The Role of Privacy Law in an Information Economy

Sari Mazzurco*

*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 Salome Viljoen for their generous commentary. This Article has also benefitted from helpful feedback from the 2023 Lewis & Clark Fall Forum 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.

The Role of Privacy Law in an Information Economy

In the past five years, twelve states have passed privacy laws aimed at protecting their residents' interests in an information economy. All afford their residents "consumer rights" enforceable against the "businesses" that collect and use their personal information. None have questioned whether this is the best role of privacy law – safeguarding individual choice by correcting "market failures" in the economic exchange of personal information for services. 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 pervasive, private surveillance: the collapse of complex and fluid social identity.

Sociological literature recognizes that an individual's development of a multi-faceted concept of self depends on the ability to play different social roles across the diverse relationships in which they engage. Privacy scholarship – both sociological and legal – adds that privacy practices nurture identity constructive play by establishing boundaries between different roles and preserving individuals' ability to withdraw from their roles and reflect on those roles' content. Surveillance threatens multi-faceted selfhood by eliminating the boundaries that make social roles distinct and hindering the possibility of withdrawal from view. 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? This Article argues the answer lay 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." Privacy law should be attentive to the social roles it ascribes to the data collectors and Internet users it 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.

There are multiple role-relationships 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. It characterizes private, online surveillance 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.

INTRODUCTION

Since 2018, twelve states have passed privacy laws aimed at protecting their residents' interests in an information economy.[1] Five 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.

No states 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

---

[1] California Consumer Privacy Act (2018);California Privacy Rights Act (2020); Colorado Privacy Act (2021); Connecticut Data Privacy Act (2022); Delaware Personal Data Privacy Act (2023); Indiana Consumer Data Protection Act (2023); Iowa Consumer Data Protection Act (2023); Montana Consumer Data Privacy Act (2023); Oregon Consumer Privacy Act (2023); Tennessee Information Protection Act (2023); Texas Data Privacy and Security Act (2023); Utah Consumer Privacy Act (2022); Virginia Consumer Data Protection Act (2021).

[2] Mass. S.D. 745; Mass. S.D. 1971; Massachusetts H.D. 3245; N.J. A. 505; N.C. S.B. 525; Penn. H.B. 1201; Penn. H.B. 708.

[3] See supra note 1.

[4] See infra notes 221-226.

[5] See id.

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 multi-faceted 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 lays 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 agenda 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 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] and spousal

---

[6] George Herbert Mead, MIND, SELF & SOCIETY (1934).
[7] See infra note [x].
[8] Julie Cohen, CONFIGURING THE NETWORKED SELF 149 (2012); Anita Allen, *Coercing Privacy*, 40 WM. & MARY L. REV. 723, 754 (1999).
[9] See FED. R. EVID. 502.
[10] *Id.* 501.

relationships,[11] and sectoral laws like the Health Insurance Portability and Accessibility Act[12] and the Family Educational Rights and Privacy Act.[13] And, as Dan 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, laws also shapes *what it means to be* a spouse, patient, or student, 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 is 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 since spread to Federal Trade Commission enforcement under Section 5 of the FTC Act and jurisprudence on generalist privacy laws like the Wiretap Act and state torts. 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 criminal case against petitioner).
[12] 45 CFR Part 160; 45 CFR Part 164, Subparts A and E.
[13] 20 U.S.C. § 1232g.
[14] Daniel Solove & Neil Richards, *Privacy's Other Path: Recovering the Law of Confidentiality*, 96 Geo. L. J. 123, 134-40 (2007).
[15] See infra note [x].
[16] See *supra* notes 9-14 and accompanying text.

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.[17] These roles justify the much-decried "notice-and-consent" approach that dominates online privacy law.[18]

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.[19] 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."[20] It thwarts the roleplay that fuels dynamic identity formation.

Regaining our selves in an information economy will require lawmakers to radically 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. And there has never been a better political moment to enact such change. A recent Northern District of California held the First Amendment protects *businesses* from legal limits on the personal information they collect from children.[21]

There are multiple role-relationships other than a "business-consumer" relationship that could frame privacy rights

---

[17] See *infra* note 146 and accompanying text.

[18] See, e.g., Daniel Solove, *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. UNIV. L. REV. 1461 (2019).

[19] Shoshana Zuboff, THE AGE OF SURVEILLANCE CAPITALISM (2018).

[20] Julie Cohen, *Privacy, Visibility, Transparency, and Exposure*, 75 UNIV. CHI. L .REV. 181, 187 (2008).

[21] NetChoice v. Bonta, No. 22-cv-08861 (N.D. Cal. Sept. 18, 2023).

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 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 the 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 "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 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 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

---

[22] Julie E. Cohen, *Examined Lives: Informational Privacy and The Subject As Object*, 52 STAN. L REV. 1373, 1428-32 (2000); Daniel J. Solove, *Conceptualizing Privacy*, 90 CALIF. L. REV. 1087, 1116-19 (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); Julie E. Cohen, *What Privacy is For*, 126 HARV. L. REV. 1904, 1908-10 (2013); Helen Nissenbaum, *Privacy as Contextual Integrity*, 79 WASH. L. REV. 119, 138-40 (2004); Neil M. Richards, *Intellectual Privacy*, 87 TEX. L. REV. 387, 407-26 (2008); Priscilla M. Regan, LEGISLATING PRIVACY: TECHNOLOGY, SOCIAL VALUES, AND PUBLIC POLICY 213 (1995).

[23] George A. Akerlof et al., IDENTITY ECONOMICS: HOW OUR IDENTITIES SHAPE OUR WORK, WAGES, AND WELL-BEING 11 (2010)

various contexts.[24] As Berger and Luckmann put it, social roles are a "building block" of social reality because they give social interactions meaning and they 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's 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 doesn't meet these expectations, it's 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

---

[24] Frank Dobbin, *Economic Sociology*, *in* TWENTY-FIRST CENTURY SOCIOLOGY: A REFERENCE HANDBOOK 320 (2007); Ralf Dahrendorf, ESSAYS IN THE THEORY OF SOCIETY 35-37 (1968); Neal Gross et al., EXPLORATIONS IN ROLE ANALYSIS 59-60, 63 (1958); Bruce J. Biddle, *Recent Development in Role Theory*, 12 ANN. REV. SOC. 67, 70-71 (1986); J. Scott, *Status and Role: Structural Aspects*, *in* INT'L ENCYCLOPEDIA SOC. & BEHAVIORAL SCIS. (2001).

[25] Meir Dan-Cohen, *Between Selves and Collectivities: Toward a Jurisprudence of Identity*, 61 UNIV. CHI. L. REV. 1213, 1218-19 (1994), 1228-29; Peter L. Berger & Thomas Luckmann, THE SOCIAL CONSTRUCTION OF REALITY 60-61, 74-76 (1967).

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

[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 (2016); 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).

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's 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 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; that is to say, individuals and groups persistently clash over what social roles are and the norms that should characterize them.[33] Even

---

[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).

[31] Peter M. Hall, *Asymmetric Relationships and Processes of Power*, *in* STUDIES IN SYMBOLIC INTERACTION 273, 315 (1985); Frank Dobbin, *Economic Sociology*, in TWENTY-FIRST CENTURY SOCIOLOGY: A REFERENCE HANDBOOK 321 (2007); Jeffrey K. Hass, ECONOMIC SOCIOLOGY: AN INTRODUCTION 9 (2006); Neil Fligstein, THE ARCHITECTURE OF MARKETS 28, 36 (2018); David Arditi, *Digital Hegemony*, *in* THE DIALECTIC OF DIGITAL CULTURE 13 (2019).

[32] Hass, *supra* note 31, at 9; Mark Granovetter, *Economic Action and Social Structure: The Problem of Embeddedness*, 91 AM. J. SOC. 481, 486 (1985); Fligstein, *supra* note 31, at 27-28.

[33] Berger & Luckmann, *supra* note 25, at 61. Ideas about social roles may also differ dramatically between different communities. One could imagine, for instance, Christian

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 even if they never interact with one because they have access to cultural knowledge about a military'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 role-playing, is essential to individuals' identity formation and continual re-formation. Privacy literature historically separated concepts of privacy and identity into "liberal" and "social" accounts.[36] But, since the 1990s, more complex accounts have

---

ideas of what it means to be a parent, father, or mother diverging from secular ideas about these roles.

[34] Fligstein, ARCHITECTURE, *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 191-208 (2009); Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1609, 1647-67 (1999); Allen Westin, PRIVACY AND FREEDOM 24, 26 (1967); Mark Burdon, *Contextualizing The Tensions and Weaknesses of Information Privacy and Data Breach Notification Laws*, 27 SANTA CLARA COMP. & HIGH TECH. L.J. 63, 67-73 (2011); Richard Warner & Robert H. Sloan, "*I'll See": How Surveillance Undermines Privacy by Eroding Trust*, 32 SANTA CLARA COMP. & HIGH TECH. L. J. 221, 245-46 (2016); 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 COMP. & TECH. L.J. 1, 6-9 (1998);

demonstrated that "liberal" and the "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 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' point of view and recognizing themselves as the object of others' view.[43] Social theorist Valerie Steeves adds that "the social

---

Mark MacCarthy, *Privacy Policy and Contextual Harm*, 13 I/S: J. L. & POL'Y FOR INFO. SOC'Y 399, 405-19 (2017). "Liberal" in this application refers to liberal political philosophy that characterizes persons by their separateness. See JOHN RAWLS, A THEORY OF JUSTICE 27 (1971); ROBERT NOZICK, ANARCHY, STATE, AND UTOPIA 32-33 (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).

[38] Westin, *supra* note 36, at 7.

[39] *Id.* at 44-45.

[40] Michael Sandel, DEMOCRACY'S DISCONTENT: AMERICA IN SEARCH OF A PUBLIC PHILOSOPHY 94-100 (1996).

[41] Puri, *supra* note 36, at 498-502; Hargreaves, *supra* note 36, at 460-64. 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 decisionmaking requisite to a democratic society).

[42] Byford, *supra* note 36, at 15 (citing Frank Johnson, *The Western Concept of Self*, in CULTURE AND SELF: ASIAN AND WESTERN PERSPECTIVES 91, 129 (1985)).

[43] Byford, *supra* note 36, at 15-16 (citing Mead, *supra* note 6); Steeves, *supra* note 36, at 204 (citing Jurgen Habermas, *Individuation through Socialization: On George Herbert Mead's Theory of Subjectivity*, in POSTMETAPHYSICAL THINKING: PHILOSOPHICAL ESSAYS 153 (1992)).

negotiation of a desired boundary between self and other" can only be achieved through interaction and information-sharing.[44] Social privacy—norms that emerge about what information one should share and how the other 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 don't 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 come to know themselves by playing 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, "persons [are] 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 to withdraw.

But, as Robert Post explains, the social norms that give a relationship its shape and individuals' autonomous decisions to

---

[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 (citing Ferdinand D. Schoeman, PRIVACY AND SOCIAL FREEDOM 6 (1992)).
[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. & I.P. 61, 67-69 (2014).
[51] Allen, *supra* note 8, at 753-54.

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're 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 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 role-playing are closely connected when it comes to the practice of identity formation. As the earlier subpart explained, 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.[54] 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).[55] Liberal privacy allows individuals to modulate their exposure within a network of relationships so that they can move from one role to the next;[56] social privacy communicates what kinds of exposure are appropriate within each role.[57] Bruce Schneier writes, "Privacy isn't about hiding something. It's about being able to control how we present

---

[52] Post, *Social Foundations*, *supra* note 37, at 959.
[53] *Id.* at 973.
[54] See Solove, Virtues of Knowing Less, supra note 30, at 1037.
[55] Puri, *supra* note 36, at 498-505, 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 460-64.
[56] Hargreaves, *supra* note 36, at 476.
[57] See *supra* notes 41-50 and accompanying text.

ourselves to the world."[58] Choosing to perform social privacy in different role-relationships helps a social identity flourish.[59]

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."[60] Privacy provides individuals with "breathing room" to not have to live up to particular social roles' behavioral norms.[61] 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.[62] 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.[63]

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

---

[58] Bruce Schneier, *Crypto-Gram*, SCHNEIER ON SECURITY (Sept. 15, 2015), https://www.schneier.com/cryptogram/archives/2015/0915.html. Dan Solove has observed that privacy laws also aid role-switching and withdrawal. Solove, Virtues of Knowing Less, supra note 30, at 1037.

[59] MacCarthy, *supra* note 36, at 407-08, 419; Richard Warner & Robert H. Sloan, *Relational Privacy: Surveillance, Common Knowledge, and Coordination*, 11 UNIV. ST. THOMAS J. L. & PUB. POL. 1, 9-10 (2017).

[60] Allen, *supra* note 8, at 739.

[61] Burdon, *supra* note 36, at 113; Byford, *supra* note 36, at 24-25; MacCarthy, *supra* note 36, at 411.

[62] Allen, *supra* note 8, at 740.

[63] 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.").

identities.[64] Erving Goffman's studies of total institutions, such as prisons and asylums, demonstrate that the deprivation of privacy destroys individuals' sense of self.[65] Not only do total institutions "mortify" the self by exposing every aspect of one's life to others, they disrupt individuals' ability to keep their various roles separate.[66] Dan 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."[67] 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 [are] fully accountable to the same people for all aspects of behavior."[68] Jeffrey Reiman writes that data surveillance replicates total institutions' privacy deprivations by "render[ing] the individual perpetually visible and transparent."[69] 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.[70]

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;[71] acts of respect when someone fulfills social privacy expectations;[72] play in multiple social roles;[73] and withdrawal from particular roles.[74]

---

[64] Hargreaves, *supra* note 36, at 451; Sloan & Warner, *"I'll See"*, *supra* note 36, at 225-33.

[65] Erving Goffman, ASYLUMS 6, 23-32 (1961).

[66] *Id.* at 14-35. Paul Schwartz adds that surveillance undermines individuals' capacity for free choice: "the more that is known about an individual, the easier it is to force his obedience." Schwartz, Privacy and Participation, supra note 41, at 559-60.

[67] Solove, Virtues of Knowing Less, supra note 30, at 1038.

[68] Irwin Altman, THE ENVIRONMENT AND SOCIAL BEHAVIOR 40 (1975).

[69] 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 COMP. & HIGH TECH. L.J. 27, 39 (1995).

[70] Puri, *supra* note 36, at 490-94; Steeves, *supra* note 36, at 206.

[71] Ari Ezra Waldman, *Designing Without Privacy*, 55 HOUS. L. REV. 659, 704-05 (2018).

[72] Byford, *supra* note 36, at 12-15; Post, *Social Foundations*, *supra* note 37, at 967; MacCarthy, *supra* note 36, at 416.

[73] Steeves, *supra* note 36, at 205.

[74] Allen, *supra* note 8, at 739.

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, "the 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."[75] 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.[76] 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.[77] 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 transmission principles that stipulate the terms of the exchange.[78] A novel practice violates information privacy when it breaches a context-relative informational norm.[79] 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."[80] 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 are relevant to privacy."[81]

A focus on role reveals that, in many cases, the details that populate Nissenbaum's four parameters often flow from an

---

[75] Erving Goffman, *The Territories of the Self*, in RELATIONS IN PUBLIC 57-58 (1971).
[76] Helen Nissenbaum, PRIVACY IN CONTEXT 84-85 (2007).
[77] *Id.*
[78] *Id.* at 132-35.
[79] *Id.* at 140.
[80] *Id.* at 133.
[81] *Id.* at 142.

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.[82]

Moreover, as this Article discusses more thoroughly in Part II.A, *law* typically operates through the idiom of social role, rather than predominantly through other aspects of context. Law seeks to change the behaviors of entities acting in particular roles, rather than any entity at a car dealership during business hours.[83] It would 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 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.[84] (One who does not divulge this information might not 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., description of intimate sexual encounters, criminal activity, or

---

[82] Sloan & Warner, "*I'll See*", *supra* note 36, at 252.

[83] See Part II.A.

[84] See *The Common App*, APPLICATION GUIDE FOR FIRST-YEAR STUDENTS, https://www.commonapp.org/apply/first-year-students.

fabrications).[85] Norms (and, to an extent, law) constrain what universities may do with this information.[86] 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 look books about courses, financial aid, class composition,[87] but not about whether faculty tend to interact with one another cooperatively or adversarially.

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.[88] "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."[89] Their focus is on cooperative endeavors, where "people voluntarily limit[] their knowledge of each other" out of respect for role-based privacy norms.[90] But role-based privacy norms may also guide behaviors—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 themself.[91] 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 primarily bargaining chit.[92] The union would be well-served to know the maximum an employer could pay workers while remaining profitable, but the employer knows

---

[85] Amy Allen, *How to Write a Personal Essay for Your College Application*, HARV. BUS. REV. (Dec. 14, 2021), https://hbr.org/2021/12/how-to-a-personal-essay-for-your-college-application.
[86] See, e g., 20 U.S.C. § 1232g.
[87] See, e.g., *You Belong Here*, SMU (last accessed Mar. 6, 2023), https://hbr.org/2021/12/how-to-a-personal-essay-for-your-college-application.
[88] Sloan & Warner, "*I'll See*", *supra* note 36, at 248.
[89] *Id.* at 258.
[90] *Id.* at 224.
[91] Sari Mazzurco, *Democratizing Platform Privacy*, 31 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 793, 822-23 (2021).
[92] *Id.* at 839-40.

that revealing that detail would reduce its leverage.[93] 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.[94] 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.[95] 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.

Part II.A introduces law's role-scripting function. Part 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,

---

[93] *Id.* at 822-23.
[94] Fligstein, ARCHITECTURE, *supra* note 31, at 27.
[95] NAACP v. Claiborne Hardware, 458 U.S. 886 (1982).

articulating an idealized vision of how one should handle certain information when acting in the regulated role. Part 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 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 proposes a legislative agenda 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.[96] Modern liberal democracies typically govern entities based on a perception of their social roles.[97] There are some laws that regulate certain acts without reference to the actor's social role. For instance, whether you're 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.[98] 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 construct a preliminary social role.[99]

Some commentators argue law may only reflect settled social roles (and imperfectly at that).[100] But others recognize that

---

[96] 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*, 130 HARV. L. REV. 659, 678 (2016).

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

[98] RESTATEMENT (2D) OF TORTS § 652C; N.Y. CIV. R. CIV. L. § 50.

[99] Mitnick, *supra* note 29, at 824, 828, 831, 833, 868-69; Rehbinder, *supra* note 97, at 951-52; Dan-Cohen, *supra* note 25, at 1228-30; Huang, *supra* note 96, at 678.

[100] Harlan Fiske Stone, LAW AND ITS ADMINISTRATION 34 (1915); Paul Bohannan, *The Differing Realms of the Law*, 67 AM. ANTHROPOLOGIST 33, 35-37 (1965).

law also sometimes creates new social roles or redefines substantially existing roles' behavioral norms.[101] 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 rights and responsibilities and periodically adjusting them.[102] 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.[103]

The corporation is an emblem of legally created social roles. The corporation and the suite of roles within it all originate as legal constructs.[104] 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 to the public.[105] Corporate law defined what it means to be a "corporation" and it created many roles *within* the corporation (e.g., shareholders, officers, directors, chair, etc.), each with their own legally scripted behavioral obligations.[106] Antitrust law also contributed to the boundaries of appropriate corporate behavior.[107] And, in recent years, the Supreme Court has recognized a range of corporations' rights, such as the right to speak, fund electioneering communications, and practice religion, suggesting these are all normal social behaviors for corporations.

---

[101] Sunstein, *supra* note 96, at 923; Dan-Cohen, *supra* note 25, at 1229-30; Mitnick, *supra* note 29, at 824, 865; Stone, *supra* note 100, at 78-79, 82; Neil Fligstein, *Transformation of Corporate Control*, *in* THE NEW ECONOMIC SOCIOLOGY: A READER 408-09 (2004); William G. Roy, *Socializing Capital: The Rise of the Large Industrial Corporation in America*, *in* THE NEW ECONOMIC SOCIOLOGY: A READER 438-39, 450-51 (2004).

[102] Stone, *supra* note 100, at 78-79.

[103] *Id.*

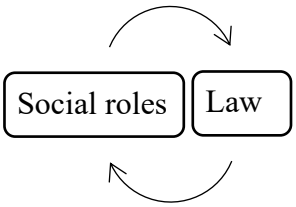
[104] *Id.* at 82; Fligstein, *Corporate Control*, *supra* note 101, 408-09; Roy, *supra* note 101, at 438-39, 450-51.

[105] Fligstein, *Corporate Control*, *supra* note 101, 408-09; Roy, *supra* note 101, at 450-51.

[106] *See, e.g.*, N.Y. BUS. CORP. L. arts. 6-7.

[107] Fligstein, *Corporate Control*, *supra* note 101, 408-09.

The legal system itself contains well-recognized examples of legally scripted social roles. Juror, defendant, prosecutor, and judge, and the behavioral norms associated with them, derive from law.[108] Law supplied the initial social meaning of these roles, but they are continually redefined as actors interact *in* the roles and *with* the roles.[109] Roberto 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 explicit and perfected bargains."[110]



Society and law define social roles dialogically. Paul Bohannan describes this phenomenon as law being perpetually, but constructively "out of phase" with society.[111] 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 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 their influence on their perceptions.[112] For example, Bert Huang conducted an experimental

---

[108] Dan-Cohen, *supra* note 25, at 1230.

[109] 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 is 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,* in COURSE CATALOG, HARV. BUS. SCHOOL (last visited Nov. 15, 2021), https://www.hbs.edu/coursecatalog/2010.html.

[110] ROBERTO MANGABEIRA UNGER, THE CRITICAL LEGAL STUDIES MOVEMENT 80, 81 (1983).

[111] Bohannan, supra note 100, at 35-37.

[112] Mitnick, *supra* note 29, at 826. *See also* Huang, *supra* note 96, at 694-95.

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.[113] His study suggests individuals often translate legal definitions into social norms on instinct, especially when norms are not settled.[114]

The possibility of legal sanctions for non-compliance augmentslaw's ability to enforce social roles and norms.[115] 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.

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 LGBT advocacy to normalize servicemembers' homosexuality, but the Trump Administration's 2019 ban of transgender persons in the military swung the pendulum the other way.

Legal definitions of social roles also delineate the scope of possible legal reform and legal claims on a particular subject.[116] For instance, when in vitro fertilization became more widely available the 1990s, courts had to decide whether gestating women had any rights to non-biological children they birth. In *Johnson v. Calvert*, the California court found that a gestating woman who refused to turn over a child to their genetic parents had no parental right to the child—she was not a "mother" but a "gestational surrogate."[117] By

---

[113] Huang, *supra* note 96, 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 citizens. Elizabeth Anderson, *Beyond Homo Economicus: New Developments in Theories of Social Norms*, 29 PHIL. & PUB. AFFS. 170, 197 (2000).

[114] See Lawrence Lessig, *The Regulation of Social Meaning*, 62 UNIV. CHI. L. REV. 943, 1030 (1995).

[115] Dahrendorf, *supra* note 24, at 42-43; Rehbinder, *supra* note 97, at 953; Dan-Cohen, *supra* note 25, at 1233; Anderson, *supra* note 113, at 193.

[116] Jack M. Balkin, *Understanding Legal Understanding: The Legal Subject and the Problem of Legal Coherence*, 103 YALE L.J. 105, 121-23 (1993).

[117] 5 Cal.4th 84, 86 (1993).

contrast, in *Perry-Rogers v. Fasano*, the New York court found 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.[118] 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 (re)vision 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 in 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. … [H]ow political actors frame [the issue] may impact the kinds of solutions proposed." The public's acceptance, rejection, or alteration of legal role-scripts foments support for or resistance to possible future reform.

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, adjudications 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.

---

[118] 276 A.D.2d 67, 73 (N.Y. App. Div. 2000).

The idea of *law* constructing social roles may seem odd, considering social roles typically stem from everyday interactions.[119] Legal prescription might seem paternalistic. But this critique misses that law largely unavoidably shape social roles because it must categorize entities—whether it re-defines existing social roles or creates them anew.[120] Scripting roles well requires attention directed 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 it is difficult to imagine how privacy law might function without regard to the roles actors play in a particular relationship or legal dispute. This Part 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 HIPAA,[121] GLBA,[122] VPPA,[123] and FERPA[124] explicitly regulate privacy within specific role relationships. Likewise, evidentiary privileges attach on the basis of one's role as a psychotherapist,[125] spouse,[126] or attorney.[127] 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 Amendment[128] and a suite of federal statutes[129] regulate the privacy relationship between the government and citizens. In the process, they articulate a vision of

---

[119] *See supra* note 32 and accompanying text.
[120] *See supra* notes 101-110 and accompanying text.
[121] 45 CFR Part 160; 45 CFR Part 164, Subparts A and E.
[122] 15 U.S.C. § 6809.
[123] 18 U.S.C. § 2710.
[124] 20 U.S.C. § 1232g.
[125] See FED. R. EVID. 501.
[126] *Id.* 502.
[127] See Trammel v. United States, 445 U.S. 40, 53 (1980).
[128] U.S. CONST. AMEND. IV.
[129] See The Privacy Act of 1974, 5 U.S.C. § 552a; The Freedom of Information Act of 1974, 5 U.S.C. § 552; The Right to Financial Privacy Act of 1978, 12 U.S.C. Ch. 35; the Electronic Communications Privacy Act of 1986, 18 U.S.C. Ch. 119.

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,[130] 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.

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 wards or property of their husbands.

This notion of wives' social and legal status animated both marital rape laws and the evidentiary privilege shielding marital communications. In the 17th 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 and contract the wife hath given up herself in this kind to her husband which she cannot retract."[131] 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 couldn't testify for or against her husband because she was considered the same legal person as her husband.

---

[130] RESTATEMENT (2D) OF TORTS § 652.

[131] Sir Matthew Hale, THE HISTORY OF THE PLEAS OF THE CROWN 629 (1736).

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 on the ground "the law should not force or encourage testimony which might alienate husband and wife, or further inflame existing domestic differences."[132] Anita Allen writes that this norm of wives' "[s]eclusion 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 … in the private sphere."[133]

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 in continued voluntary association and grounded in bilateral loyalty.[134] States began to outlaw marital rape in the 1970s and, by 1980, the Court modified *Hawkins* to allow voluntary adverse spousal testimony. It reasoned the "ancient foundations" for the rule against adverse testimony "have long since disappeared," and "when one spouse is willing to testify against the other . . . there is probably little in the way of marital harmony for the privilege to preserve."[135] Though spousal privacy reforms purported to sync up with already changed societal understandings of the marital relationship, over time they helped drive new spousal norms from the margins to the mainstream.

Healthcare privacy.

---

[132] 358 U.S. 74 (1958).

[133] Allen, *supra* note 8, at 744.

[134] 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.").

[135] Trammel, 445 U.S. at 52.

Notions of privacy within a healthcare relationship date back to the Hippocratic Oath.[136] In the United States, state and federal law 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."[137] 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.[138] Early breach of confidence tort cases that regarded hospital-patient and doctor-patient relationships as confidential reinforced those norms.[139]

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 protected the existing norm of doctor-patient confidentiality[140] but it also confronted an unsettled norm: the extent and limits of patient autonomy. The U.S. Department of Health and Human Services, 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

---

[136] "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." Hippocrates, *Hippocratic Oath*, in Michael North, NATIONAL LIBRARY OF MEDICINE (2002).

[137] MacCarthy, *supra* note 36, at 434-35.

[138] *Id.*

[139] Richards & Solove, *supra* note 14, at n.198.

[140] 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.").

took a mixed approach on consent, allowing providers to use patient health information for a set of specifically defined purposes and requiring patient consent for any other uses.[141] 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 promote a new norm for healthcare providers—"the adoption and meaningful use of health information technology."[142] And, in 2016, Congress passed the 21st Century Cures Act to encourage greater information sharing between healthcare providers by prohibiting "information blocking."[143] 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.

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 e-mail 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.[144] 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 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

---

[141] Tschider, *supra* note 36, at 645-46.
[142] 45 CFR Part 160.
[143] Carleen M. Zubrzycki, *Privacy From Doctors*, 39 YALE L. & POL'Y REV. 526, 535 (2021).
[144] 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/.

postal privacy.[145] "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."[146] Through its "Secret Office," "the British post office created intelligence by opening, detaining, or copying correspondence, and sending 'interceptions' to the Secretaries of State."[147] British law forbad tampering with the mail, but this was mostly a formality.[148] 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.[149] 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.'"[150]

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.[151] And, after the founding, the 1792 Post Office Act simultaneously founded the United States Post Office and guaranteed postal privacy.[152] It forged a new relationship between the post and the public based in confidentiality, trust, and responsibility. Desai points out that this norm of postal privacy became such a powerful custom that it ascended to constitutional status.[153] In *Ex parte Jackson*, the Supreme Court decided mailed letters qualify as the sender's "papers" for Fourth Amendment purposes, such that the government couldn't open a sender's mail without a warrant.[154]

---

[145] 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).
[146] *Id.* at 560.
[147] *Id.*
[148] *Id.*
[149] *Id.* at 562.
[150] *Id.* at 564.
[151] *Id.* at 566.
[152] 1792 Post Office Act § 16.
[153] Desai, *supra* note 145, at 577.
[154] 96 U.S. 727, 732 (1878).

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 (e-mail) providers. The Electronic Communications Privacy Act generally bars email providers from intercepting the emails they transmit and requires the government to satisfy legal process before it can engage in interception.[155]

Privacy torts.

Legal scholars often characterize the privacy torts first espoused by Warren and Brandeis and developed further by Prosser as generalist privacy laws. Neil Richards and Dan Solove assert 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."[156] "Warren and Brandeis," they write, "sought a right against the world to protect hurt feelings."[157] Richards and Woodrow Hartzog argue Warren and Brandeis advocated for this sort of general right to privacy because "the aggressive press" which concerned Warren and Brandeis most "didn't have a relationship with [its] subjects."[158] 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."[159]

The privacy torts at face value seem to support the view they are not concerned with relationships. In practice, however, they too often reflect and direct social roles. As written in the Second Restatement, the privacy torts prohibit unreasonable intrusion upon another's seclusion, the appropriation of another's name or likeness, unreasonable publicity to another's private life, and publicity that unreasonably places another publicly in a false

---

[155] 18 U.S.C. § 2511.
[156] Solove & Richards, *supra* note 14, at 125.
[157] *Id.* at 132.
[158] Neil Richards & Woodrow Hartzog, *A Relational Turn for Data Protection?*, 4 EUR. DATA PROTECTION L. REV. 492, 493 (2020).
[159] Woodrow Hartzog & Neil Richards, *The Surprising Virtues of Data Loyalty*, 71 EMORY L.J. 985, 992-93 (2022).

light regardless of the invador and invadee's roles.[160] But three of the four torts hinge liability on whether the act would be "highly offensive to a reasonable person."[161] Robert Post explains that the "reasonable person" the torts consider "is a genuine instantiation of community norms."[162] And, as explained in Part 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 "rights against the world" but, when applied, courts often evaluate whether the invasion would 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).

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.[163] For instance, "liability 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."[164] 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 Tel. & Tel. Co.*, the Louisiana court found it was unreasonable for employees to enter a fellow employee's home without permission because they did so "in furtherance of their employer's interest and designed to prove plaintiff's unworthiness as a supervisory employee."[165] In *K-Mart v. Trotti*, the Texas court held "[w]here [an] employee purchases and uses his own lock on [employer-provided] lockers, with the employer's knowledge," one can reasonably conclude "the

---

[160] RESTATEMENT (2D) OF TORTS § 652A.
[161] *Id.*
[162] Post, *Social Foundations*, *supra* note 37, at 961.
[163] Pauline T. Kim, *Privacy Rights, Public Policy, and The Employment Relationship*, 57 OHIO ST. L.J. 671, 679 (1996).
[164] *Id.* at 675.
[165] 263 So. 2d 460, 466 (La. Ct. App. 1972).

employee manifested, and the employer recognized, an expectation that the locker and its contents would be free from intrusion and interference."[166] 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.[167]

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 Electronics Communications Privacy Act and privacy torts, construed online privacy through the framework of a "one-size-fits-all" neoclassical business-consumer relationship. 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

---

[166] 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.* at 637 ("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.").

[167] This is also the case when courts find no invasion occurred. For instance, in *McClain v. Boise Cascade Corp.*, the 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 passer[s]by on [the] road running in front of his property." 271 Or. 549, 556 (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.

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 agenda 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.[168] The first government effort to consider private-sector information privacy was the Privacy Protection Study Commission ("PPSC"), established by the Privacy Act of 1974.[169] The Commission'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.[170]

Though the PPSC did not explicitly state its analysis of privacy issues and recommendations were based on a business-consumer relationship, 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."[171] The PPSC reasoned two commercial speech Supreme Court opinions, *Lamont v. Postmaster General*[172] and *Virginia State Board of Pharmacy v. Virginia Citizens Consumer Council*[173], militated against statutory

---

[168] Christopher W. Savage, *Managing the Ambient Trust Commons: The Economics of Online Consumer Information Privacy*, 22 STAN. TECH. L. REV. 95, 100 (2019).
[169] 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, 587 (2018); Regan, *supra* note 22, at 83; James P. Nehf, *Recognizing the Societal Value in Information Privacy*, 78 WASH. L. REV. 1, 45 (2003).
[170] THE REPORT OF THE PRIVACY PROTECTION STUDY COMMISSION, PERSONAL PRIVACY IN AN INFORMATION SOCIETY (1977) [hereinafter "PPSC REPORT"].
[171] PPSC REPORT, at 21-22; Regan, *supra* note 22, at 84.
[172] 381 U.S. 301 (1965).
[173] 425 U.S. 748 (1976).

restrictions on information flows and for individual choice.[174] Ultimately, it concluded Congress should rely on organizations' voluntary compliance with a stripped-down notice-and-consent regime.[175]

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.[176]

Though the Report's recommendations were never enacted into law,[177] 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.[178] 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.[179] Writing around that time, Paul Schwartz observed "the Clinton Administration and legal commentators increasingly view the role of the Internet law of privacy as facilitating wealth-creating transmission of . . . personal data."[180] The White Paper overtly focused on "consumers'" interest

---

[174] PPSC REPORT, at 23-24 (citing *Lamont v. Postmaster General*, 381 U.S. 301 (1965); *Virginia State Board of Pharmacy v. Virginia Citizens Consumer Council*, 425 U.S. 748 (1976)).
[175] *Id.* at 26-27, 34, 36.
[176] *See id.* at 26-27.
[177] Regan, *supra* note 22, at 85.
[178] *See generally* U.S. Information Infrastructure Task Force Working Group on Privacy, PRIVACY AND THE NII: SAFEGUARDING TELECOMMUNICATIONS-RELATED PERSONAL INFORMATION 26-27 (1995).
[179] *Id.*
[180] Schwartz, *Privacy and Democracy*, *supra* note 36, at 1611.

in information privacy, defined as an individual's control over how information about her 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."[181] It concluded these interests would be served well by a notice-and-consent approach,[182] 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.[183]

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 website *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.[184] When the Internet was first opened up to commerce in the early 1990s,[185] commercial websites

---

[181] U.S. Information Infrastructure Task Force Working Group on Privacy, *supra* note 178.
[182] *Id.*
[183] *Id.* 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.").
[184] Steven A. Hetcher, *The Emergence of Website Privacy Norms*, 7 MICH. TELECOMM. & TECH. L. REV. 97, 131, 139 (2000); Steven Hetcher, *Changing The Social Meaning of Privacy in Cyberspace*, 15 HARV. J. L. & TECH. 149, 176 (2001).
[185] Boucher Amendment to National Science Foundation Act, 42 U.S.C. Ch. 16 (1992) (expanding "acceptable use" of Internet beyond "research and education in science and

proliferated and began to collect and use personal data—either by requesting it or by simply taking it.[186] With the development of web cookies, data collection skyrocketed, and Americans began to express distrust and an aversion to Internet use.[187] Congress urged the FTC to get involved.[188] Beginning in 1998, the FTC released a series of reports to try to motivate websites to "self-regulate" to protect "consumer privacy" with the ultimate aim of "increas[ing] consumer confidence and . . . their participation in the online marketplace."[189] It was not until the FTC threatened to advocate for online privacy legislation[190] 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."[191] 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)[192] and, occasionally, websites that collect and use individuals' personal information without providing any privacy disclosures at all (deemed "unfair.")[193]

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

---

engineering."); Hetcher, *Website Privacy Norms*, *supra* note 184, at 107; Stephen Segaller, NERDS 2.0.1: A BRIEF HISTORY OF THE INTERNET 295, 297 (1998).

[186] Hetcher, *Website Privacy Norms*, *supra* note 184, at 107-08; Steven A. Hetcher, *Norm Proselytizers Create a Privacy Entitlement in Cyberspace*, 16 BERKELEY TECH. L.J. 877, 888 (2001).

[187] Hetcher, *Website Privacy Norms*, *supra* note 184, at 108; Hetcher, *Norm Proselytizers*, *supra* note 186, at 888, 895.

[188] Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 598 (2014).

[189] Savage, *supra* note 168, at 126.

[190] Katie McInnis, *The Evolution of Consumer Attitudes Toward Online Tracking, 1995-2019*, 32, CONSUMER REPS. (May 2020); Hetcher, *Website Privacy Norms*, *supra* note 184, at 104-05, 139.

[191] *Privacy Online: Fair Information Practices in the Electronic Marketplace*, FED. TRADE COMM. (2000); Hetcher, *Website Privacy Norms*, *supra* note 184, at 129; Savage, *supra* note 168, at 105-06, 126-27.

[192] Solove & Hartzog, *supra* note 188, at 628.

[193] *Id.* at 638-43.

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.[194] 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 framing.[195] 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.)[196] 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."[197]

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 business and consumers support minimal legal intervention and undermine normativity because they are fundamentally unsocialized.[198] Economics is not concerned what businesses or consumers *should* do, in a normative sense. Instead, it makes predictions about what they *will* do, from the baseline

---

[194] Savage, *supra* note 168, at 106.

[195] Hetcher, *Social Meaning*, *supra* note 184, at 162; Solove & Hartzog, *supra* note 188, at 587, 596-97; 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 W. Haynes, *Online Privacy Policies: Contracting Away Control Over Personal Information?*, 111 PENN. ST. L. REV. 587, 597-99, 607 (2007); Electronic Communications Privacy Act of 1986, 18 U.S.C. § 2510, *et seq.* (1986).

[196] *See, e.g.*, Motion for Summary Judgment, Calhoun et al. v. Google LLC, No. 5:20-cv-05146 (N.D. Cal. Nov. 30, 2021); *Rodriguez v. Google LLC*, No. 20-cv-04688, 2021 WL 2026726 (May 21, 2021); Order Denying Motion to Dismiss, Brown et al. v. Google LLC, No. 5:20-cv-03664 (N.D. Cal. Mar. 12, 2021); *In re Facebook, Inc. Internet Tracking Litig.*, 956 F.3d 589 (2020); *Backhaut v. Apple, Inc.*, 74 F. Supp. 3d 1033 (2014).

[197] *See, e.g.,* Calhoun v. Google LLC, 526 F. Supp. 3d 605, 626 (2021); Brown v. Google LLC, 525 F. Supp. 3d 1049, 1071 (2021); Dunbar v. Google Inc., No. 5:10-cv-194, 2011 WL 12907501, at *1 (E.D. Tex. May 23, 2011).

[198] 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.

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.[199] 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 failures or externalities. And, when government intervenes, it is limited to correcting those particular issues.[200] 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.[201] As Woodrow Hartzog and Neil Richards explain, "[t]he current U.S. approach to privacy flattens the power dynamics within relationships with a giant *caveat emptor* sign."[202] Privacy norms rely on societal notions of what privacy expectations are "reasonable" for a relationship.[203] But within a neoclassical business-consumer relationship, social norms are inapposite; expectations are bound to the business's disclosures about its practices. Ari Ezra Waldman expounds that "privacy law's

---

[199] Lucy Black Creighton, PRETENDERS TO THE THRONE: THE CONSUMER MOVEMENT IN THE UNITED STATES 2 (1976).
[200] Joshua D. Wright, *The Antitrust/Consumer Protection Paradox: Two Policies At War With Each Other*, 121 YALE L.J. 2216, 2218 (2012).
[201] *See* Mazzurco, *supra* note 91, at 807-15.
[202] Hartzog & Richards, *Surprising Virtues*, *supra* note 159, at 993.
[203] Post, *Social Foundations*, *supra* note 37, at 959-61.

performances are constructions of industry."[204] At a structural level, the business-consumer relationship places data collectors in a conceptually and legally legitimated position to dictate 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. 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 behavior. 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 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

---

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

Act of 2020, reflect the same tendency.[205] 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.[206] 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.[207] 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 bills in Congress.[208]

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 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

---

[205] CCPA § 1798.100, *et seq.*; California Privacy Rights Act of 2020, AB-1490, Reg. Sess. (2021) [hereinafter "CPRA"].
[206] CCPA § 1798.100, *et seq.*; CPRA.
[207] CCPA § 1798.110; CPRA §§ 5-11.
[208] Karl Evers-Hillstron & Rebecca Klar, *Corporate lobbying could imperil sweeping data privacy bill*, THE HILL (Aug. 3, 2022), https://thehill.com/lobbying/3585322-corporate-lobbying-could-imperil-sweeping-data-privacy-bill/.

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*

Neil Richards and Woodrow Hartzog argue in favor of a "relational turn" for privacy law.[209] 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.[210] As Parts II.B and 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: a neoclassical business-consumer relationship. Ari Ezra Waldman stresses it is time for privacy discourse to focus on "what should be" to "change baseline assumptions about what privacy is for."[211] In Dan Solove's words, "By redefining relationships, the law would make a significant change to the architecture of the information economy."[212] A core component of that pivot will be a change to the social roles online privacy law scripts for data collectors and Internet users.

The neoclassical business-consumer relationship is an unfit frame for privacy law in an information economy for a number of reasons.

---

[209] Richards & Hartzog, *Relational Turn*, *supra* note 158, at 493.
[210] *Id.*
[211] Waldman, *Privacy, Practice*, *supra* note 204, at 1228.
[212] Daniel J. Solove, The Digital Person: Technology and Privacy in the Information Age 104 (2008).

First, the constitutionality of privacy law that responds to a business-consumer relationship is highly precarious following *NetChoice v. Bonta*. In *Bonta*, the Northern District of California court characterized businesses' data collection as speech the First Amendment protects.[213] Online privacy law likely *must* abandon casting data collectors as businesses to reduce the specter of First Amendment deregulation.[214]

Second, 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,"[215] 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 role-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 positions all of these entities to decide their information practices (however surveillant) unilaterally.

Third, 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 didn't have to be this way. Writing contemporaneously with commercial Internet's emergence, Paul Schwartz identified "the true promise of the Internet [] not [] as a

---

[213] No. 22-cv-08861 (N.D. Cal. Sept. 18, 2023).

[214] See Amanda Shanor, The New Locher, 2016 Wisc. L. Rev. 133 (2016).

[215] *7 Advertising Verticals to Target in 2022*, BROADSTREET (Apr. 12, 2022), https://broadstreetads.com/7-advertising-verticals-to-target-in-2022/.

place for electronic commerce, but as a forum for deliberative democracy."[216] 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 be adequate for all situations; our task is to develop nuanced concepts for use in charting and fixing the bounds of different privacy domains.[217]

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.[218]

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 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

---

[216] Schwartz, *Privacy and Democracy*, *supra* note 36, at 1614.

[217] *Id.*

[218] But see Solove, Virtues of Knowing Less, supra note 30, at 1050 (arguing law shouldn't 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 Parts I.A&B (explaining complex identity depends on the ability to play multiple social roles, which surveillance threatens).

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 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.

i. Data Protection

Data protection law has become the predominant mode of U.S. privacy reform at the state level. Between 2020 and 2023, twelve states passed comprehensive "data privacy" or "data protection" laws.[219] 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.[220]

The CPRA's prefatory language and operative provisions show a shift from a lingering "business-consumer" role relationship

---

[219] Andrew Folks, US State Privacy Legislation Tracker, IAPP (Sept. 15, 2023), https://iapp.org/resources/article/us-state-privacy-legislation-tracker/.
[220] CPRA § 1798.100.

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."[221] It characterizes the data protection relationship as a "contractual arrangement" in which goods or services are exchanged for personal information.[222] The problem is "consumers often have no good way to value the transaction."[223] 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.[224] Businesses' responsibilities correspond to these nominatively "consumer" rights. Additionally, businesses "may offer financial incentives, including payments to consumers as compensation" for the collection, sale, sharing, or retention of their personal information.[225] These rights and responsibilities aim to "place the consumer in a position to knowingly and freely negotiate with a business over the business's use of the consumer's personal information."[226]

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.[227] The prevailing theory of a property relation, reflected in the Restatement of Property, is it denotes "legal relations between persons with respect to a thing."[228]

---

[221] Id. at S. 2(A).
[222] Id. at S. 2(E).
[223] Id.
[224] Id. at 4-10.
[225] Id. at 11(b).
[226] Id. (3)(c)(3).
[227] 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 227, at 772; David W. Opderbeck, Social Network Analysis of Trade Secrets and Patents as Social Relations, 41 AIPLA Q. J. 355, 376 (2013)
[228] David Frisch, Remedies as Property: A Different Perspective on Specific Performance Clauses, 35 Wm. & Mary L. Rev. 1691, 1704 (1994); Joseph William Singer, The

Following this account, scholars typically characterize property owners as interested in "control," expounded in various ways.[229] For Blackstone, "control" manifested in "sole and despotic dominion."[230] Whereas for Hohfeld, property relations were "a bundle of entitlements regulating relations among persons concerning a valued resource."[231] A.M. Honoré classified these entitlements as rights to possess (i.e., exert control), use, manage, receive income from, alienate, and security in one's property, among other things.[232]

It is striking how well state laws' data protection relationship shares those characteristics. It situates data protection within a relationship of 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,"[233] 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."[234] And, in practice, it entrenches "data controllers" prerogative to

---

Reliance Interest in Property, 40 Stan. L. Rev. 611, 635-36 (1988); Morris, supra note 227, at 772; Di Robilant, supra note 227, at 880.

[229] James Grimmelmann & Christina Mulligan, Data Property, 72 Am. Univ. L. Rev. 829, 847 (2023); Singer, supra note 228, at 636; Frisch, supra note 228, at 1707; Nestor M. Davidson, Property and Relative Status, 107 Mich. L. Rev. 757, 769 (2009).

[230] Singer, supra note 228, at 636. By contrast, Joseph Singer emphasizes the many limitations property law (such as nuisance laws) place on property owners' use and enjoyment of their property. Id. at 642-45.

[231] Di Robilant, supra note [x], at 871; Singer, supra note 228, at 663.

[232] Frisch, supra note 228, at 1707-08. "Security" is explained as a right against unconsented expropriation by a nonowner without first obtaining the owner's permission. Id.

[233] Mistale Taylor, The EU's human rights obligations in relation to its data protection laws with extraterritorial effect, 5 Int'l Data Privacy L. 246, 247-49 (2015).

[234] European data protection laws arguably derive from the U.S. HEW Fair Information Practices, vis a vis the 1980 Organization for Economic Cooperation and Development guidelines. Solove, Digital Person, supra note 212, at 105; Steven S. McCarty-Snead & Anne Titus Hilby, Research Guide to European Data Protection Law, 42 Int'l J. Legal Info. 348, 360 (2014).

unilaterally decide their collection and use of "data subjects" personal information,[235] 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."[236] And the U.S. Constitution protects rights of property owners under the Fifth Amendment.

Data protection laws cast Internet users as "data property owners" interested in controlling information about them.[237] On the other end of the "contractual arrangement" are data businesses[238] which follow an instrumental logic, gathering, processing, and using personal information (as a "valuable resource") to pursue organizational goals.[239]

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 and applications or others that embed the platforms' web trackers.[240] They collect details such as the links individuals click,

---

[235] McCarty-Snead & Hilby, supra note 234, 362.

[236] Jeremy Waldron, The Right to Private Property 353.

[237] Grimmelmann & Mulligan, supra note 229, at 859; Julie E. Cohen, *How (Not) to Write a Privacy Law*, KNIGHT FIRST AM. INST. (Mar. 23 2021), https://knightcolumbia.org/content/how-not-to-write-a-privacy-law; Robert C. Post, *Privacy, Speech, and the Digital Imagination*, in FREE SPEECH IN THE DIGITAL AGE 106-19 (2019) ("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."); 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); Daniel J. Solove, *The Myth of the Privacy Paradox*, 89 GEO. WASH. L. REV. 1, 5-6 (2021).

[238] *See* CCPA § 1798.100(a) (directing obligations to "a business that controls the collection of a consumer's personal information"); § 1798.140(v) (defining personal information as information that "relates to" a particular consumer or household).

[239] Notably, ADPPA covers entities beyond for-profit commercial enterprises, such as not for profit organizations that would not have otherwise been outside the Federal Trade Commission's jurisdiction. H.R. 8152 § 2(9). See also Post, *Digital Imagination*, *supra* note 237, at 107-08; Post, *Google Spain*, *supra* note 237, at 991.

[240] *See Data Policy*, FACEBOOK, https://www.facebook.com/policy.php; *Privacy Policy*, GOOGLE, https://policies.google.com/privacy?hl=en-US; Dina Srinivasan, The Antitrust Case Against Facebook, 17 BERKELEY BUS. L.J. 39, 70-76 (2018); Justin Brookman, *Understanding the Scope of Data Collection by Major Technology Platforms*, 16,

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.[241] The platforms aggregate this information about individuals to draw insights about their likely attributes, behaviors, and interests.[242] 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.[243] 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.[244]

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.[245] 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' access ot 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 permissions if they disagree with data businesses' use.) Data businesses personal information practices—ranging from sharing personal information

---

CONSUMER REPS. (May 2020); Complaint at ¶ 36, Rodriguez et al. v. Google LLC, 3:20-cv-4688 (N.D. Cal. July 14, 2020).

[241] *See* Brookman, *supra* note 240.

[242] Cohen, *Privacy Law*, *supra* note 237; Sandra Wachter & Brent Mittelstadt, *A Right to Reasonable Inferences, Re-Thinking Data Protection*, 2019 COLUM. BUS. L. REV. 494, 506-10 (2019); Louise Matsakis, *Facebook's Targeted Ads Are More Complex Than It Lets On*, WIRED (Apr. 25, 2018), https://www.wired.com/story/facebooks-targeted-ads-are-more-complex-than-it-lets-on/.

[243] Matsakis, *supra* note 242.

[244] Zuboff, *supra* note 19.

[245] Grimmelmann & Mulligan, supra note 229, at 860.

for surreptitious political influence,[246] to selling identifying information together with comprehensive, precise geolocation history[247]—do not implicate societal notions of appropriate uses of personal information.

An Internet user could reasonably assert she is injured when, for instance, she discovers Google retained her search history though she demanded that Google delete it.[248] But she could not reasonably assert Google acted inappropriately by sharing her search history with credit rating organizations before she 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."[249] It 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's 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.[250]

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

---

[246] Nicholas Confessore, Cambridge Analytica and Facebook: The Scandal and the Fallout So Far, N.Y. Times (Apr. 4, 2018).

[247] Kochava v. Federal Trade Commission, No. 2:22-cv-00349, 2023 WL 3250496 (May 3, 2023).

[248] *C.f.* Order Denying Motion to Dismiss, Brown et al. v. Google LLC, No. 5:20-cv-03664 (N.D. Cal. Mar. 12, 2021) (Plaintiffs argue Google Chrome browser's collection of personal information—including web browsing history—while users are in "Incognito" mode subverts their control.).

[249] Adam D.I. Kramer et al., *Experimental evidence of massive-scale emotional contagion through social networks*, Proceedings of the Nat. Acad. of Sci. of the U.S.A. (June 2, 2014), https://www.pnas.org/content/111/24/8788.

[250] Richards & Hartzog, *Relational Turn*, *supra* note 158, at 495.

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 assymetry.[251] It is also a one-size-fits-all approach, such that it would work against the formation and the ability to distinguish between multiple role-relationships.[252] 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.[253] 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 2009.[254] 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,

---

[251] 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.").

[252] See Schwartz, *Privacy and Democracy*, *supra* note 36, at 1660.

[253] *See generally* CPRA, GDPR.

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

analytics, and marketing.[255] Law might also tinker with Internet users' rights to alienate their personal information. Paul Schwartz, for example, has long advocated for legal "inalienabilities" to accompany a propertized personal information regime: "namely, a restriction on the use of personal data combined with a limitation on their [further] transferability."[256]

Law that responds to this relationship is only justified in limited circumstances. As Schwartz writes, "[R]estrictions must respond to concerns about private market failures."[257] 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 involve significant transaction costs, or other similar impediments to perfect competition in personal information.[258]

ii. Information Fiduciaries

In 2004, Dan Solove made a radical proposal: that law should regulate the companies that collect and use individuals' personal information as fiduciaries.[259] Jack Balkin, Neil Richards, and Woodrow Hartzog further developed that proposal,[260] adopting

---

[255] Jon Healey, *What are those annoying website popups about cookies? And what should you do about them?*, LA TIMES (Sept. 1, 2021), https://www.latimes.com/business/technology/story/2021-09-01/what-are-website-cookies-how-do-they-impact-internet-data. 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 GDPR require as much for websites targeting EU residents, and member countries have enacted more specific requirements. See GDPR rec. 30; Directive 2009/136/EC ("ePrivacy Directive"); Cookies et autres traceurs : la CNIL publie des lignes directrices modificatives et sa recommendation, CNIL (Oct. 1, 2020), https://www.cnil.fr/fr/cookies-et-autres-traceurs-la-cnil-publie-des-lignes-directrices-modificatives-et-sa-recommandation.

[256] Schwartz, Property, Privacy, supra note 22, at 2095.

[257] Id. at 2096; see also Singer, supra note 228, at 634.

[258] See generally, market failure, Encylcopedia Brittanica (Oct. 1, 2019), https://www.britannica.com/money/topic/market-failure.

[259] Solove, Digital Person, supra note 212, at 103.

[260] Jack M. Balkin, *Free Speech Is a Triangle*, 118 COLUM. L. REV. 2011, 2047-54 (2019); Jack M. Balkin, *Information Fiduciaries and the First Amendment*, 49 U.C. DAVIS L. REV. 1183, 1205-09, 1225-30 (2016); Woodrow Hartzog & Neil M. Richards, *Privacy's Constitutional Moment*, 61 B.C. L. REV. 1687, 1750 (2020); Neil Richards & Woodrow Hartzog, *Taking Trust Seriously in Privacy Law*, 19 STAN. TECH. L. REV. 431, 457-58

the view that privacy is a quality of "relationships of trust" in which information is divulged, not a quality of information itself.[261] 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.[262]

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.[263] Traditional fiduciary relationships in law include those between lawyer and client, doctor and patient, and real estate buyer's agent and buyer.[264] In each of these relationships, the professionals providing services have knowledge and skills the beneficiaries don't, they must collect information from beneficiaries to provide them with services, and beneficiaries are ill-equipped to monitor the professionals' actions and assess risk.[265] Because of the asymmetries of power and knowledge within the relationship, beneficiaries have no alternative but to trust professionals to act in beneficiaries' best interest.[266] In these sorts of relationships, law typically imposes two obligations on professionals: a duty of care and a duty of loyalty.[267] Fiduciaries must take care to act competently and diligently, so not to harm their beneficiaries' interests, they must keep their beneficiaries' interests in mind, and they must act in their beneficiaries' interest.[268]

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

(2016); Neil Richards & Woodrow Hartzog, *A Duty of Loyalty for Privacy Law* (2020) (unpublished manuscript) (on file with authors).

[261] Solove, Digital Person, supra note 212, at 102; Balkin, *Information Fiduciaries*, *supra* note 260, at 1187.

[262] *See* Notes, FED. R. EVID. 501.

[263] Balkin, *Information Fiduciaries*, *supra* note 260, at 1121-22; Richards & Hartzog, *Loyalty*, *supra* note 260, at 19, 22.

[264] Balkin, *Information Fiduciaries*, *supra* note 260, at 1187, 1121; Ari Ezra Waldman, *Cognitive Biases, Dark Patterns, and the "Privacy Paradox,"* 31 CURRENT OP. IN PSYCH. 105, 107 (2020).

[265] Balkin, *Information Fiduciaries*, *supra* note 260, at 1121-22, 1124, 1216-17.

[266] *Id.* at 1216-17.

[267] *Id.* at 1207-08; Balkin, *Triangle*, *supra* note 260, at 2051-52; Hartzog & Richards, *supra* note 260, at 1749-50.

[268] Balkin, *Information Fiduciaries*, *supra* note 260, at 1207-08.

> 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 valuable data that might be used to our disadvantage -- and they know that we know it too.[269]

He asserts the law should hold data collectors to reasonable ethical standards of trust and confidentiality as to how they handle individuals' information.[270] 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.[271] 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 children . . . .[272]

Two bills in Congress also incorporate an information fiduciaries approach.[273]

---

[269] *Id.* at 1222.
[270] *Id.* at 1224.
[271] Hartzog & Richards, *supra* note 260, at 1749-50; Richards & Hartzog, *Loyalty*, *supra* note 260, at 41-52.
[272] Cal. Civ. Code § 1798.99.29.
[273] *See* Data Care Act of 2021, § 919, 117th Cong. (2021); H.R. 8152 §§ 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. REFL. 5, 370 (2022).

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 doesn't.[274] One can imagine the difficulty an Internet user would encounter if she tried to piece together her 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.[275] Data collectors as information fiduciaries also must collect certain personal to provide these services. A social network without any information 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.[276] Their information use becomes inappropriate, however, when it contravenes their beneficiaries' best interest.[277] Richards and Hartzog imagine this might manifest in "strict and robust rules limiting what data can be collected, how long it can be kept, and what it can be used for,"[278] potentially ending behaviorally targeted advertising altogether.[279]

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.[280] 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.[281] Internet users as beneficiaries are interested in two

---

[274] Balkin, *Information Fiduciaries*, *supra* note 260, at 1224.
[275] *Id.* at 1222.
[276] *Id.* at 1227; Richards & Hartzog, *Loyalty*, *supra* note 260, at 10-11.
[277] Richards & Hartzog, *Loyalty*, *supra* note 260, at 65.
[278] *Id.* at 33, 71.
[279] *Id.* at 55-57; Balkin, *Information Fiduciaries*, *supra* note 260, at 1222.
[280] Richards & Hartzog, *Loyalty*, *supra* note 260, at 57; Balkin, *Information Fiduciaries*, *supra* note 260, at 1222.
[281] Richards & Hartzog, *Loyalty*, *supra* note 260, at 57; Balkin, *Information Fiduciaries*, *supra* note 260, at 1222.

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.[282]

Information fiduciaries proponents 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 expert 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 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. These are the sorts of expectations Richards and Hartzog hope fiduciary obligations will elicit.[283] Down the line, users may expect data collectors to act as trustworthy experts beyond online privacy. For instance, they might

---

[282] Richards & Hartzog, *Loyalty*, *supra* note 260, at 57; Balkin, *Information Fiduciaries*, *supra* note 260, at 1222.

[283] Richards & Hartzog, *Loyalty*, *supra* note 260, at 16, 29-30.

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 decisionmakers when it comes to privacy and other matters.[284]

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."[285] 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, dependence, and unilateral discretion,[286] 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.[287] The relationship could also support lawmaking that imposes or enforces both broader and more granular standards of data collectors'

---

[284] Lina Khan & David Pozen, *A Skeptical View of Information Fiduciaries*, 133 HARV. L. REV. 497, 535 (2019).
[285] Hartzog & Richards, *Surprising Virtues*, *supra* note 159, at 994.
[286] *Id.* at 990.
[287] Balkin, *Information Fiduciaries*, *supra* note 260, at 1187; Richards & Hartzog, *Loyalty*, *supra* note 260, at 16, 29-30.

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.[288] 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.[289]

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.[290] 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 whether it improves the quality of data collectors' services to users or whether it 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.

C. *A Proposal for Privacy Governance*

There is an alternative for privacy law. It can respond to a privacy governance[291] relationship that casts data collectors as

---

[288] *See, e.g.*, N.Y. R. PROF. CONDUCT, 22 NYCRR 1200.0 *et seq.*

[289] *Id.*

[290] *See, e.g.,* Priyanjana Bengani, *Controlling the Conversation: The Ethics of Social Platforms and Content Moderation*, Platforms and Publishers: Policy Exchange Forum III, UNIV. S. CAL. ANNENBERG (Feb. 23, 2018); Angel Diaz & Laura Hecht-Felella, *Double Standards in Social Media Content Moderation*, BRENNEN CTR. FOR JUSTICE (Aug. 4, 2021), https://www.brennancenter.org/our-work/research-reports/double-standards-social-media-content-moderation; Social Media: Misinformation and Content Moderation Issues for Congress, CONG. RSCH. SERV. (Jan 27, 2021), https://sgp.fas.org/crs/misc/R46662.pdf.

[291] This proposal adopts the term "privacy governance" to draw a subtle but substantive distinction from Salome Viljoen's use of the term "data governance law." Professor Viljoen defines data governance law as "the legal regime that governs how data about people is collected, processed, and used." Salome Viljoen, *A Relational Theory of Data Governance*, 131 YALE L.J. 573, 577 (2021). Her construction places focus on how *law* governs data.

"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 agenda. 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.[292] 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.[293] 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.[294] Scholars such as Sidney and Beatrice Webb 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).[295] The state of online privacy shares or amplifies many of these qualities. Large data collectors are legally and technically empowered to decide their information practices unilaterally; they have tremendous insight into Internet users'

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.

[292] Mazzurco, *supra* note 91, at 796.

[293] *Id.* at 822.

[294] *Id.*

[295] *Id.*

behaviors and preferences; and they do not rely on any one user's personal information.[296]

Progressive political and legal scholars suggested democracy was imperative *within* the private governance of labor.[297] Worker powerlessness within the workplace not only placed workers at the mercy of employers to be able to sustain their lives. It also risked "transform[ing] society into a nation of robots, unfit to perform the duties which democratic government demanded of its citizens."[298] 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.[299] Because the labor relationship was, in important part, antagonistic, the pathway to democratic participation required workers to have "countervailing power" through collective action.[300]

Privacy law oriented around a privacy governance relationship seeks to materialize the Internet's democratic potential Paul Schwartz identified early on.[301] 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.[302] He prescribed "privacy rules for cyberspace" that "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."[303] To that end, Schwartz proposed Fair

---

[296] *Id.* at 824.
[297] *Id.* at 827.
[298] *Mr. Justice Brandeis, Competition and Smallness: A Dilemma Re-Examined*, 66 YALE L.J. 69, 73 (1956).
[299] *Id.*
[300] Mazzurco, *supra* note 91, at 827.
[301] Schwartz, *Privacy and Democracy*, *supra* note 36, at 1648-49. Of course, not all Internet users live within democratic nation-states and so 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.
[302] *Id.* 1653.
[303] *Id.* Schwartz's focus was on data protection law law that respects and encourages an individual's capacity for decisionmaking, to give effect to their autonomy and participate in the processes of democratic government, His "privacy as participation" model didn't

Information Practices (FIPs) for online privacy.[304] 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.[305]

This form of privacy law also finds support in Salome Viljoen's more recent work on relational data governance.[306] 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.[307] Viljoen approves of "public management and control over existing proprietary data flows," whether through mandated public access or public trust.[308]

This Article operationalizes the project of democratizing online privacy. It articulates a "privacy governance" legislative agenda 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.[309]

Privacy governance law requires a particular normative orientation: privacy law must target a problematic power structure that positions data collectors to hegemonically "govern" Internet users' privacy in data collectors' self-interest. This normative

---

relate to democratic participation *within* Internet users' relationship with data collectors. Schwartz, Privacy and Participation, supra note 41, at 555, 557-58.

[304] *Id.* 1670-72.

[305] Solove, Digital Person, supra note 212, at 104.

[306] See generally Viljoen, *supra* note 291.

[307] *Id* at 579.

[308] *Id.* at 645.

[309] 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 Posner, Glen Weyl, and Jaren Lanier 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 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.

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,[310] this proposal envisions that Internet users as citizens should be informed participants in governance decisions.[311] 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.[312] 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)[313] with some necessary adaptations to match an information economy's context.

---

[310] See Sarah Wallace Goodman, CITIZENSHIP IN HARD TIMES Chs. 1 & 2 (2022).
[311] *Id.* At 35.
[312] There are certain limits to state-level privacy governance law. For instance, it would necessarily be limited to organizing efforts of Internet users resident 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 might serve as an instructive test case for future Federal reform.
[313] 29 U.S.C. § 151.

Privacy governance law should, as a first measure, provide the subjects of commercial data collection[314] the fundamental right to seek better information practices and designation of representation without fear of retaliation or liability under antitrust laws.[315] It should provide Internet users the right to self-organization into collective bargaining associations (CBAs), to bargain collectively through representatives they choose and engage in other related activities, and the right to abstain from self-organization and collective bargaining.[316] It should also define a preliminary set of unfair information practices, that a Data Protection Agency could further elaborate.[317] 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.[318] It should also provide a mechanism for enforcement of legally binding collective bargaining agreements.[319]

There is, of course, a volume of details lawmakers would have to work out to draft this sort of legislation.[320] 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 – if they have any chance to

---

[314] The proposal envisions that rights would be reserved to U.S., human subjects of data collection and commercial exploitation.

[315] See *National Labor Relations Act Guidance*, NLRB NATIONAL LABOR RELATIONS BOARD (last visited Mar. 28, 2023), https://www.nlrb.gov/guidance/key-reference-materials/national-labor-relations-act.

[316] See 29 U.S.C. § 157.

[317] Id. §§ 153, 158 (a).

[318] See *id.* § 158(d).

[319] See *id.* § 160.

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

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 agenda contrasts starkly with the European Union's recent Digital Markets Act.[321] Though the Act seeks to rectify the power imbalance between "gatekeepers" and "end users,"[322] it relies heavily on data protection's property role-relationship. It treats personal data as a "thing of value"[323] that is alienable for specified purposes with the end user's consent.[324] 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.[325]

This Article's privacy governance law implores 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

---

[321] Regulation (EU) 2022/1925 (14 September 2022) [hereinafter "Digital Markets Act" or "DMA"].
[322] *Id.* at (3).
[323] *Id.* at (36).
[324] The DMA 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.* at Ch. III, Art. 5(2) (listing prohibitions on gatekeepers' practices "unless the end user . . . has given consent"); *id.* at Ch. III, Art. 6(1) (requiring gatekeepers to provide business users with end users' personal data connected to end users' interaction with business users).
[325] *Id.* at Ch. III, Art. 6(9).

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 an information fiduciary relationship demands. Rather, citizens and private governors are expected to have conflicting interests that collective bargaining mediates. 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/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[326], and law's expressive support might provide further motivation.[327] 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

[326] See *Data Dignity*, RADICALXCHANGE (last visited Mar. 28, 2023), https://www.radicalxchange.org/.

[327] Some may perceive the woeful state of tech worker unionization as an indication 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.

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 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 re-socializes 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 on them 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-envisions 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're 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 it 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.