sections I.A–B (explaining complex identity depends on the ability to play multiple social roles, which surveillance threatens).

interrogating the statements they make about the entities they regulate and the public they serve. These include statements expressed about the governed relationship's legal attributes (e.g., power asymmetry, dependency) and parties' relevant attributes and interests (e.g., knowledge, trust), as well as role characteristics implied from the rights, duties, behavioral constraints, and entitlements that attach to those who meet expressed attributes. The subparts then analyze how each reform's social roles will likely guide behavior beyond explicit legal requirements, affect the play necessary for identity formation, and direct future legal reform.

1. Data Protection

Data protection law has become the predominant mode of U.S. privacy reform at the state level. Between 2018 and 2024, nineteen states passed comprehensive “data privacy” or “data protection” laws.²²⁵ Though they differ to a certain extent on substantive requirements and prohibition, they follow the same basic framework for the roles at play in a “data protection” relationship—casting data collectors as “businesses” and individuals as “data property owners.” The California Privacy Rights Act (CPRA) serves as a good example.²²⁶

The CPRA's prefatory language and operative provisions show a shift from a lingering “business-consumer” role relationship to a “data business-property owner” role relationship. The Act describes as “fundamental” to the right to privacy “the ability of individuals to control the use, including the sale, of their personal information.”²²⁷ It characterizes the data protection relationship as a “contractual arrangement” in which goods or services are exchanged for personal information.²²⁸ The problem is “consumers often have no good way to value the transaction.”²²⁹ On this basis, the law affords “consumers” a right to notice of businesses' information practices and a right to access, correct, delete, and stop the sale or disclosure of their personal information.²³⁰ Businesses' responsibilities correspond to these nominatively “consumer” rights. Additionally, “[B]usiness[es] may offer

²²⁵ See *supra* note 1; Andrew Folks, *US State Privacy Legislation Tracker*, IAPP (July 22, 2024), <https://iapp.org/resources/article/us-state-privacy-legislation-tracker> [https://perma.cc/PYE5-MDQS].

²²⁶ CAL. CIV. CODE § 1798.100 (2023).

²²⁷ CPRA § 2(A).

²²⁸ *Id.* § 2(E).

²²⁹ *Id.*

²³⁰ *Id.* §§ 2(h), 3(A).

financial incentives, including payments to consumers as compensation” for the collection . . . [,] sale[,] . . . sharing, . . . or . . . retention of [their] personal information.”²³¹ These rights and responsibilities aim to “place the consumer in a position to knowingly and freely negotiate with a business over the business’ use of the consumer’s personal information.”²³²

Though the California law purports to afford “consumer” rights, the substance of its regulation and its characterization of the data protection relationship bear a much stronger resemblance to a property relationship. Any description of a property relationship is, no doubt, contingent and contested.²³³ The prevailing theory of a property relation, reflected in the Restatement of the Law of Property, is that it denotes “legal relations between persons with respect to a thing.”²³⁴ Following this account, scholars typically characterize property owners as interested in “control,” expounded in various ways.²³⁵ For Blackstone, “control” manifested in “sole and despotic dominion.”²³⁶ Whereas for Hohfeld, property relations were “a bundle of entitlements regulating relations among persons concerning a valued resource.”²³⁷ A.M. Honoré classified these entitlements as “right[s] to possess” (i.e., exert control), use, manage, receive income from, alienate, and security in one’s property, among other things.²³⁸

State laws’ data protection relationship shares many of those characteristics.²³⁹ It situates data protection within a relationship of

²³¹ *Id.* § 11(b)(1) (amending CAL. CIV. CODE § 1798.125).

²³² *Id.* § 3(C)(3).

²³³ Meghan L. Morris, *Property’s Relations: Tracing Anthropology in Property Theory*, 73 ALA. L. REV. 767, 775–76 (2022); Anna di Robilant, *Property: A Bundle of Sticks or a Tree?*, 66 VAND. L. REV. 869, 873–74 (2013). Property scholars have pointed out that property relationships can serve any number of values, “such as autonomy, democracy, justice, community, and human flourishing.” Morris, *supra* note 233, at 772; see David W. Opderbeck, *Social Network Analysis of Trade Secrets and Patents as Social Relations*, 41 AIPLA Q.J. 355, 376 (2013).

²³⁴ David Frisch, *Remedies as Property: A Different Perspective on Specific Performance Clauses*, 35 WM. & MARY L. REV. 1691, 1704 (1994) (quoting RESTATEMENT OF PROP. ch. 1, intro. note at 3 (AM. L. INST. 1936)); see Joseph William Singer, *The Reliance Interest in Property*, 40 STAN. L. REV. 611, 635–36 (1988); Morris, *supra* note 233, at 772; di Robilant, *supra* note 233, at 880.

²³⁵ James Grimmelmann & Christina Mulligan, *Data Property*, 72 AM. U. L. REV. 829, 847 (2023); Singer, *supra* note 234, at 636; Frisch, *supra* note 234, at 1707; Nestor M. Davidson, *Property and Relative Status*, 107 MICH. L. REV. 757, 769 (2009).

²³⁶ Singer, *supra* note 233, at 637 (quoting 2 WILLIAM BLACKSTONE, COMMENTARIES *2). By contrast, Joseph Singer emphasizes the many limitations property laws (such as nuisance laws) place on property owners’ “use and enjoyment of their property.” *Id.* at 641–43.

²³⁷ di Robilant, *supra* note 233, at 871; Singer, *supra* note 234, at 663.

²³⁸ Frisch, *supra* note 234, at 1707–08. “Security” is explained as a right against unconsented “expropriat[ion] by a nonowner without first obtaining [the owner’s] permission.” *Id.*

²³⁹ See *supra* notes 226–232 and accompanying text.

economic exchange, where personal information is a potentially compensable thing of value, over which individual consumers rightfully have control in various forms.

Data protection law in Europe, which has a longer legacy and more extensive articulation, generally accords. In Europe, data protection is typically characterized as a “fundamental” or “human right[.]”²⁴⁰ which, at face value, seems qualitatively different than a “property right.” The connection lies just below the surface. First, European law, historically and in its newest forms, affords “data subjects” the same sorts of rights the CPRA affords “consumers.”²⁴¹ And, in practice, it entrenches “data controllers” prerogative to unilaterally decide their collection and use of “data subjects” personal information,²⁴² as long as those “data subjects” have given consent. Second, it is not so far-fetched to consider “property rights” a type of “fundamental” or “human right.” Hegel, for instance, tied “mastery over objects” to the development of “free will.”²⁴³ And the U.S. Constitution protects the rights of property owners under the Fifth Amendment.

Data protection laws cast internet users as “data property owners” interested in controlling information about themselves.²⁴⁴ On the other end of the “contractual arrangement” are data businesses²⁴⁵ which follow

²⁴⁰ Mistale Taylor, *The EU's Human Rights Obligations in Relation to Its Data Protection Laws with Extraterritorial Effect*, 5 INT'L DATA PRIV. L. 246, 247 (2015).

²⁴¹ European data protection laws arguably derive from the U.S. Department of Health, Education, and Welfare (HEW) Fair Information Practices, vis-à-vis the 1980 Organization for Economic Cooperation and Development guidelines. SOLOVE, DIGITAL PERSON, *supra* note 220, at 104–05; Steven S. McCarty-Snead & Anne Titus Hilby, *Research Guide to European Data Protection Law*, 42 INT'L J. LEGAL INFO. 348, 360 (2014).

²⁴² McCarty-Snead & Hilby, *supra* note 241, at 361.

²⁴³ JEREMY WALDRON, THE RIGHT TO PRIVATE PROPERTY 353 (1988).

²⁴⁴ Grimmelmann & Mulligan, *supra* note 235, at 859; Julie E. Cohen, *How (Not) to Write a Privacy Law*, KNIGHT FIRST AMEND. INST. AT COLUM. UNIV. (Mar. 23, 2021), <https://knightcolumbia.org/content/how-not-to-write-a-privacy-law> [<https://perma.cc/ZTY9-NZJ5>] [hereinafter Cohen, *Privacy Law*]; Robert C. Post, *Privacy, Speech, and the Digital Imagination*, in FREE SPEECH IN THE DIGITAL AGE 104, 107 (Susan J. Brison & Katharine Gelber eds., 2019) [hereinafter Post, *Digital Imagination*] (“The point of data privacy is to endow data subjects with the appropriate level of control over the use of their personal data. It is irrelevant whether data subjects suffer material or psychological harm from failure to comply with fair information practices, because damage is conceptualized as losing control to which data subjects are otherwise entitled.” (footnote omitted)); Robert C. Post, *Data Privacy and Dignitary Privacy: Google Spain, the Right to Be Forgotten, and the Construction of the Public Sphere*, 67 DUKE L.J. 981, 993–94 (2018) [hereinafter Post, *Google Spain*]; Daniel J. Solove, *The Myth of the Privacy Paradox*, 89 GEO. WASH. L. REV. 1, 5–6 (2021).

²⁴⁵ See CAL. CIV. CODE § 1798.100(a) (2023) (directing obligations to “[a] business that controls the collection of a consumer’s personal information”); *id.* § 1798.140(v)(1) (2024) (defining “[p]ersonal information” as information that “relates to . . . a particular consumer or household.”).

an instrumental logic: gathering, processing, and using personal information (as a valuable resource) to pursue organizational goals.²⁴⁶

Facebook and Google's behavioral advertising systems are apt examples of data businesses. The two platforms collect information about internet users when they visit the platforms' webpages, applications, or others that embed the platforms' web trackers.²⁴⁷ They collect details such as the links individuals click, the amount of time they spend on a particular screen, their mouse movements, the text they type in fields, and the individuals with whom they interact.²⁴⁸ The platforms aggregate this information about individuals to draw insights about their likely attributes, behaviors, and interests.²⁴⁹ They monetize the information by providing advertisers with tools that enable them to target their ads to particular audiences that share certain demographic features, affinities, or proclivities.²⁵⁰ All throughout the behavioral advertising cycle, the platforms make decisions about the information they gather and how they will process and use it based on their overriding organizational goal—advertising profit.²⁵¹

Privacy law in service of this role-relationship renders internet users “market participants” in individuated negotiations with data collectors over licenses to or sales of their personal information.²⁵² It supports a set of privacy norms in line with a data business-property owner relationship. These include, for example, the expectation that internet users should decide individually whether to allow data collectors “access” to their personal information and take action to terminate data collectors’

²⁴⁶ Post, *Digital Imagination*, *supra* note 244, at 107; Post, *Google Spain*, *supra* note 244, at 993–94. Notably, the American Data Privacy Protection Act (ADPPA) covers entities beyond for-profit commercial enterprises, such as not-for-profit organizations that would have otherwise been outside the Federal Trade Commission's jurisdiction. American Data Privacy and Protection Act, H.R. 8152, 117th Cong. § 2(9) (2022).

²⁴⁷ See, e.g., *Privacy Policy*, META (June 26, 2024), <https://www.facebook.com/privacy/policy> [<https://perma.cc/P5MU-F9HK>]; *Privacy & Terms*, GOOGLE (Mar. 28, 2024), <https://policies.google.com/privacy> [<https://perma.cc/W9J5-NQMA>]; Dina Srinivasan, *The Antitrust Case Against Facebook: A Monopolist's Journey Towards Pervasive Surveillance in Spite of Consumers' Preference for Privacy*, 16 BERKELEY BUS. L.J. 39, 70–76 (2019); JUSTIN BROOKMAN, CONSUMER REPS.: DIGIT. LAB, UNDERSTANDING THE SCOPE OF DATA COLLECTION BY MAJOR TECHNOLOGY PLATFORMS 16 (2020); Complaint at 10, *Rodriguez v. Google LLC*, No. 20-cv-4688 (N.D. Cal. July 14, 2020).

²⁴⁸ See BROOKMAN, *supra* note 247, at 8, 16.

²⁴⁹ Cohen, *Privacy Law*, *supra* note 244; Sandra Wachter & Brent Mittelstadt, *A Right to Reasonable Inferences: Re-Thinking Data Protection in the Age of Big Data and AI*, 2019 COLUM. BUS. L. REV. 494, 506–09 (2019); Louise Matsakis, *Facebook's Targeted Ads Are More Complex Than It Lets on*, WIRED (Apr. 25, 2018, 4:04 PM), <https://www.wired.com/story/facebook-targeted-ads-are-more-complex-than-it-lets-on> [<https://perma.cc/6HB5-SE3W>].

²⁵⁰ Matsakis, *supra* note 249.

²⁵¹ ZUBOFF, *supra* note 20, at 15–16.

²⁵² Grimmelmann & Mulligan, *supra* note 235, at 860 (emphasis added).

access or use when it no longer serves their self-interest. It is wrong for data businesses to take data property owners' personal information without their permission. But, once data businesses have lawful access, they have legitimate authority to decide, in their sole discretion, how they will use or share that personal information. (Again, it is up to data property owners to rescind permission if they disagree with data businesses' use.) Data businesses' personal information practices—ranging from sharing personal information for surreptitious political influence,²⁵³ to selling identifying information together with comprehensive, precise geolocation history²⁵⁴—do not implicate societal notions of appropriate uses of personal information.

An internet user could reasonably assert they are injured when, for instance, they discover Google retained their search history though they demanded that Google delete it.²⁵⁵ But they could not reasonably assert Google acted inappropriately by sharing their search history with credit rating organizations before they demanded deletion. The law's relationship framing instead promotes that kind of behavior. Much like a business-consumer relationship, the data business-property owner relationship obfuscates public concerns that data collectors may use personal information in ways they find disrespectful or distressing, such as when Facebook allowed researchers to run an experiment "leading people to experience . . . emotions without their awareness."²⁵⁶ Framing privacy law around a data business-property owner relationship calls into question whether these claims of privacy invasion concern privacy at all.

The data business-property owner relationship guides data collectors to make these sorts of decisions and internet users to accept them. The relationship suggests it is unreasonable for individuals to contest data collectors' decisional authority over their personal information collection and use. It thus leaves largely intact the power imbalance characteristic of online privacy law's business-consumer relationship.²⁵⁷

²⁵³ Nicholas Confessore, *Cambridge Analytica and Facebook: The Scandal and the Fallout So Far*, N.Y. TIMES (Apr. 4, 2018), <https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html> [<https://perma.cc/YC55-SS7L>].

²⁵⁴ *Kochava, Inc. v. Fed. Trade Comm'n*, No. 22-cv-00349, 2023 WL 3250496, at *1 (D. Idaho May 3, 2023).

²⁵⁵ *Cf.* Order Denying Motion to Dismiss at 1055–59, *Brown v. Google LLC*, 525 F. Supp. 3d 1049 (N.D. Cal. 2021) (No. 20-cv-3664) (outlining plaintiff's argument that Google Chrome browser's collection of personal information—including web browsing history—while users are in "Incognito mode" subverts their control).

²⁵⁶ Adam D.I. Kramer, Jamie E. Guillory & Jeffrey T. Hancock, *Experimental Evidence of Massive-Scale Emotional Contagion Through Social Networks*, 111 PROC. NAT'L ACAD. SCI. 8788, 8788 (2014).

²⁵⁷ Richards & Hartzog, *Relational Turn*, *supra* note 162, at 495.

By extension, a data protection relationship does not improve much on the business-consumer relationship when it comes to roleplay and identity formation. Unlike the business-consumer relationship, the data protection relationship is structurally antagonistic. It imagines data businesses have an extraction imperative—a maximal approach to data collection and use to serve their profit motives—whereas property owners seek to exert control over the extraction of their personal information. This is a slight improvement in that it at least appreciates individuals must be able to withdraw from the relationship, which may offer some opportunity for creative reflection. But the data protection relationship's main weakness is its lack of sociality; it conceives of businesses and property owners as atomized individual actors in an economic exchange, rather than a relationship characterized by acts of respect and intimacy and plagued by power asymmetry.²⁵⁸ It is also a one-size-fits-all approach, such that it would work against the formation of and the ability to distinguish between multiple role-relationships.²⁵⁹ Instead, it construes all online relationships as economic exchanges over personal information.

There are a few tracks further privacy lawmaking could take if it responds to a data business-property owner relationship. Much like the business-consumer relationship, law might require additional, clearer, or more detailed disclosures from data collectors about their information practices.²⁶⁰ This is reflected in the CPRA. It might also endow property owners with additional rights to control information about them, whether more extensive or more granular. Law might, for instance, require data collectors to provide individuals with mechanisms to prevent data collectors from collecting personal information from them in the first instance, such as the “Do Not Track” proposal floated in 2010.²⁶¹ It might also endow individuals with the right to refuse certain uses of their information, along the lines of the current self-regulatory initiative to provide website visitors with the ability to opt out of websites' use of cookies for particular purposes, such as site functionality, analytics, and marketing.²⁶² Law might also tinker with internet users' rights to alienate

²⁵⁸ See Kenneth A. Bamberger & Deirdre K. Mulligan, *Privacy on the Books and on the Ground*, 63 STAN. L. REV. 247, 298 (2011) (“This framing, moreover, often provides no ‘decision heuristic,’ no substantive touchstone, to guide the choices of those with far greater power to shape privacy’s treatment” (footnote omitted)).

²⁵⁹ See Schwartz, *Privacy and Democracy*, *supra* note 36, at 1660.

²⁶⁰ See generally CPRA; Council Regulation 2016/679, General Data Protection Regulation, 2016 O.J. (L 119) 1 (EU) ¶ (11)–(14).

²⁶¹ Joel R. Reidenberg et al., *Disagreeable Privacy Policies: Mismatches Between Meaning and Users’ Understanding*, 30 BERKELEY TECH. L.J. 39, 50 (2015).

²⁶² Jon Healey, *What Are Those Annoying Website Popups About Cookies? And What Should You Do About Them?*, L.A. TIMES (Sept. 1, 2021, 8:00 AM), <https://www.latimes.com/business/>

their personal information. Schwartz, for example, has long advocated for legal “inalienabilities” to accompany a “[p]roprietized personal information” regime: “[N]amely, a restriction on the use of personal data combined with a limitation on their [further] transferability.”²⁶³

Law that responds to this relationship is only justified in limited circumstances. As Schwartz writes, “[R]estrictions must respond to concerns about private market failure[s].”²⁶⁴ That is to say, the possibility of any of these further reforms (and the legitimacy of the CPRA) likely depend on some evidence of negative externalities of businesses’ information-handling decisions, personal information as a public good, data business-property owner negotiations involving significant transaction costs, or other similar impediments to perfect competition in personal information.²⁶⁵

2. Information Fiduciaries

In 2004, Solove made a radical proposal: that law should regulate the companies that collect and use individuals’ personal information as fiduciaries.²⁶⁶ Balkin, Richards, and Hartzog further developed that proposal,²⁶⁷ adopting the view that privacy is a quality of “relationships of trust” in which information is divulged, not a quality of information

technology/story/2021-09-01/what-are-website-cookies-how-do-they-impact-internet-data [https://perma.cc/H5LE-2DTC]. Though no U.S. law requires websites to enable users to control the collection of cookies, European laws, including the e-Privacy Directive and the General Data Protection Regulation (GDPR), require as much for websites targeting EU residents and member countries have enacted more specific requirements. See Council Regulation 2016/679, General Data Protection Regulation, 2016 O.J. (L 119) 1 (EU) ¶ (30); Council Directive 2009/136, art. 2(5), 2009 O.J. (L 337) 11, 30 (EC) ¶ (66) [hereinafter e-Privacy Directive]; *Cookies et Autres Traceurs: La CNIL Publie des Lignes Directrices Modificatives et sa Recommendation [Cookies and Other Trackers: The CNIL Publishes Amended Guidelines and its Recommendation]*, CNIL (Sept. 29, 2020), <https://www.cnil.fr/fr/cookies-et-autres-traceurs-la-cnil-publie-des-lignes-directrices-modificatives-et-sa-recommandation> [https://perma.cc/32CH-GFLZ].

²⁶³ Schwartz, *Property, Privacy*, *supra* note 22, at 2095.

²⁶⁴ *Id.* at 2096; see Singer, *supra* note 234, at 634.

²⁶⁵ See generally Erik Bækkeskov, *Market Failure*, BRITANNICA MONEY (Sept. 30, 2019), <https://www.britannica.com/money/topic/market-failure> [https://perma.cc/XNG8-MABG].

²⁶⁶ SOLOVE, *DIGITAL PERSON*, *supra* note 220, at 103.

²⁶⁷ Jack M. Balkin, *Free Speech Is a Triangle*, 118 COLUM. L. REV. 2048–54 (2018) [hereinafter Balkin, *Triangle*]; Jack M. Balkin, *Information Fiduciaries and the First Amendment*, 49 U.C. DAVIS L. REV. 1183, 1205–09, 1225–30 (2016) [hereinafter Balkin, *Information Fiduciaries*]; Woodrow Hartzog & Neil Richards, *Privacy’s Constitutional Moment and the Limits of Data Protection*, 61 B.C. L. REV. 1687, 1750 (2020) [hereinafter Hartzog & Richards, *Privacy’s Constitutional Moment*]; Neil Richards & Woodrow Hartzog, *Taking Trust Seriously in Privacy Law*, 19 STAN. TECH. L. REV. 431, 457–58 (2016); Neil Richards & Woodrow Hartzog, *A Duty of Loyalty for Privacy Law*, 99 WASH. U. L. REV. 961, 964–67 (2021) [hereinafter Richards & Hartzog, *Loyalty*].

itself.²⁶⁸ Relationships of trust range broadly and they are protected differently by law. Consider the distinct evidentiary rules governing privileged communications between spouses, attorneys and clients, and psychotherapists and patients.²⁶⁹

Law imposes fiduciary obligations in the context of particular relationships of trust marked by one participant's dependence on the other and an imbalance of power and knowledge between the two.²⁷⁰ Traditional fiduciary relationships in law include those between lawyer and client, doctor and patient, and real estate buyer's agent and buyer.²⁷¹ In each of these relationships, professionals providing services have knowledge and skills the beneficiaries do not, they must collect information from beneficiaries to provide them with services, and beneficiaries are ill-equipped "to monitor professional[s] actions] and assess risk."²⁷² "Because of the asymmetr[ies]" of power and knowledge within the relationship, beneficiaries have no alternative but to "trust[professionals] to act in . . . [beneficiaries'] best interest."²⁷³ In these sorts of relationships, law typically imposes two obligations on professionals: a duty of care and a duty of loyalty.²⁷⁴ "[F]iduciar[ies] must take care to act competently and diligently, so as not to harm their [beneficiaries'] interests"; they "must keep their beneficiaries' interests in mind[, and they must] act in their beneficiaries' interest."²⁷⁵

Balkin explains the characteristics of online privacy relationships that support imposing fiduciary obligations:

First, end-users' relationships with many online service providers involve significant vulnerability, because online service providers have considerable expertise and knowledge and end-users usually do not Second, we find ourselves in a position of relative dependence with respect to these companies Third, in many cases, but not all, online service providers hold themselves out as experts in providing certain kinds of services in exchange for our personal information Fourth, online service providers know that they hold

²⁶⁸ Balkin, *Information Fiduciaries*, *supra* note 267, at 1187; see SOLOVE, *DIGITAL PERSON*, *supra* note 220, at 102.

²⁶⁹ See FED. R. EVID. 501 advisory committee's note to 1974 enactment.

²⁷⁰ Balkin, *Information Fiduciaries*, *supra* note 267, at 1220; Richards & Hartzog, *Loyalty*, *supra* note 267, at 986–87.

²⁷¹ Balkin, *Information Fiduciaries*, *supra* note 267, at 1187, 1206 n.106, 1221; Ari Ezra Waldman, *Cognitive Biases, Dark Patterns, and the 'Privacy Paradox'*, 31 *CURRENT OP. PSYCH.* 105, 108 (2020); 23 *WILLISTON ON CONTRACTS* § 62:18 (4th ed. 2009).

²⁷² Balkin, *Information Fiduciaries*, *supra* note 267, at 1216–17, 1222, 1224.

²⁷³ *Id.* at 1216.

²⁷⁴ *Id.* at 1207–08; Balkin, *Triangle*, *supra* note 267, at 2051; Hartzog & Richards, *Privacy's Constitutional Moment*, *supra* note 267, at 1749–50, 1752.

²⁷⁵ Balkin, *Information Fiduciaries*, *supra* note 267, at 1207–08.

valuable data that might be used to our disadvantage -- and they know that we know it too.²⁷⁶

He asserts the law should hold data collectors to “reasonable ethical standards of trust and confidentiality” as to how they handle individuals’ information.²⁷⁷ Richards and Hartzog suggest law should impose a duty of loyalty on information fiduciaries that obliges them to act in the best interests of individuals who share information with them.²⁷⁸ The California Age-Appropriate Design Code Act sought to impose a fiduciary duty on businesses that provide online services to children, finding:

- (a) Businesses that develop and provide online services . . . that children are likely to access should consider the best interests of children when designing, developing, and providing that online service
- (b) If a conflict arises between commercial interests and the best interests of children, companies should prioritize the privacy, safety, and well-being of children²⁷⁹

Two bills in Congress also incorporate an information fiduciaries approach.²⁸⁰

The information fiduciaries proposal translates traditional notions of fiduciary relationships to fit an information economy’s context and, in effect, constructs two new social roles: data collectors as information fiduciaries and internet users as beneficiaries. Data collectors as information fiduciaries have special abilities to provide services that the average internet user does not.²⁸¹ One can imagine the difficulty an internet user would encounter if they tried to piece together their own online social network or collect information from across the web (without the assistance of a search engine). Information fiduciaries, by contrast, have specialized technical knowledge to provide these services.²⁸² Data collectors as information fiduciaries also must collect certain personal data to provide these services. A social network without any information

²⁷⁶ *Id.* at 1222.

²⁷⁷ *Id.* at 1224–25.

²⁷⁸ Hartzog & Richards, *Privacy’s Constitutional Moment*, *supra* note 267, at 1750; Richards & Hartzog, *Loyalty*, *supra* note 267, at 1000–03.

²⁷⁹ CAL. CIV. CODE § 1798.99.29 (2023).

²⁸⁰ See Data Care Act of 2021, S. 919, 117th Cong. § 3 (2021); American Data Privacy and Protection Act, H.R. 8152, 117th Cong. §§ 101–104. This is in stark contrast to Hartzog & Richards’ duty of loyalty model, which begins with a general duty to act in data subjects’ best interests and follows with more tailored subsidiary duties. See Woodrow Hartzog & Neil Richards, *Legislating Data Loyalty*, 97 NOTRE DAME L. REV. REFLECTION 356, 370 (2022).

²⁸¹ Balkin, *Information Fiduciaries*, *supra* note 267, at 1224.

²⁸² *Id.* at 1222.

about participants or a search engine unable to collect users' search queries simply could not function as such. But beyond what they must collect, information fiduciaries are also expected to collect and monetize personal information for their profit.²⁸³ Their information use becomes inappropriate, however, when it contravenes their beneficiaries' best interest.²⁸⁴ Richards and Hartzog imagine this might manifest in "strict and robust rules limiting what data can be collected, how long it could be kept, and for what it could be used,"²⁸⁵ potentially ending behaviorally targeted advertising altogether.²⁸⁶

Internet users as beneficiaries are characterized as dependent and vulnerable. Their dependency owes to data collectors providing them with services that have become indispensable to their daily lives, from email to app stores.²⁸⁷ Their vulnerability arises from the knowledge asymmetry between data collectors and internet users—data collectors collect much revealing information about internet users but maintain a high degree of secrecy about their practices.²⁸⁸ Internet users as beneficiaries are interested in two things: receiving data collectors' services (much like a patient seeks a doctor's medical treatment) and being treated consistent with the trust they grant data collectors.²⁸⁹

Proponents of information fiduciary regulations argue for data collector fiduciary obligations based on empirical observations about the relationship dynamic between data collectors and internet users but, importantly, information fiduciary obligations are aspirational. Data collectors hold themselves out as experts and so they should act as experts; they present themselves as trustworthy and thus they should honor users' trust. In this manner, the proposal operates on the level of norms, directing data collectors to behave as trustworthy experts and legitimating people's emerging notions that data collectors cause harm when they use personal information in surprising and unsettling ways, like sharing people's information with Cambridge Analytica for political psychographic profiling and targeting.

An information fiduciary-beneficiary relationship departs partially, but significantly, from a business-consumer relationship. The two similarly focus on interpersonal dynamics and expect data collectors to

²⁸³ *Id.* at 1227; Richards & Hartzog, *Loyalty*, *supra* note 267, at 971.

²⁸⁴ Richards & Hartzog, *Loyalty*, *supra* note 267, at 968.

²⁸⁵ *Id.* at 997.

²⁸⁶ *Id.* at 1019.

²⁸⁷ Balkin, *Information Fiduciaries*, *supra* note 267, at 1222.

²⁸⁸ Richards & Hartzog, *Loyalty*, *supra* note 267, at 1007–09; Balkin, *Information Fiduciaries*, *supra* note 267, at 1222–23.

²⁸⁹ Richards & Hartzog, *Loyalty*, *supra* note 267, at 964–65; Balkin, *Information Fiduciaries*, *supra* note 267, at 1222.

pursue profits and people to pursue their individual interests. However, users' interests as beneficiaries are only partially articulable in price and quality terms. Beneficiaries are also interested in being treated with respect, which is irreducible to price and quality. This interest makes the relationship socially thick—it supports the emergence and evolution of norms that govern what respect is owed within the relationship.

Behavioral expectations that attach to an information fiduciary relationship are likely to fluctuate over time as social mores, technology, and forms of interaction continue to evolve. Users may come to expect, in the near term, that data collectors should not use “dark patterns” to nudge users to overshare information or use the information they collect to manipulate people's purchasing and political decisions.²⁹⁰ These are the sorts of expectations Richards and Hartzog hope fiduciary obligations will elicit.²⁹¹ Down the line, users may expect data collectors to act as trustworthy experts beyond online privacy. For instance, they might expect data collectors to engage in content moderation using professional expertise and in users' interests. More pessimistically, the information fiduciary proposal might direct users to accept their dependency on data collectors and treat them as legitimate decision-makers when it comes to privacy and other matters.²⁹²

Despite its improvement on data protection law, information fiduciary law offers limited support for the kind of roleplay that gives rise to complex identity. Hartzog and Richards assert that: “One of the main virtues of a duty of loyalty is that it remedies the misguided approach . . . that treats all [online] interactions . . . as arms-length relationships.”²⁹³ An information fiduciary relationship is a step toward rich role-based privacy norms in that it centers and seeks to nurture normativity—specifically trust and respect. Yet, its qualities of trust, dependence, and data collectors' discretion would limit the flourishing of multiple role-relationships that diverge on those points. It is conceivable, for instance, that internet users do not (or should not) trust data brokers to make decisions in their best interests and they reject dependence on data brokers. That sort of relationship would be characterized by antagonism, opposition, and collective control. Information fiduciary law would misconstrue or misdirect that sort of relationship. Though it would enable play in multiple roles that share the basic qualities of trust,

²⁹⁰ Richards & Hartzog, *Loyalty*, *supra* note 267, at 974.

²⁹¹ Richards & Hartzog, *Loyalty*, *supra* note 267, at 974–77, 990–91.

²⁹² Lina M. Khan & David E. Pozen, *A Skeptical View of Information Fiduciaries*, 133 HARV. L. REV. 497, 535 (2019).

²⁹³ Hartzog & Richards, *Surprising Virtues*, *supra* note 163, at 989.

dependence, and unilateral discretion,²⁹⁴ it would constrain access to play in characteristically antagonistic role-relationships.

An information fiduciary relationship could support a range of legal reforms that regulate data collectors as trusted experts and serve users' interests in receiving data collectors' services and being treated with respect. Immediate legal obligations might include abstaining from manipulating beneficiaries based on knowledge about their behaviors and ensuring third parties who receive beneficiaries' information accord it the same respect.²⁹⁵ The relationship could also support lawmaking that imposes or enforces both broader and more granular standards of data collectors' professional conduct. Consider, for instance, the extensive regulation of the legal profession. Lawyers' direct fiduciary obligations to clients are one strain of many laws that regulate lawyers as trusted experts.²⁹⁶ Lawyers are also bound to standards of professional conduct as they interact with judges, deponents, and witnesses, limitations on solicitation and advertising, and requirements for educational attainment, among others.²⁹⁷

Law that similarly regards data collectors as trusted experts might impose a suite of professional standards on data collectors based on their particular services. For instance, scholars have asked how speech data collectors might follow professional ethics when engaging in content moderation, much like reputable newspapers follow journalistic ethics in publishing.²⁹⁸ An information fiduciary framing supports the possibility professional content-moderation standards could be backed up by the force of law. Law that responds to an information fiduciary relationship would be evaluated in terms of whether it improves the quality of data collectors' services to users or safeguards users' trust in data collectors. While the first consideration hews closely to lawmaking that responds to a business-consumer relationship, the second suggests reforms that safeguard trust might be justified *even if* they come at a cost to consumers' interests.

²⁹⁴ *Cf. id.* at 990.

²⁹⁵ Balkin, *Information Fiduciaries*, *supra* note 267, at 1227; Richards & Hartzog, *Loyalty*, *supra* note 267, at 990–92, 996–97.

²⁹⁶ See, e.g., N.Y. COMP. CODES R. & REGS. tit. 22, § 1200.0 (2022).

²⁹⁷ *Id.*

²⁹⁸ See, e.g., PRIYANJANA BENGANI, MIKE ANANNY & EMILY BELL, TOW CTR. DIGIT. JOURNALISM, CONTROLLING THE CONVERSATION: THE ETHICS OF SOCIAL PLATFORMS AND CONTENT MODERATION 2 (2018); Ángel Diaz & Laura Hecht-Felella, *Double Standards in Social Media Content Moderation*, BRENNAN CTR. JUST. (Aug. 4, 2021), <https://www.brennancenter.org/our-work/research-reports/double-standards-social-media-content-moderation> [<https://perma.cc/ZH99-SUND>]; JASON A. GALLO & CLARE Y. CHO, CONG. RSCH. SERV., R46662, SOCIAL MEDIA: MISINFORMATION AND CONTENT MODERATION ISSUES FOR CONGRESS 8–18 (2021).

C. *A Proposal for Privacy Governance*

There is an alternative for privacy law. It can respond to a privacy governance²⁹⁹ relationship that casts data collectors as “private governors” and internet users as “citizens.” A privacy governance relationship targets the power asymmetry that enables a small number of data collectors (e.g., large online platforms and data brokers) to set self-serving online privacy norms in their relationship with internet users. This relationship framing has received some academic interest, but it has not yet been reduced to a legislative proposal. This final subpart articulates a normative basis for “privacy governance law” and sketches the legislation it would manifest. Privacy governance law works to effect structural change that empowers internet users to engage in identity constructive roleplay, even in an information economy.

A privacy governance relationship draws from a concept of private governance that arose in the labor context during the Progressive Era. At the turn of the twentieth century, labor relationships between employers and workers involved a stark power asymmetry.³⁰⁰ Employers had the ability to unilaterally determine the terms and conditions of unskilled workers’ labor and the incentive to set those terms at employers’ lowest cost.³⁰¹ Employers had a pronounced “bargaining advantage” over workers: they had a better sense of the “state of the market and . . . demand for labor”; they had more experience and skill at bargaining; and they did not depend on any particular worker’s labor.³⁰² Scholars such as Sidney and Beatrice Webb³⁰³ conceived of this relationship as characteristically one of *governance*, albeit hegemonic governance, because of the power employers had to set and enforce rules for all manner of workplace behavior (and even some behavior outside the workplace).³⁰⁴ The state of online privacy shares or amplifies many of these qualities. Large data collectors are legally and technically

²⁹⁹ This proposal adopts the term “privacy governance” to draw a subtle but substantive distinction from Salomé Viljoen’s use of the term “data governance law.” Viljoen defines data governance law as “the legal regime that governs how data about people is collected, processed, and used.” Salomé Viljoen, *A Relational Theory of Data Governance*, 131 *YALE L.J.* 573, 577 (2021). Her construction focuses on how *law* governs data. By contrast, privacy governance concerns privacy norm-setting power within a social structure—how participants in a relationship, social group, or society collectively determine standards of appropriate information practices.

³⁰⁰ Mazzurco, *supra* note 92, at 796.

³⁰¹ *Id.* at 822.

³⁰² *Id.*

³⁰³ See SIDNEY & BEATRICE WEBB, *INDUSTRIAL DEMOCRACY* 807–50 (The Authors for the Students of the Workers’ Educational Association 1913) (1897) (representing the decision-making dynamic between employers and workers and its relationship to democratic government).

³⁰⁴ Mazzurco, *supra* note 92, at 822.

empowered to decide their information practices unilaterally; they have tremendous insight into internet users' behaviors and preferences; and they do not rely on any one user's personal information.³⁰⁵

Progressive political and legal scholars suggested democracy was imperative *within* the private governance of labor.³⁰⁶ Worker powerlessness within the workplace not only placed workers at the mercy of employers to be able to sustain their lives, but also risked transforming society "into a nation of robots, unfit to perform the duties which a democratic government demanded of its citizens."³⁰⁷ Participation in workplace decision-making, by contrast, would be an exercise of citizenship that might motivate those engaged to become more active in other spheres of civic life as well.³⁰⁸ Because the labor relationship was, in important part, antagonistic, the pathway to democratic participation required workers to have "countervailing power" through collective action.³⁰⁹

Privacy law oriented around a privacy governance relationship seeks to materialize the internet's democratic potential, as Schwartz identified early on.³¹⁰ He asserted that online privacy laws should nurture "the group-oriented process of democratic deliberation and the functioning of each person's capacity for self-governance" on which democratic society depends.³¹¹ He prescribed "[p]rivacy rules for cyberspace [tha]t set aside areas of limited access to personal data in order to allow individuals, alone and in association with others, to deliberate about how to live their lives."³¹² To that end, Schwartz proposed Fair Information Practices (FIPs) for online privacy.³¹³ Though FIPs as initially conceived contained a range of protections, including data minimization and a right to correct records, in early practice, they were reduced to notice and consent.³¹⁴

³⁰⁵ *Id.* at 824.

³⁰⁶ *Id.* at 827.

³⁰⁷ *Mr. Justice Brandeis, Competition and Smallness: A Dilemma Re-Examined*, 66 *YALE L.J.* 69, 73 (1956).

³⁰⁸ *Id.* at 73–74, n.25.

³⁰⁹ Mazzurco, *supra* note 92, at 827.

³¹⁰ Schwartz, *Privacy and Democracy*, *supra* note 36, at 1648–49. Of course, not all internet users live within democratic nation-states and so they may not have expectations of democracy at all, let alone in private governance relationships. This Article proposes privacy governance law within the United States that serves American (specifically, civic republican) democratic values.

³¹¹ *Id.* at 1653.

³¹² *Id.* Schwartz's focus was on data protection law that respects and encourages an individual's capacity for decision-making to give effect to their autonomy and participate in the processes of democratic government. His "privacy as participation" model did not relate to democratic participation *within* internet users' relationship with data collectors. Schwartz, *Privacy and Participation*, *supra* note 41, at 555, 557.

³¹³ Schwartz, *Privacy and Democracy*, *supra* note 36, at 1670–72.

³¹⁴ SOLOVE, *DIGITAL PERSON*, *supra* note 220, at 104–06.

This form of privacy law also finds support in Salomé Viljoen's work on relational data governance.³¹⁵ She argues data should be governed democratically as a collective resource because data collectors derive population-level insights, and even facially "personal" data (i.e., data about a single individual) bears on countless others who share bonds or demographic features.³¹⁶ Viljoen approves of "public management and control over existing proprietary data flows," whether through "mandated public access or . . . public trust."³¹⁷

This Article operationalizes the project of democratizing online privacy. It articulates a "privacy governance" legislative proposal that follows from the premise online data collection relationships are a form of privacy governance. A privacy governance relationship directs privacy law to enable and protect collective participation in the information handling decisions that stimulate privacy norms.³¹⁸

Privacy governance law requires a particular normative orientation: privacy law must target a problematic power structure in which data collectors hegemonically "govern" internet users' privacy in data collectors' self-interest. This normative orientation casts data collectors as privacy governors and internet users as democratic citizens. Certain rights and responsibilities—distinct from those offered by data protection and information fiduciary law—flow from redefining the data collector-internet user relationship in this way.

Data collectors as private governors set and enforce information practices in a manner that affects internet users' well-being and their capacity for collective self-determination. Their governance decisions also affect a considerable segment of the population. So conceived, the legitimacy of their governance would depend on internet users' participation in decision-making and data collectors' accountability to users. Internet users as citizens are antagonistic to hegemonic private governance; trust is not assumed but built through democratic participation and accountability. Though citizenship norms are too extensive and contested to provide a full account,³¹⁹ this proposal

³¹⁵ See generally Viljoen, *supra* note 299.

³¹⁶ *Id.* at 579.

³¹⁷ *Id.* at 645.

³¹⁸ The connection this subpart draws to the labor context runs some risk readers may interpret it as an endorsement of "Data as Labor" ("DaL"), an idea espoused by Eric A. Posner and E. Glen Weyl that data production is either a form of capital or a form of labor deserving of compensation. See ERIC A. POSNER & E. GLEN WEYL, *RADICAL MARKETS: UPROOTING CAPITALISM AND DEMOCRACY FOR A JUST SOCIETY* 205–49 (2018). This proposal does not depend on DaL, nor does it take a position on whether data collectors ought to compensate data subjects. Rather, it connects online privacy to labor on the plane of private governance: how, in each context, the social structure involves a (non-government) ruling class and a ruled class.

³¹⁹ See SARA WALLACE GOODMAN, *CITIZENSHIP IN HARD TIMES* 1–56 (2022).

envisions that internet users as citizens should be “informed participant[s]” in governance decisions.³²⁰ This interest may be described as collective autonomy.

Privacy law that responds to a privacy governance relationship should, at the most general level, work toward evening out the power asymmetry that stymies data internet users’ ability to participate in privacy norm formation online. This can be done at the federal or state level.³²¹ It can also leave undisturbed existing sectoral privacy laws. Legislation that strives to provide internet users “countervailing power” might draw from the National Labor Relations Act (which served an analogous end for workplace democracy)³²² with some necessary adaptations to match an information economy’s context.

Privacy governance law should, as a first measure, provide the subjects of commercial data collection³²³ “the fundamental right to seek better” information practices “and designation of representation without fear of retaliation” or liability under antitrust laws.³²⁴ It should provide internet users the right to self-organize into collective bargaining associations (CBAs), bargain collectively through representatives they choose, engage in other related activities, as well as abstain from self-organization and collective bargaining.³²⁵ It should also define a preliminary set of unfair information practices, which a Data Protection Agency could further elaborate.³²⁶ Privacy governance law should also oblige data collectors and authorized CBAs to bargain collectively in good faith, which requires data collectors to disclose to CBAs their relevant information practices, subject to non-disclosure protections, and limitations on user surveillance.³²⁷ It should also provide a mechanism for the enforcement of legally binding collective bargaining agreements.³²⁸

³²⁰ *Id.* at 35.

³²¹ There are certain limits to state-level privacy governance law. For instance, it would necessarily be limited to organizing efforts of internet users residing in that state. It might also present compliance challenges for online platforms because they operate nationally (or internationally). However, there has been quite a lot of legislative momentum for state privacy laws and state-level reform that might serve as an instructive test case for future federal reform.

³²² 29 U.S.C. § 151–169.

³²³ This proposal envisions that rights would be reserved to human subjects of data collection and commercial exploitation in the U.S.

³²⁴ See *Guidance: National Labor Relations Act*, NLRB, <https://www.nlrb.gov/guidance/key-reference-materials/national-labor-relations-act> [<https://perma.cc/SZQ7-NM4P>].

³²⁵ See 29 U.S.C. § 157.

³²⁶ See *id.* §§ 153, 158(a).

³²⁷ See *id.* § 158(d).

³²⁸ See *id.* §§ 158(d), 160.

There is, of course, a volume of details lawmakers would have to work out to draft this sort of legislation.³²⁹ Beyond filling in the gaps of this preliminary proposal, law that responds to a privacy governance relationship might construct a robust rule system to guide organizing practices and information practices online.

Data collectors' information advantage bolsters their ability to coerce privacy protections in their favor. Rectifying the information asymmetry between data collectors and internet users will be an important component of these reforms. Internet users must know about data collectors' information handling practices—as they pertain to personal information—to have any chance to influence them. They must also be protected from surveillance that undermines good faith bargaining. Internet users' insight into how data collectors use personal information encourages participation in informed joint decision-making.

A privacy governance relationship could also support specific bans of informational practices insofar as the bans aid collective bargaining. Law might, for instance, prohibit online platforms like Facebook and Google from prospectively identifying potential CBA members and targeting them with anti-collective bargaining or self-serving messaging (e.g., “Facebook protects your privacy. A CBA might not.”). Law might also come to protect collective bargaining beyond privacy, such as in the domain of content moderation. Or it might extend its reach transnationally through treaties.

This “privacy governance” legislative proposal contrasts starkly with the European Union's recent Digital Markets Act.³³⁰ Though the Act seeks to rectify the power imbalance between “gatekeepers” and “end users,”³³¹ it relies heavily on data protection's property role-relationship. It treats personal data as a thing of value³³² that is alienable for specified purposes with the end user's consent.³³³ One of its more novel requirements—that gatekeepers must enable end users to “port[]” their data to other providers—follows from a property owner's interest in control and free alienability.³³⁴

³²⁹ See, e.g., Eugene K. Kim, *Data as Labor: Retrofitting Labor Law for the Platform Economy*, 23 MINN. J.L. SCI. & TECH. 131 (2022).

³³⁰ Council Regulation 2022/1925, Digital Markets Act, 2022 O.J. (L 385) (EU).

³³¹ *Id.*

³³² *Id.*

³³³ The Digital Markets Act contains numerous prohibitions and requirements as to gatekeepers' practices, some having little to do with personal data. Those provisions that do concern personal data, however, consistently reflect this property relation. See, e.g., *id.* ch. III, art. 5(2) (listing prohibitions on gatekeepers' practices “unless the end user . . . has given consent”); *id.* ch. III, art. 6(1) (requiring gatekeepers to provide business users with end users' personal data connected to end users' interaction with business users).

³³⁴ *Id.* ch. III, art. 6(9).

This Article's privacy governance law urges internet users to think of themselves as citizens. It would hopefully drive them to prioritize the collective good over idiosyncratic individual preferences and demand data collectors' information practices align with collectively determined social values. Citizens' relationship with private governors is simultaneously antagonistic and cooperative. There need not be the sort of presumed trust in data collectors' discretion and information fiduciary relationship demands. Rather, citizens and private governors are expected to have conflicting interests that collective bargaining can mediate. The cooperative aspect is limited to the expectation citizens *want* to engage with private governors and so intend to have an ongoing relationship. Moreover, privacy law that protects collective bargaining empowers the sort of civic participation associated with citizens because organizing into a CBA is fundamentally voluntary. Internet users will have to decide collectively which relationships with data collectors are so important as to merit collective bargaining.

The privacy law proposal outlined in this subpart faces certain limitations and challenges. For one, the proliferation of artificial intelligence (AI) and machine learning (ML) might hinder the possibility of collective bargaining or privacy norm formation more generally. Privacy relationships imply human participants, whether individually or collectively in an organization. But the concern about AI and ML is tempered by the fact that they are written and deployed by humans—at least currently—and they may be the object of negotiation rather than the subject. It may also be difficult to motivate internet users to participate in CBAs. There are preliminary efforts underway, like RadicalxChange,³³⁵ and law's expressive support might provide further motivation.³³⁶ Finally, some may assert collective bargaining would further erode online privacy if it requires CBA members to share their personal information with the CBA. This sort of critique fails to recognize the social foundation of privacy. Sharing personal information does not relinquish privacy; it is an act of participation within a privacy relationship that signals trust or intimacy. What matters is that the CBA then adheres to the privacy norms that structure its relationship with its members.

These limitations aside, privacy law in service of a privacy governance relationship has the greatest prospect of deeply empowering

³³⁵ See *Data Dignity*, RADICALXCHANGE, <https://www.radicalxchange.org/wiki/data-dignity> [<https://perma.cc/5KMP-ZZR7>].

³³⁶ Some may perceive the woeful state of tech worker unionization as an indication that internet user collective action is unlikely. However, it may instead indicate the need to update federal labor laws to include (as I suggest for internet users) a prohibition on worker surveillance that undermines worker organization.

internet users to shape the online privacy norms that contribute to their identity formation.

First, a privacy governance relationship is not one-size-fits-all. It supplies a basic structure that could be “filled in” differently depending on a particular relationship’s context. Privacy governance law focuses on the decisional process—it is a procedural intervention that targets a problematic social structure. It deliberately refrains from specifying particular “good” and “bad” privacy practices and the substantive values those practices should serve (such as, potentially, protecting vulnerable populations, generating wealth, participating in public discourse, etc.). That is because it would be reasonable for substantive objectives and obligations to vary among the diverse data collection relationships present in an information economy. The Uber driver-Uber relationship may demand characteristically different privacy norms than the Uber passenger-Uber relationship. The space for granularity, nuance, and difference supports the boundaries between multiple roles that contribute to a complex, social self.

Second, privacy governance supports internet users’ collective participation in norm formation, rather than reliance on data collectors’ discretion or unilateral authority. Participation resocializes privacy and helps fortify the link between liberal and social privacy. Users’ privacy practices become identity performances of their own choosing, both individually and collectively.

Third, a privacy governance relationship supports legal limits on data surveillance during collective bargaining or in violation of a collective bargaining agreement. These protections afford internet users the possibility of withdrawal from their relationships with data collectors to reflect and figure out how to redefine them. This is precisely the sort of roleplay that invigorates a dynamic, emergent identity.

CONCLUSION

Online privacy may be able to recover from its current dysfunctional state. The character of its recovery will depend on how privacy law re-visions the roles data collectors and internet users play in an information economy. Data protection and information fiduciary laws each promise protection and empowerment for internet users based on distinct visions of the role-relationship they are regulating. A social role lens reveals that each falls short of supporting the kind of roleplay that animates multidimensional, fluid social identities.

This Article’s original proposal for “privacy governance law” improves on that score. Privacy governance law prioritizes the importance of individuals’ complex, fluid selfhood, rather than control

over personal information for its own sake or maintaining trust in data-collection relationships—where trust might not be due. It casts data collectors as “private governors” and internet users as “citizens” in a problematic private governance relationship. It identifies the *role of privacy law* as empowering internet users to participate collectively in the development of online privacy norms. Privacy governance law would afford space for multiple role-relationships with data collectors, constituted by different privacy norms. It is also pliant enough to accommodate the emergence of new technologies or modes of online engagement. This form of privacy law offers the greatest prospect of resuscitating the emergent selfhood that data surveillance mortifies.