

Information Privacy and Corporate Power: Towards a Re-Imagination of Information Privacy Law

Marcy E. Peek*

This Article contends that there is a fundamental dynamic involved in the information privacy landscape that has heretofore remained largely unexamined and has resulted in intractable problems in information privacy law and jurisprudence—namely, corporate power. More specifically, this Article argues that information privacy is governed not just by governmental law but also by corporations via private governance. Part I of this Article briefly canvasses the current state of information privacy law and jurisprudence. Part II argues that domestic and international legal regimes are governed not only by governments but also by private actors, including corporations. Part III presents three examples of corporations engaging in private governance of information privacy. Part IV addresses some of the implications of the private governance model as applied to information privacy law.

* Visiting Assistant Professor of Law, St. Louis University School of Law; Assistant Professor of Law, Whittier Law School; J.D., Harvard Law School 1997; Harvard Law Review (1995–97); B.A, Yale University 1993. I would like to thank James Alton Alsup III, Judy Daar, Hari Osofsky, Radha Pathak, and Laura Rosenbury for their invaluable comments on this Article and/or support and advice during the writing process. I would also like to thank my research assistants, Amanda Klingler and Ronald Clifford. Finally, I would like to thank the participants at the 2005 Cardozo/Stanford/Berkeley/DePaul IP Scholars Conference, who provided a great deal of insightful feedback.

“[T]hat which goes unrecognized is difficult to regulate.”¹

INTRODUCTION

Information privacy laws and jurisprudence are at an impasse. For the most part, scholars are engaged in well-meaning but intractable debates.² The majority of the information privacy scholarship focuses on one of the following projects: defining or describing privacy;³ finding adequate metaphors for privacy;⁴ locating, defending, or critiquing privacy law (beginning with Warren and Brandeis’s seminal article published in 1890, the *Right to Privacy*);⁵ locating particular privacy wrongs;⁶ or balancing privacy interests with other interests such as national security.⁷ In addition, in response to the many problems of information privacy—problems such as computer profiling,⁸ personal data collection and sharing by companies,⁹ iden-

¹ A. Claire Cutler, *Private International Regimes and Interfirm Cooperation*, in *THE EMERGENCE OF PRIVATE AUTHORITY IN GLOBAL GOVERNANCE* 23, 24 (Rodney Bruce Hall & Thomas J. Biersteker eds., 2002).

²

Given the political history of the privacy debate in this country, no significant shift in U.S. policy seems likely to occur until some crisis or highly publicized event forces us to look at the issue from a new perspective. Indeed, in the current political climate, efforts to press a fundamental shift in policy appear to be losing momentum. . . . Without a sense of urgency, special interest politics and a general anti-regulatory sentiment will likely dominate political discourse in the United States on this issue for the foreseeable future.

James P. Nehf, *Recognizing the Societal Value in Information Privacy*, 78 WASH. L. REV. 1, 90–91 (2003).

³ See generally, ALAN F. WESTIN, *PRIVACY AND FREEDOM* (1967); Ruth Gavison, *Privacy and the Limits of Law*, 89 YALE L.J. 421 (1980); Tal Z. Zarsky, *Thinking Outside the Box: Considering Transparency, Anonymity, and Pseudonymity as Overall Solutions to the Problems of Information Privacy in the Internet Society*, 58 U. MIAMI L. REV. 991 (2004).

⁴ See, e.g., Daniel J. Solove, *Privacy and Power: Computer Databases and Metaphors for Information Privacy*, 53 STAN. L. REV. 1393 (2001).

⁵ See Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890).

⁶ See generally, Joel Reidenberg, *Privacy Wrongs in Search of Remedies*, 54 HASTINGS L.J. 877 (2003).

⁷ See generally, Sadiq Reza, *Privacy and the Post-September 11 Immigration Detainees: The Wrong Way to a Right (and Other Wrongs)*, 34 CONN. L. REV. 1169 (2002).

⁸ See generally, Comment, Janet Dean Gertz, *The Purloined Personality: Consumer Profiling in Financial Services*, 39 SAN DIEGO L. REV. 943 (2002).

⁹ See, e.g., DANIEL SOLOVE, MARC ROTENBERG & PAUL M. SCHWARTZ, *INFORMATION PRIVACY LAW* 623–35 (2006).

tity theft,¹⁰ and problems of non-secure computer databases containing personal information¹¹—privacy scholars have put forth a variety of possible solutions. Some of these solutions are based in traditional bodies of law such as tort law,¹² contract law,¹³ and property law.¹⁴ Other solutions call for statutory reform in matters pertaining to data collection, sharing, and use.¹⁵ But the answers to the problems in information privacy have remained elusive.

This Article contends that that there is a fundamental dynamic involved in the information privacy landscape that has heretofore remained largely unexamined and has resulted in intractable problems in information privacy—namely, corporate power. More specifically, this Article argues that information privacy is governed not just by governmental law but also by corporations via private governance. Unless corporate power vis-à-vis the individual and the governance of information privacy law by corporations is addressed, the law will continue to strengthen corporate power and erode privacy in the guise of privacy-enhancing efforts. Scholars must delve beneath the façade of privacy laws and Federal Trade Commission (“FTC”) enforcement actions in order to expose the power dynamics that pervade information privacy law and policy.

Hans Morgenthau famously argued in a seminal work examining power¹⁶ that “the element of power as the immediate goal of the policy pursued is explained and justified in ethical, legal, or biological terms. That is to say: the true nature of the policy is concealed by ideological justifications and rationalizations.”¹⁷ In regard to privacy, I similarly argue that the stated reasons and purposes of information

¹⁰ See generally, Lynn M. LoPucki, *Human Identification Theory and the Identity Theft Problem*, 80 TEX. L. REV. 89 (2001).

¹¹ See generally, Nina Bernstein, *Electronic Eyes: What the Computer Knows*, N.Y. Times, A1, Sept. 15, 1997, 1997 WLNR 4871741.

¹² See, e.g., Jessica Litman, *Information Privacy/Information Property*, 52 STAN. L. REV. 1283 (2000) (arguing against treating personal information as property and suggesting a “breach of trust” cause of action based in tort law).

¹³ See, e.g., Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 STAN. L. REV. 1193 (1998) (arguing for contractual default rules in favor of individuals).

¹⁴ See, e.g., LAWRENCE LESSIG, *CODE AND OTHER LAWS OF CYBERSPACE* (1999); Richard S. Murphy, *Property Rights in Personal Information: An Economic Defense of Privacy*, 84 GEO. L.J. 2381 (1996). But see Pamela Samuelson, *Privacy as Intellectual Property?*, 52 STAN. L. REV. 1125 (2000) (arguing that privacy cannot be properly protected by property rights).

¹⁵ DANIEL SOLOVE, *THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE* 101 (2004).

¹⁶ HANS J. MORGENTHAU, *POLITICS AMONG NATIONS: THE STRUGGLE FOR POWER AND PEACE* (5th ed. 1973).

¹⁷ *Id.* at 88.

privacy law conceal the true nature and driving forces of information privacy law.¹⁸ Moreover, the privacy debate and scholarship is at an impasse because the underlying force that is at the center of privacy law is also the white elephant in information privacy law: the dominance of corporate power and corporate governance¹⁹ of information privacy law.

A few definitional understandings are in order.²⁰ When I speak of privacy and corporate power, I speak not of surveillance,²¹ but rather of domination over the individual.²² Furthermore, when I speak of privacy, I refer to information privacy—primarily in regard to federal statutory law²³ and enforcement—rather than decisional privacy (such as the right to abortion)²⁴ or other types of privacy.²⁵ In

¹⁸ See *infra* Part III.

¹⁹ When I use the term “corporate governance” in this Article, I use it as shorthand for “governance of others by corporations.” In other words, as used in this Article, corporate governance should not be confused with the traditional understanding of corporate governance, *i.e.*, a corporation’s internal governance of itself.

²⁰ This is particularly necessary because “[t]oday, we have hundreds of laws pertaining to privacy—the common law torts, criminal law, evidentiary privileges, constitutional law, at least twenty federal statutes, and numerous statutes in each of the fifty states.” Daniel Solove, *The Origins and Growth of Information Privacy Law*, 828 PLI/PAT 23, 27 (2005).

²¹ Surveillance can be thought of as “the cloak-and-dagger stuff of hidden microphones” or alternatively as “the increasingly routine use of personal data and systematic information in the administration of institutions, agencies, and businesses.” JOHN GILLIOM, *OVERSEERS OF THE POOR* 2 (2001).

²² See generally, Solove, *supra* note 4.

²³ Most notably, this Article’s scope does not include the constitutional right to information privacy. One commentator explains the distinction between constitutional decisional privacy and constitutional information privacy thusly:

Four years after *Roe v. Wade*, in 1977, the Court held in *Whalen v. Roe* that the constitutionally protected ‘zone of privacy’ extends to two distinct types of interests: (1) ‘independence in making certain kinds of important decisions’; and (2) the ‘individual interest in avoiding disclosure of personal matters.’ The former interest describes *Griswold* and *Roe*; the latter interest was one that the Court had not yet defined. This latter interest has been called the ‘constitutional right to information privacy.’

Solove, *supra* note 20, at 47.

²⁴ The decisional/informational binary has been criticized by some scholars or acknowledged by others as a binary with overlapping areas:

Information privacy concerns the collection, use, and disclosure of personal information. Information privacy is often contrasted with “decisional privacy,” which concerns the freedom to make decisions about one’s body and family But information privacy increasingly incorporates elements of decisional privacy as the use of data both expands and limits individual autonomy.

DANIEL J. SOLOVE & MARC ROTENBERG, *INFORMATION PRIVACY LAW* 1 (2003).

addition, this project primarily focuses on information privacy relations between corporations and individuals. A larger project—which is beyond the scope of this Article—would focus more closely on the tripartite relationship between corporations, individuals, and the government in regard to information privacy.²⁶

Part I of this Article will briefly canvass the current state of information privacy law and jurisprudence. Part II argues that domestic and international legal regimes are governed not only by governments but also by private actors, including corporations. Part III presents three examples of corporations engaging in private governance of information privacy. Part IV addresses some of the implications of the private governance model as applied to information privacy law.

PART I

THE CURRENT STATE OF INFORMATION PRIVACY

Before embarking on the fundamental argument regarding corporate power's influence on the lack of consumer privacy, it is first necessary to briefly describe the current landscape of information privacy law and scholarship.

A. *Definitional Debates*

Privacy scholars have devoted much energy to defining the concept of privacy.²⁷ This definitional project has resulted in a wide array of notions of what privacy means. For example, privacy has been variously understood to mean transparency,²⁸ anonymity,²⁹ the right to control one's personal information,³⁰ and the right to be let alone.³¹ Some privacy scholars understand information privacy to

²⁵ See generally Anita L. Allen-Castellitto, *Understanding Privacy: The Basics*, 865 PLI/PAT 23, 28 (2006) (stating that “[t]here are at least four basic types of privacy. They are (1) informational privacy; (2) physical privacy; (3) decisional privacy; and proprietary.”).

²⁶ See generally ROBERT O’ HARROW, JR., *NO PLACE TO HIDE* (2004) (examining this tripartite relationship).

²⁷ “Privacy as a concept involves what privacy entails and how it is to be valued. Privacy as a right involves the extent to which privacy is (and should be) legally protected.” SOLOVE ET AL., *supra* note 9, at 39.

²⁸ See generally DENNIS BAILEY, *THE OPEN SOCIETY PARADOX: WHY THE 21ST CENTURY CALLS FOR MORE OPENNESS—NOT LESS* (2004).

²⁹ WESTIN, *supra* note 3, at 31–32.

³⁰ See Anita Allen, *Origins and Growth of U.S. Privacy Law*, 701 PLI/PAT 83, 89 (2002).

³¹ See generally, Warren & Brandeis, *supra* note 5.

mean secrecy.³² The secrecy paradigm posits that “privacy is invaded by uncovering one’s hidden world, by surveillance, and by the disclosure of concealed information.”³³ Similarly, “the invasion conception” understands privacy as “violated by the invasive actions of particular wrongdoers who cause direct injury to victims.”³⁴ Other paradigms of privacy include surveillance, intrusion, solitude, mental distance, and limited access to the self.³⁵ For example, Charles Fried argues that, “[p]rivacy is not simply an absence of information about us in the minds of others; rather it is the *control* we have over information about ourselves.”³⁶ Ruth Gavison describes privacy as “concern for limited accessibility,”³⁷ while Jeffrey Rosen maintains that “[p]rivacy protects us from being misdefined and judged out of context in a world of short attention spans, a world in which information can easily be confused with knowledge.”³⁸ As one commentator explains, “[t]raditionally, privacy violations have been understood in a particular manner The dominant metaphor for modern invasions of privacy is Big Brother, the ruthless totalitarian government in George Orwell’s novel *1984*.”³⁹ Such understandings of privacy generally explore how the individual does, or should, construct his or her privacy, or lack thereof.

Other scholars’ understandings of privacy incorporate broader concepts such as human dignity, self-development, and democracy. For example, Julie E. Cohen argues that “[t]he condition of no-privacy threatens not only to chill the expression of eccentric individuality, but also, gradually, to dampen the force of our aspirations to it.”⁴⁰ And Paul M. Schwartz contends that “[t]he maintenance of a democratic order requires both deliberative democracy and an individual capacity for self-determination [T]he emerging pattern

³² Of course, some scholars critique the notion of privacy altogether, arguing that “the best way to curtail the need for governmental control and intrusion is to have somewhat less privacy.” AMITAI ETZIONI, *THE LIMITS OF PRIVACY* 213 (1999). Other critics argue that privacy is not a distinct concept at all. See, e.g., Neil M. Richards, *The Information Privacy Law Project*, 94 *Georgetown L. J.* 1087 134-35 (2006).

³³ SOLOVE, *supra* note 15, at 8.

³⁴ *Id.*

³⁵ See generally, WESTIN, *supra* note 3.

³⁶ Charles Fried, *Privacy*, 77 *YALE L.J.* 475, 482 (1968).

³⁷ Gavison, *supra* note 3, at 423.

³⁸ JEFFREY ROSEN, *THE UNWANTED GAZE: THE DESTRUCTION OF PRIVACY IN AMERICA* 8 (2000).

³⁹ SOLOVE, *supra* note 15, at 7.

⁴⁰ Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 *STAN. L. REV.* 1373, 1426 (2000).

of information use in cyberspace poses a risk to these two essential values.”⁴¹

B. Proposed Solutions

Scholars approach the problem of information privacy law from a variety of approaches and with a myriad of doctrinal tools. For example, some scholars call for treating personal information as property.⁴² Others argue that violations of personal information should be treated as tortious acts.⁴³ Still others maintain that information privacy should be subsumed within the rubric of contract law; that is, consumers should have the ability to contract with companies for the use, sharing, or collection of their information.⁴⁴

On the statutory side, some commentators call for a privacy regime that covers the entire field, rather than the current sectoral approach to privacy.⁴⁵ Such a regime would emulate the European Union’s comprehensive approach to informational privacy⁴⁶ and would certainly evoke the Fair Information Practice Standards of 1977.⁴⁷ For example, in arguing for a change in the architecture of privacy, Daniel Solove responds negatively to those who argue for market-based solutions to problems of information privacy⁴⁸ and argues that

⁴¹ Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1609, 1658 (1999).

⁴² See *supra* note 14.

⁴³ See *supra* note 12.

⁴⁴ See *supra* note 13.

⁴⁵ See, e.g., SOLOVE, *supra* note 15, at 101.

⁴⁶ See Council Directive 95/46, art. 4, § 1(c), 1995 O.J. (L 281) 31, 39 (EC).

⁴⁷ *Id.*

Fair Information Practices were recommended by the Report of the U.S. Privacy Protection Commission published in 1977. Under various models of ‘fair information practices,’ standards such as these should be met to the extent possible: (1) the existence of data systems containing personal information should not be a secret; (2) personal information should only be collected for narrow, specific purposes; (3) personal information should only be used in a ways that are similar to and consistent with the primary purposes for its collection; (4) personal information should be collected only with . . . informed consent . . . ; (5) personal information should not be shared with third parties without notice or consent; (6) . . . the duration of storage of personal information should be limited; and (7) individuals should have access to personal information about themselves and should be permitted to correct errors; (8) those who collect personal data should insure the security and integrity of personal data and data systems.”

Allen-Castellitto, *supra* note 25, at 35–36.

⁴⁸ See SOLOVE, *supra* note 15, at 80–87. Solove also argues that “law should hold that companies collecting and using our personal information stand in a fiduciary relationship with us.” *Id.* at 103.

“law must restructure our relationships with the entities collecting and using our personal information”⁴⁹ that cause privacy failures and that information privacy is “a question of social design.”⁵⁰ One of his proposals is to expand the jurisdiction of the FTC and provide the FTC with greater resources.⁵¹ Calls for a change in the architecture of information privacy appear to represent the coming trajectory of information privacy scholarship and law.

C. *Deficiencies in Federal Information Privacy Law*

The FTC and many federal privacy statutes have been criticized as not being effective enough in protecting privacy.⁵² These statutes include, *inter alia*, the Gramm-Leach-Bliley Act,⁵³ the Fair Credit Reporting Act and its amendment,⁵⁴ the Fair and Accurate Credit Transactions Act of 2003,⁵⁵ the Telephone Consumer Protection Act of 1991,⁵⁶ the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”),⁵⁷ and the Children’s Online Privacy Protection Act.⁵⁸ Generally, the scholarly discussion proceeds by attacking some of the flaws in these statutes and then suggesting some relatively minor patches, such as changing opt-out rights to opt-in rights.⁵⁹

Yet most federal information privacy laws are toothless. For example, the Gramm-Leach-Bliley Act purports to protect individuals by requiring companies to disseminate privacy notices.⁶⁰ But as has of-

⁴⁹ *Id.* at 226.

⁵⁰ *Id.*

⁵¹ *Id.* at 108.

⁵² See, e.g., Paul Lansing & Mark D. Halter, *Internet Advertising and Right to Privacy Issues*, 80 U. DET. MERCY L. REV. 181, 195 (2003).

⁵³ 15 U.S.C. §§ 6801–09 (2000).

⁵⁴ 15 U.S.C. § 1681 (2000).

⁵⁵ Pub. L. No. 108-159, 117 Stat. 1952 (2003).

⁵⁶ Pub. L. No. 102-243, 105 Stat. 2394 (codified at 47 U.S.C. § 227 (2000)). This Act “permits people to request that telemarketers not call them again. If the telemarketer continues to call, people can sue for damages of up to five hundred dollars for each call.” Solove, *supra* note 20, at 61.

⁵⁷ Pub. L. No. 104-191, 110 Stat. 1936 (1996).

⁵⁸ 15 U.S.C. §§ 6501–06 (2000). “HIPAA required the Department of Health and Human Services (HHS) to draft regulations to protect the privacy of medical records. HHS’s regulations, among other things, require that people authorize all uses and disclosures of their health information that are not for treatment, payment, or health care operation (such as for marketing purposes).” Solove, *supra* note 20, at 62.

⁵⁹ See generally, Jeffrey M. Lacker, *The Economics of Financial Privacy: To Opt out or Opt in?*, ECON. Q. FED. RES. BANK OF RICH., 7–10 (2002), available at http://privare.fbk.eur.nl/Literature/references/lacker_the%20economics%20of%20financial%20privacy_to%20opt%20out%20or%20opt%20in.pdf.

⁶⁰ 15 U.S.C.S. § 1603 (LexisNexis 2006).

ten been noted, these privacy policies in fact serve to inform individuals of what privacy consumers *do not* have, and are too cumbersome and legalistic for most people to read.⁶¹ Moreover, they tend to make the option of opting out such a hassle that most consumers don't even bother.⁶²

Another example of federal privacy laws' impotence is the Fair and Accurate Credit Transaction Act of 2003 ("FACTA"), which added new sections to the federal Fair Credit Reporting Act ("FCRA").⁶³ The FCRA was intended to help consumers fight the growing crime of identity theft and protect their personal credit information.⁶⁴ These federal statutes purport to give consumers the power to find out what is in their credit report and correct erroneous tradelines. But the reality is that consumers have a notoriously difficult time when they try to have errors corrected.⁶⁵ A large part of the reason it is so hard for individuals to correct errors is because these federal credit-reporting statutes are, for the most part, written in favor of the Credit Reporting Agencies ("CRA"). For example, entities can only obtain your credit file for a "permissible purpose."⁶⁶ However, this "permissible purpose" requirement has been stretched to the point of irrelevancy. The CRAs release credit reports carelessly, knowing that it will be difficult for any person to bring a successful suit against them, because the liability standard is malice or intent.⁶⁷ Thus, a CRA will only be found liable for sharing credit reports or failing to correct erroneous information if their actions were malicious or intentional. This standard of proof is much too high for consumers. Negligence is generally what is occurring at the CRAs,⁶⁸ and the standard for liability should be just that—negligence.

The Telephone Consumer Protection Act ("TCPA") of 1991 was intended to protect the privacy interests of telephone users by restricting telemarketers' ability to place unsolicited calls.⁶⁹ But as one

⁶¹ See, e.g., Janice A. Alwin, Comment, *Privacy Planning: Putting the Privacy Statutes to Work for You*, 14 DEPAUL BUS. L.J. 353, 362 (2002).

⁶² See *infra*, Part III.A.

⁶³ 15 U.S.C.S. § 1681–1681x (LexisNexis 2006).

⁶⁴ 15 U.S.C.S. § 1681 (LexisNexis 2006).

⁶⁵ See, e.g., United States Public Interest Research Group, *Mistakes Do Happen: Credit Report Errors Mean Consumers Lose*, March 1998, at p. 9, <http://uspirg.org/uspig.asp?id2=5970> (concluding that there is still tremendous difficulty in clearing one's name after mistake or fraud occurs).

⁶⁶ 15 U.S.C.S. § 1681b (LexisNexis 2005).

⁶⁷ 15 U.S.C. § 1681h(e) (2000).

⁶⁸ See Joel R. Reidenberg, *Privacy in the Information Economy: A Fortress or Frontier for Individual Rights?*, 44 Fed. Comm. L.J. 195, 211-12 (1992).

⁶⁹ See 47 U.S.C.S. § 227 (LexisNexis 2006).

scholar has noted, the very purpose of the statute is misguided: “[t]he TCPA . . . aims at redressing the aggravation of disruptive phone calls, and it does not govern the collection, use, or sale of personal data.”⁷⁰

The preceding discussion regarding the inadequacy of federal statutory law is closely connected to a second problem with domestic information privacy law: the gaping areas of privacy that are left unprotected and unaddressed by current law. In other words, statutory law “protects” privacy by type, e.g., medical information, video rental information, financial information, etc. “Despite the growth of the Information Society, the United States has resisted all calls for omnibus or comprehensive legal rules for fair information practice in the private sector.”⁷¹ As one scholar admonishes, a “strategy of narrowly targeted sector-specific reforms has been used in U.S. information privacy law for the last two decades with disastrous results”⁷² These “disastrous results” have been the complete lack of protection for certain types of activities (rather than types of personal information), such as grocery stores selling their customers’ data to corporate data aggregators such as Acxiom and ChoicePoint, and allowing such third party companies to construct disturbingly detailed profiles on millions of (indeed, most) Americans and American households.⁷³

Moreover, the Privacy Act of 1974, arguably “the most comprehensive U.S. law pertaining to privacy,”⁷⁴ applies only to government actors. Therefore, “private corporations are not bound by the fair information practices, open-access rules, and data-ownership principles embodied in the Act.”⁷⁵

PART II

CORPORATE POWER AND CORPORATE GOVERNANCE

Part II of this Article argues that the scholarly attempts at resolving problems in information privacy law have failed because there is a fundamental dynamic at work that has gone unrecognized. Information privacy laws actually have the effect of facilitating greater collec-

⁷⁰ SOLOVE, *supra* note 15, at 69.

⁷¹ Joel R. Reidenberg, *Setting Standards for Fair Information Practice in the U.S. Private Sector*, 80 IOWA L. REV. 497, 500 (1995).

⁷² Jane K. Winn, *Contracting Spyware by Contract*, 20 BERKELEY TECH. L.J. 1345, 1346 (2005).

⁷³ See Richard Behar, *Never Heard of Acxiom? Chances Are It's Heard Of You*, FORTUNE, Feb. 23, 2004, at 140.

⁷⁴ John M. Eden, *When Big Brother Privatizes: Commercial Surveillance, the Privacy Act of 1974, and the Future of RFID*, 2005 DUKE L. & TECH. REV. 20, *4 (2005).

⁷⁵ *Id.*

tion, sharing, and use of personal information because information privacy is governed as much by corporate actions and corporate decision-making as by governmental regulation. In other words, information privacy is governed not just by governmental law but also by corporations.⁷⁶

As Daniel Greenwood has observed:

Once corporations are understood as power sources, a part of our governance system rather than an object of it, then *the market for law appears radically illegitimate*, an example of the powerful seizing the power of the state to increase their own power. Rather than seeing corporations as Tocquevillian intermediate institutions restraining the state, we should see them as state-like themselves, part of the classic liberal nightmare of a state acting in its own interest and not that of its citizens.⁷⁷

The required discussion that has thus far been largely ignored but is at the heart of information privacy law and policy is this: privacy laws and enforcement represent a façade of protection for consumers, keeping them complacent in the purported knowledge that someone is protecting their privacy interests. Information privacy law and privacy enforcement are primarily deflections from the fact that individuals' privacy is a façade because corporate power drives information privacy law.

A. *Corporate Power*

It is certainly well recognized that corporations exert enormous power⁷⁸ both domestically and globally.⁷⁹ Corporate power has been on the rise since the late nineteenth century,⁸⁰ when corporations

⁷⁶ I understand corporate power by defining power as "possession of control, authority, or influence over others." M-W.com dictionary definition, <http://www.m-w.com/dictionary/power> (last visited September 25, 2006).

⁷⁷ Daniel J.H. Greenwood, *Markets & Democracy: The Illegitimacy of Corporate Law*, 74 UMKC L. REV. 41, 44 (2005) (emphasis added).

⁷⁸ Robert Dahl, *Power as the Control of Behavior*, in POWER 37 (Steven Lukes ed., 1986). "The analysis of power is often concerned . . . with the identification of elites and leadership, the discovery of the ways in which power is allocated to different strata, relations among leaders and between leaders and non-leaders, and so forth." *Id.*

⁷⁹ See generally, TED NACE, GANGS OF AMERICA I (2003) ("[T]he corporation has become the core institution of the modern world. Designed to see profit and power, it has pursued both with endless tenacity, steadily bending the framework of law and even challenging the sovereign status of the state.").

⁸⁰ Comment, Katie J. Thoennes, *Frankenstein Incorporated: The Rise of Corporate Power and Personhood in the United States*, 28 HAMLINE L. REV. 203, 205 (2005) ("[C]orporations have come to dominate society and politics at both a national and state level by securing for themselves rights and privileges that were once reserved

were recognized as legal persons.⁸¹ It has been reported that twenty-two American corporations have a market capitalization greater than the gross domestic product of twenty-two specified individual nations.⁸² Moreover, a recent *Business Week* poll showed that nearly three-quarters of Americans think “[b]usiness has gained too much power over too many aspects of American life.”⁸³ One commentator has stated with alarm that “as corporations gain in autonomous institutional power and become more detached from people and place, the human interest and the corporate interest increasingly diverge.”⁸⁴ Indeed, scholars have even gone so far as to attribute godly status to corporations.⁸⁵ This corporate power has, more often than not, been at the expense of individuals. Corporations drive the continual erosion of personal information privacy. It is not just the data aggregators or data brokers driving this erosion; rather, it is the entirety of corporate America and Fortune 500 companies that view personal information as a commodity and believe that it is their corporate right to exploit and manipulate personal information as they see fit.⁸⁶

Individuals’ personal information is of enormous economic value to the business world. In fact, personal information fuels the wheels of commerce. According to one scholar,

Marketers “rent” lists of names and personal information from database companies, which charge a few cents to a dollar for each name. Over 550 companies compose the personal information industry, with annual revenues in the billions of dollars. The sale of mailing lists alone (not including the sales generated by the use of the lists) generates \$3 billion a year. The average consumer is on around 100 mailing lists and is included in at least 50 databases. An increasing number of companies with databases . . . are

exclusively for the American people.”).

⁸¹ *Santa Clara County v. S. Pac. R.R.*, 118 U.S. 394, 396 (1886) (wherein the Court stated that “[t]he Court does not wish to hear argument on the question whether the provision in the Fourteenth Amendment to the Constitution, which forbids a State to deny to any person within its jurisdiction the equal protection of the laws, applies to these corporations. We are all of opinion that it does.”).

⁸² LAWRENCE E. MITCHELL, *CORPORATE IRRESPONSIBILITY* 2 (2001).

⁸³ *Business Week/Harris Poll: How Business Rates: By the Numbers*, BUS. WK., Sept. 11, 2000, at 144 available at http://www.businessweek.com/2000/00_37/b3698004.htm.

⁸⁴ DAVID. C. KORTEN, *WHEN CORPORATIONS RULE THE WORLD* (2001).

⁸⁵ See generally, Douglas Litowitz, *The Corporation as God*, 30 J. CORP. L. 501 (2005).

⁸⁶ See, e.g., Paul Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1609, 1633–34 (1999) (arguing that “personal information in the private sector is often unaccompanied by the presence of basic legal protections. Yet, private enterprises now control more powerful resources of information technology than ever before.”).

realizing that their databases are becoming one of their most valuable assets⁸⁷

Because personal information is of such importance to corporations and because corporations exert so much influence in the realm of information privacy, the problem of the erosion of individual information privacy can be solved only by crippling corporations' stranglehold on our information privacy laws and policies.⁸⁸

It is important to draw a distinction between "corporate power" and a more general concept of "business power." As has been well established in the political, economic, and legal literature, the corporation is a unique historical and sociological beast that is both formally and instrumentally very much different from other business entities, such as partnerships or sole proprietorships. As David C. Korten describes corporations in his influential work, *When Corporations Rule the World*:

The publicly-traded, limited liability corporation is capitalism's institutional form of choice because it allows the virtually unlimited concentration of power with minimal public accountability or legal liability. Actual shareholders . . . bear no personal liability beyond the value of their investments. Directors and officers are protected from financial liability from acts of negligence or commission by the corporation's massive legal resources and company-paid insurance policies. . . . Unlike real people, who are eventually rendered equal by the grave, corporations are able to grow and reproduce themselves without limit, "living" and amassing power indefinitely.⁸⁹

In other words, concerns regarding the social ills emanating from business tend to focus on the limited liability corporation because, "the large, limited-liability, publicly traded . . . corporations dominate our economy, politics, and culture. The limited-liability corporation dominates our entire society."⁹⁰

Moreover, as Lawrence Mitchell forcefully argues, corporations' primary purpose is to maximize shareholders' short-term profits.⁹¹

⁸⁷ SOLOVE, *supra* note 15, at 19.

⁸⁸ Indeed, information privacy law and enforcement is merely an exercise in legitimization, *i.e.*, a cover or masquerade for corporate domination of the American consumer.

⁸⁹ KORTEN, *supra* note 84, at 104–05. *See generally*, Litowitz, *supra* note 85, at 525 ("The underlying dilemma is that corporations have tremendous economic and political power (not to mention their power to shape public opinion) but they are ruled by a handful of appointed managers.").

⁹⁰ Charlie Cray & Lee Drutman, *Corporations and the Public Purpose: Restoring the Balance*, 4 SEATTLE J. SOC. JUST. 305, 306 (2005).

⁹¹ MITCHELL, *supra* note 82, at 4–5.

Thus, corporations' main purpose conflicts with many values of community such as environmental protection, wage increases, and privacy.

The understanding that corporate power is a dominant global and domestic force is merely a foundational understanding for unearthing the dynamic at the core of the impasse in information privacy law.

B. Governance by Corporations

As critical legal scholars argue, law often serves merely as legitimization or rationalization of the existing structure; in other words, ostensibly neutral norms and laws deflect attention from hegemonic forces.⁹² This argument can also be applied to information privacy law, inasmuch as most of our U.S. information privacy laws are seemingly neutral but in fact are largely driven by corporate interests—and thus erode consumer privacy rather than enhance it. In the field of information privacy and in the law more generally, “[c]orporations are power centers, loci of value struggles, political fora. They are not citizens but governance structures and not neutral but deeply influential—if illegitimate—participants in our political struggles.”⁹³

Drawing upon the general concept of corporate power, many scholars have observed that authority, legal norms, and governance are not solely the province of government. Specifically, corporations exert authority via “specific modes through which corporate actors create and shape legal regimes.”⁹⁴ While some commentators describe this dynamic as one in which corporate actors exercise authority or shape legal norms, other forward-looking scholars have gone further and argue that when corporations shape the content of legal regimes in a way that resembles government rulemaking and enforcement, they are actually engaged in governance.⁹⁵ Some of these scholars refer to the symbiotic relationship between government and multiple non-governmental actors, such as corporations, as the “new governance.” Orly Lobel argues that “[t]he new governance model challenges . . . conventional assumptions . . . [and] broadens the de-

⁹² Cf. Kimberle Williams Crenshaw, *Race, Reform & Retrenchment: Transformation and Legitimation in Antidiscrimination Law*, 101 HARV. L. REV. 1331 (1988) (arguing that the racism inherent in purportedly neutral norms must be exposed).

⁹³ Greenwood, *supra* note 77, at 43.

⁹⁴ Dan Danielsen, *How Corporations Govern: Taking Corporate Power Seriously in Transnational Regulation and Governance*, 46 HARV. INT'L L.J. 411, 412 (2005).

⁹⁵ *Id.* “To govern” means “to control the actions or behavior of” or “to exercise a deciding or determining influence on.” AMERICAN HERITAGE COLLEGE DICTIONARY 588 (3d ed. 1993).

cision-making playing field by involving more actors in the various stages of the legal process . . . [Thereby, t]he exercise of normative authority is pluralized.”⁹⁶ Dan Danielson explains that this governance is engendered by way of various types of corporate behavior:

Sometimes corporations contribute through interpretations of or reactions to a legal rule scheme. Sometimes they supply rules where none exist. Sometimes they shape the rule scheme through direct political or economic pressure on regulators. Sometimes they shape it by evading the rule scheme and doing business elsewhere. Sometimes, to satisfy other business purposes, they adopt more stringent practices than the applicable rules require. Sometimes they act on their own to get a market edge or exploit an opportunity.⁹⁷ Sometimes they act in groups to create a harmonized regulatory environment or to prevent regulation. . . . *When corporations create or shape the content, interpretation, efficacy, or enforcement of legal regimes and, in so doing, produce effects on social welfare similar to the effects resulting from rulemaking and enforcement by governments, corporate actors are engaged in governance.*⁹⁸

In other words, when corporations affect the law in ways that produce effects similar to those that result from governmental law, corporate private governance is occurring. While it is common to confuse the term “governance” with “government,” the two terms are entirely distinct; indeed, the concept of government is but a subset of the broader concept of governance. “Governance involves interaction between the formal institutions and those in civil society. Governance refers to a process whereby elements in society wield power, authority and influence and enact policies and decisions concerning public life and social upliftment.”⁹⁹

Of course, the concept of governance by corporations may be viewed as contrary to democratic principles because generally, “[f]or lawyers, governance is a constitutional issue.”¹⁰⁰ However, the “le-

⁹⁶ Orly Lobel, *The Renew Deal: The Fall of Regulation and the Rise of Governance in Contemporary Legal Thought*, 89 MINN. L. REV. 342, 373 (2004).

⁹⁷ For example, in some instances, so-called competitors “collude through cartels or strategic alliances to increase profits by setting market prices above the level of optimal efficiency.” KORTEN, *supra* note 84, at 82.

⁹⁸ Danielson, *supra* note 94, at 412 (emphasis added).

⁹⁹ The Global Development Research Center, *Understanding the Concept of Governance*, <http://www.gdrc.org/u-gov/governance-understand.html> (last visited on Oct. 9, 2006).

¹⁰⁰ Christoph Engel, *A Constitutional Framework for Private Governance 2* (MPI Collective Goods Preprint No. 2001/4, Mar. 2001), available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=269310 (last visited September 3, 2006).

gitimacy” question vis-à-vis private governance¹⁰¹ is beyond the scope of this Article. More importantly, “the normative statement that only duly elected and representative governments ‘ought’ to be capable of exercising political authority must not be confused with the empirical fact that corporations ‘are’ increasingly functioning authoritatively in ruling themselves and others.”¹⁰²

The central focus of this Article is that the traditional understanding of governance as emanating solely from the government must be—and is being—rethought. Indeed, to dichotomously understand corporate acts as “private” and government acts as “public”¹⁰³ “does not do justice to the dynamic interconnectedness of each move and countermove by state and corporate actors.”¹⁰⁴ Governments and corporate actors are engaged in an intricate and profoundly symbiotic dance of acting and reacting to the other’s behaviors, decisions, and regulations. The legal “rules” therefore often reflect a series of decisions and behaviors on the part of private actors and the government that together form the authoritative norm. As Paul Schiff Berman has noted, “[l]egal scholars and policymakers have an unfortunate tendency to assume that legal norms, once established, simply take effect and constitute a legal regime.”¹⁰⁵ Moreover, Berman applauds the groundbreaking academics that study actual practices and real-life exercises of authority to determine the *true* legal regime. He observes that such scholars:

refuse to focus solely on who has the formal authority to articulate norms or the coercive power to enforce them. Instead, they aim to study empirically which statements of authority tend to be

¹⁰¹ Randy Barnett argues that:

[a] lawmaking system is legitimate if there is a prima facie duty to obey the laws it makes. Neither “consent of the governed” nor “benefits received” justifies obedience. Rather, a prima facie duty of obedience exists either (a) if there is actual unanimous consent to the jurisdiction of the lawmaker or, in the absence of consent, (b) if laws are made by procedures which assure that they are not unjust.

Randy E. Barnett, *Constitutional Legitimacy*, 103 COLUM. L. REV. 111, 111 (2003).

¹⁰² CUTLER, *supra* note 1, at 33.

¹⁰³ Indeed, in 1969 John Galbraith argued that certain corporations are in fact public institutions: “By no known definition of private enterprise can these specialized firms or subsidiaries be classified as private corporations.” John Kenneth Galbraith, *The Big Defense Firms Are Really Public Firms and Should Be Nationalized*, N.Y. TIMES MAG., Nov. 16, 1969, at 50.

¹⁰⁴ Danielson, *supra* note 94, at 415.

¹⁰⁵ Paul Schiff Berman, *From International Law to Law and Globalization*, 43 COLUM. J. TRANSNAT’L L. 485, 498 (2005).

treated as binding in actual practice and by whom. . . . Accordingly, the nation-state is denied any special status as a law-giver.¹⁰⁶

Similarly, Claire Cutler chides those who would rather sweep the reality of private governance under a formalistic rug:

[T]he move of private authority to obscurity is at root an ideological move inspired by the “liberal art of separation” that serves to isolate and insulate increasing aspects of existence from public scrutiny and review. The formalistic associations of authority with the state function ideologically by depicting the world not as it is but as it ought to be.¹⁰⁷

An understanding of corporate behavior that incorporates the notion that corporations actually shape the legal structure and actually govern alongside local, state, and national governments allows an understanding of corporate power that is something more than a vague concept of which everyone is aware but which few can coherently explain. Understanding corporate power as a type of governance in the domestic (and transnational) spheres renders the amorphous concrete. For example, in the regulatory scheme, there may exist a governmental law alongside corporate behavior regarding that same law. In reality, the corporate “rules” and behaviors may—and increasingly do—represent the dominant mode of behavior and the actual mode of governance in that area. As another example, corporations may choose to act in ways that openly and egregiously violate the legislative mandate because governmental deterrence is weak and ineffective. These intentional violations may nevertheless operate as the “rule” in the respective arena and thus govern the field as authoritative.¹⁰⁸ Furthermore, corporations may interpret legislation in a way that favors corporate interests, and the government may acquiesce in this interpretation through silence and inaction. A final example is the profound effect that corporate lobbying has on the ultimate statutory language of privacy statutes and regulatory rules.¹⁰⁹ As

¹⁰⁶ *Id.* at 510.

¹⁰⁷ Cutler, *supra* note 1, at 24.

¹⁰⁸ Anthony J. Fejfar, *Corporate Voluntarism: Panacea or Plague? A Question of Horizon*, 17 DEL. J. CORP. L. 859, 923 (1992) (“Corporations influence legislation and its enforcement through lobbying and through the failure to abide by enacted laws and regulations.”).

¹⁰⁹ See generally Matt Taibbi, *The Secret History of the Most Corrupt Man in Washington*, ROLLING STONE MAG., at 38 (Apr. 4, 2006) (profiling lobbyist Jack Abramoff); Jon Hanson & David Yosifon, *The Situation: An Introduction to the Situational Character, Critical Realism, Power Economics, and Deep Capture*, 152 U. PA. L. REV. 129 (2003). Internationally, some scholars argue the situation is even worse.

Outside Europe and the U.S., the extent to which states have become rule-takers rather than rule-makers is greater than most citizens think,

many commentators note, corporations exert tremendous power through “their political action committees, their lobbyists, [and] their lawyers.”¹¹⁰

Conceptualizing governance as a symbiotic relationship between governmental and non-governmental actors engenders an understanding of the specific nature of corporate power. Susan Sassen argues that the question is whether “the weight of private . . . interests in [the] specific work of the state become[s] constitutive of that authority and indeed produce[s] a hybrid that is neither fully private nor fully public?”¹¹¹ Sassen answers her own question in the affirmative. Indeed, this is the fundamental difference between dualism and unity theories. In a dualistic world, the public and the private are distinct worlds and operate separately in their own spheres. In a unified world, the public and the private interact organically and the ensuing legal regime is just that—organic and informed by both spheres.

Scholars in the field of transnational law have explored this phenomenon under the academic terminology of “transnational governance.”¹¹² For example, one commentator in the field notes that “[c]onstitutions were designed to frame states, and to frame the law within the state. Today, however, it seems that the social engineering and controls embodied in such instruments have given way to ‘governance’—a loose network of constitutionally invisible, often private,

largely because when governments announce new regulatory laws they are somewhat embarrassed to disclose that the national legislature voted for those laws without having any say in shaping them.

JOHN BRAITHWAITE & PETER DRAHOS, *GLOBAL BUSINESS REGULATION* 3 (2000).

¹¹⁰ NACE, *supra* note 79, at 12. For example, “[t]hrough trade agreements, corporate libertarians press governments to provide absolute protection for the intellectual property rights of corporations.” KORTEN, *supra* note 84, at 81. Another commentator writes:

Lobbying is yet another source of corporate influence on law. Most, if not all, major corporations employ legislative liaisons assigned to monitor legislative activities and to coordinate lobbying efforts to assure that the corporate viewpoint is heard. In addition, virtually every industry has some sort of trade association or manufacturer’s association designed to present the common interests of the otherwise competing firms. Managing the law and the legislative process has become a tool of competitive strategy.

Daniel T. Ostas, *Deconstructing Corporate Social Responsibility: Insights from Legal and Economic Theory*, 38 AM. BUS. L.J. 261, 270–71 (2001).

¹¹¹ Saskia Sassen, *The State and Globalization*, in *THE EMERGENCE OF PRIVATE AUTHORITY IN GLOBAL GOVERNANCE* 91 (Rodney Bruce Hall & Thomas J. Biersteker eds., 2002).

¹¹² See, e.g., *TRANSNATIONAL GOVERNANCE AND CONSTITUTIONALISM: INTERNATIONAL STUDIES IN THE THEORY OF PRIVATE LAW* (Christian Joerges, Inger-Johanne Sand & Gunther Teubner, eds., 2004).

actors.”¹¹³ International law scholars recognize that multinational corporations have begun to take over the role of the state in many areas. “As the state was once the exclusive subject of international law, the corporation, the state’s creation, has now become a primary subject displacing the state’s exclusivity in this sphere just as it has displaced state ownership and regulation in the market.”¹¹⁴

Although the concept of corporate and private governance is being explored widely in the transnational law literature,¹¹⁵ there is a relative dearth¹¹⁶ of scholarly work on the topic in the realm of domestic law.¹¹⁷ As Paul Berman argues, “because legal scholars are so focused on the official organs of legal power—nation-state governments—they have been less likely to embrace ideas about norm-development in non-state arenas.”¹¹⁸ Dan Danielson notes that “scholars have focused little attention on explicating the precise mechanisms through which corporations contribute to transnational regulation and governance or the extent to which the social welfare effects of regulation and policy may be attributable to corporate activity.”¹¹⁹ This Article is an endeavor to bring the concept of corporate private governance into the domestic sphere and, specifically, into the informational privacy literature.

PART III

CORPORATIONS’ GOVERNANCE OF INFORMATION PRIVACY

In the area of information privacy, corporations have been given wide leeway to govern, i.e., to affect domestic information privacy in

¹¹³ Andras Sajó, *Book Review*, 3 INT’L J. CONST. L. 697, 697 (2005).

¹¹⁴ Joel R. Paul, *Holding Multinational Corporations Responsible Under International Law*, 24 HASTINGS INT’L & COMP. L. REV. 285, 290 (2001).

¹¹⁵ See *id.* at 285–86 (noting that “private individuals and non-governmental organizations acting both internationally and domestically are contributing to the emergence of new international norms. These new international norms confer greater rights and obligations on private individuals and firms, shifting the focus of international law.”).

¹¹⁶ As one scholar argues, “[p]rivate [governance] is not a new phenomenon, but public interest in it is. This explains why there is no coherent legal framework for private [governance] yet.” Engel, *supra* note 100, at 23.

¹¹⁷ But see John M. Conley & Cynthia A. Williams, *Engage, Embed, and Embellish: Theory versus Practice in the Corporate Social Responsibility Movement*, 31 J. CORP. L. 1, 6 (arguing that “understanding the realities of [corporate social responsibility] provides a unique opportunity to test new governance theory against practice”); Lobel, *supra* note 96, at 342 (arguing for a shift in legal thought from a regulatory to a new governance model).

¹¹⁸ Berman, *supra* note 105, at 490.

¹¹⁹ Danielson, *supra* note 94, at 411.

ways that produce effects similar to those that result from governmental law.

In Part III, I will present three examples of corporations' governing the field of information privacy law through corporate action and symbiotic government action or inaction. The first is an example of corporations' *interpretation* of privacy law; the second example demonstrates corporations' *bypassing* of privacy legislation; and the third example describes corporations' *intentional violation* of information privacy laws. Each of these examples represents more than corporate action or reaction to governmental law. Instead, these examples demonstrate the manners by which corporations have engaged in private governance and shaped the information privacy regime.

I argue that: (1) when corporations' actions have an effect on the market that resembles the effect of governmental authority and (2) that corporate authority goes largely unchallenged and is, in fact, accepted as the social norm, corporations are engaging in governance.¹²⁰

To give practical meaning to this definition, it might prove useful to imagine on a broader level what governance means in our everyday life. Governance is not just state, local, and federal governments passing laws or ordinances and then subjecting offenders to criminal penalties or other sanctions. Governance is the product of an interlocking web of actors, both governmental and "private," that defines how citizens live their lives and the expectations society has regarding any specific field or topic. Thus, the relevant source of authority is not merely formal law. As Christoph von Engel contends, "Most private governance is not legal in nature. Rather, it uses social norms or a technical code."¹²¹ More specifically, Claire Cutler argues that "the privatization of government activities, the deregulation of industries and sectors, increased reliance on market mechanisms in

¹²⁰ Informal private governance is to be distinguished from formal private governance. Thus, for example, the Mafia internal governance operates informally and often via force. See, e.g., Phil Williams, *Transnational Organized Crime and the State*, in *THE EMERGENCE OF PRIVATE AUTHORITY IN GLOBAL GOVERNANCE* 167 (Rodney Bruce Hall & Thomas J. Biersteker eds., 2002) ("The power of criminal organizations is a threat to the state as sovereign entity in that the state claims a monopoly of coercive power; criminal organizations also exercise such power and use violence to remove competitors and obstacles to their businesses."). Formal private governance structures, by contrast, include such bodies as non-governmental organizations and mandatory professional associations such as medical boards. See Rodney Bruce Hall & Thomas J. Biersteker, *The Emergence of Private Authority in the International System*, in *THE EMERGENCE OF PRIVATE AUTHORITY IN GLOBAL GOVERNANCE* 13–16 (Rodney Bruce Hall & Thomas J. Biersteker eds., 2002).

¹²¹ See Engel, *supra* note 100, at 3.

general, and the delegation of regulatory authority to private business associations and agencies are expanding the opportunities for the emergence of private and self-regulatory regimes.”¹²²

As Rodney Bruce Hall and Thomas J. Biersteker explain:

A growing number of actors—actors other than the state—appear to have taken on authoritative roles and functions in the international system. . . . While these new actors are not states, are not state-based, and do not rely exclusively on the actions or explicit support of states in the international arena, they often convey and/or appear to have been accorded some form of legitimate authority. That is, they perform the role of authorship over some important issue or domain. They claim to be, perform as, and are recognized as legitimate by some larger public (that often includes the states themselves) as authors of policies, of practices, of rules, and of norms. They set agendas, they establish boundaries or limits for action. . . . In short, they do many of the things traditionally, and exclusively, associated with the state. They act simultaneously both in the domestic and in the international arenas. What is most significant, however, is that they appear to have been accorded a form of legitimate authority.¹²³

As explained in Part II, the modern notion of governance correctly incorporates an understanding that true governance is not comprised solely of monolithic governmental law;¹²⁴ rather, governance involves a host of actors that define and shape citizens’ behavior, their expectations, and their accepted understandings. Our definition of governance should therefore be expanded to include the multiple actors in the domestic and international arena that have become part of the domestic and international governance regime.

A. *Corporate Interpretation of Privacy Legislation: The Gramm-Leach-Bliley Act*

In Part II of this Article, I noted that Danielsen observed that one of the ways that corporations govern is “through interpretations of or reactions to a legal rule scheme.”¹²⁵ In the realm of information privacy, this is one of the primary ways in which corporations have managed to govern the field.

One example of this phenomenon is corporations’ interpretation of the 1999 Gramm-Leach-Bliley Act (“GLB Act” or the “Act”),

¹²² Cutler, *supra* note 1, at 23.

¹²³ See Hall & Biersteker, *supra* note 120, at 4.

¹²⁴ See Engel, *supra* note 100, at 2 (arguing to “put an end to the idea that government has a monopoly on governance”).

¹²⁵ See *supra*. Part II.B

which, *inter alia*, purports to protect individuals' personal data by requiring companies to disseminate privacy notices. In short, the Act:

allows financial institutions with different branches or affiliates engaging in different services to share the "nonpublic personal information" among each branch of the company. Affiliates must inform customers of the information sharing, but people have no right to stop the companies from sharing it. However, when financial institutions desire to share customer data with third parties, people have a right to opt-out.¹²⁶

Thus, the law purports to legislate the privacy practices of financial companies.

Many commentators on information privacy criticize the Act, maintaining that the Act contains so many loopholes as to virtually eviscerate the effectiveness of the law.¹²⁷ Financial institutions are allowed to share customer data with virtually any third-party company (i.e., non-affiliated companies) as long as they give customers a right to "opt out" of these sharing practices.

Paul Schwartz and Edward Janger summarize the findings of a privacy advocacy group regarding the lack of effectiveness of the GLB Act:

Explanations of how to opt out invariably appear at the end of the notices. Thus, before they learn how to opt out, consumers must trudge through up to ten pages of fine print [M]any passages regarding opt-out . . . are obviously designed to discourage consumers from exercising their rights under the statute. For example, some financial institutions include an opt-out box only in a thicket of misleading statements Other entities attempt to dissuade consumers by implying that consumers may have already opted out or that opting out will accomplish little. A final tactic of the GLB Act privacy notices is to state that consumers who opt-out may fail to receive "valuable offers."¹²⁸

In short, financial institutions' reaction to the GLB Act's opt-out requirement has been an industry-wide effort to make the opt-out right virtually meaningless. Corporations interpret the Act to mean that as long as they give some sort of opt-out right—however, minimal and toothless—to their customers, they fall within the legal parameters of the Act. Hence began the bombardment of customers

¹²⁶ Solove, *supra* note 20, at 63.

¹²⁷ See e.g., Edward Janger & Paul Schwartz, *The Gramm-Leach-Bliley-Act, Information Privacy, and the Limit of Default Rules*, 86 MINN. L. REV. 1219, 1231 (2002); Mark Hochhauser, *Lost in the Fine Print: Readability of Financial Privacy Notices*, July 2001, <http://www.privacyrights.org/ar/GLB-Reading.htm>.

¹²⁸ Janger & Schwartz, *supra* note 127, at 1231 (internal quotations omitted).

with corporate privacy policies containing legalistic terminology, lengthy explanations of the institution's privacy practices, and opt-out provisions that often require the customer to take proactive steps to write to the company at an obscure snail mail address and specify that she wishes to opt out of data sharing.¹²⁹

In other words, the opt-out right is meaningless in practice; the right to opt out of the trafficking of one's personal information is explained in lengthy, legalistic privacy policies that most people throw away as just more junk mail. If the consumer actually bothers to read the policy and recognizes it is of some import, she is likely to be unable to decipher what the company's privacy policies actually are and exactly how she can opt out of their sharing practices.

American corporations' interpretation of the GLB Act has had an effect on the market that resembles the effect of governmental authority. Moreover, the interpretation of the GLB Act by private actors has gone largely unchallenged—indeed, it is accepted as the social norm.

This corporate interpretation of the notice requirement of the GLB Act and its reaction to that requirement has resulted in a governance regime in which consumers' choice regarding sharing of their information with non-affiliated companies has become a virtually meaningless concept. Corporations' interpretation of the Act and their industry-wide reaction to the Act has resulted in a system in which financial institutions can share customers' information without restraint in the absence of some rare opt out from the rare individual who has waded through the muddy waters of a corporate privacy policy and reacted in kind. This systematic practice has an effect on the market similar to the effect of governmental authority; in this arena, corporations "perform the role of authorship"¹³⁰ in the area of privacy practices under the GLB Act. That is, corporations "perform as, and are recognized as legitimate by some larger public (that often includes the states themselves) as authors of policies, of practices, of rules, and of norms"¹³¹ in the realm of financial institutions' privacy practices. In this domain, corporations—not the government—"set agendas [and] establish boundaries or limits for action."¹³²

¹²⁹ See generally, Annie I. Anton, Julia B. Earp, Davide Bolchini, Qingfeng He, Carlos Jensen & William Stufflebeam, *The Lack of Clarity in Financial Privacy Policies and the Need for Standardization*, N.C. STATE U. CSC TECHNICAL REP. #TR-2003-14 (2003), available at http://www.theprivacyplace.com/papers/glb_secPriv_tr.pdf.

¹³⁰ Hall & Biersteker, *supra* note 120, at 4.

¹³¹ *Id.*

¹³² *Id.*

In addition, corporations have, through their interpretation of the GLB Act, adopted industry-wide practices that not only have become the social norm but have also become socially acceptable. As Susan Strange argues, to the extent that non-governmental actors such as corporations and other private companies acquire power and “to the extent their power is not challenged, they are implicitly legitimized as authoritative.”¹³³ But it is not just that corporate power in this domain has gone unchallenged and is therefore implicitly authoritative; it is also that the privacy patterns and privacy practices of financial institutions have infiltrated the society’s consciousness in such a way that these patterns and practices have become expected and are deemed acceptable. This phenomenon reflects the exercise of power described by Steven Lukes as the “third dimension of power”¹³⁴ by which “potential issues are kept out of politics, whether through the operation of social forces and institutional practices or through individuals’ decisions.”¹³⁵ This is also an example of what Harvard economist Andrei Shleifer calls “cognitive persuasion”:¹³⁶ the

¹³³ *Id.* at 6 (summarizing Strange’s argument).

¹³⁴

Luke’s framework traces power in three dimensions: decisional power, agenda power, and manipulative power. The first dimension, decisional power, is the ability to decide the outcome of an issue in conflict. . . . Luke’s second dimension, agenda power, is the ability to determine what issues will and will not be raised for decision. To the extent that A has agenda power over B, A can negate B’s first dimension power to make decisions by foreclosing B’s decision making opportunities. A special aspect of these two dimensions of power is that they function in circumstances of overt conflict.

Unlike decisional and agenda power, third dimension power does not operate in a climate of conflict, but rather prevents circumstances of overt conflict from occurring by creating a manipulated consensus. Manipulative power is the ability to shape the wants and perceptions of another. This power operates primarily through manipulation of information. Third dimension power is the most effective form of power because it insidiously gains the support, or at least the neutrality, of others even to their own detriment. A, by manipulating B’s perceptions, can eviscerate any power that B might have to contribute to the agenda or make decisions.

Moira T. Roberts, Note, *Individual Rights and Government Power in Collision*, 49 WASH. & LEE L. REV. 1023, 1037–38 (1992).

¹³⁵ JOHN GAVENTA, POWER AND POWERLESSNESS: QUIESCENCE AND REBELLION IN THE APPALACHIAN VALLEY 12 (1980). “In a nutshell, Luke’s first dimension is simple, traditional authority; the second dimension is the power to put issues on the agenda; and the third is the power to actually influence or affect public opinion, as the media so often does.” Saru Jayaraman, *Letting the Canary Lead: Power and Participation Among Latino/a Immigration Workers*, 27 N.Y.U. REV. L. & SOC. CHANGE 103, 108 (2001).

¹³⁶ Craig Lambert, *Resisting Temptation: Economics Discovers the Irrational*, HARV. MAG. Mar.–Apr. 2006, at 57 (describing Shleifer’s work).

process by which the persuader (in this case the financial corporation) convinces people of an idea by triggering associations that are consistent with our beliefs and that resonate with our pre-existing ideas. In the case at hand, corporations send detailed “privacy policies” to customers that are in fact anti-privacy policies. Yet the consumer receives a document labeled “Privacy Policy” and, based on rational expectations and ideas about what privacy means (i.e., associations), is persuaded that the policy is indeed about the many ways in which their financial institution vigilantly protects their privacy.

Of course, this private governance could not exist—and might be proven non-authoritative—without the inaction of the government. Congress could, of course, amend the legislation so that customers must opt in to sharing practices rather than opt out. Congress could also amend the legislation such that clear, understandable, and easy opt-out provisions are mandatory. But in the absence of governmental action, corporations’ interpretation and molding of the Act operate as the dominant governing force: “[t]o the extent that regulators . . . acquiesce in or do not react to the standards selected [by corporations], one could reasonably say the . . . rule . . . is established by the decisions of . . . corporate actors.”¹³⁷

B. Corporate Bypassing of Privacy Legislation: The Children’s Online Privacy and Protection Act

The Children’s Online Privacy and Protection Act¹³⁸ (“COPPA” or the “Act”) was passed in 2000 with the purpose of protecting children from the dangers and lures of the Internet by protecting the personal information of children (those under the age of thirteen) online. COPPA aims to do this primarily by requiring parental consent before a commercial website or an online service directed at children¹³⁹ collects, uses, or discloses personal information on a child. The COPPA Rule,¹⁴⁰ which implements COPPA, also requires that websites and online services “[e]stablish and maintain reasonable procedures to protect the confidentiality, security, and integrity of

¹³⁷ Danielsen, *supra* note 94, at 414.

¹³⁸ 15 U.S.C. §§ 6501–08 (2000).

¹³⁹ This includes websites or online services that have knowledge that they collect personal information from children. FEDERAL TRADE COMMISSION ET AL., HOW TO COMPLY WITH THE CHILDREN’S ONLINE PRIVACY PROTECTION RULE 9 (1999), *available at* <http://www.ftc.gov/bcp/online/pubs/buspubs/coppa.pdf>.

¹⁴⁰ Children’s Online Privacy Protection Rule, 16 C.F.R. § 312 (2006).

personal information collected from children.”¹⁴¹ The Act requires that websites subject to COPPA post a privacy policy informing parents of their privacy practices and the contact information for each operator of their website.¹⁴²

How have corporations treated the Act?

First, as Susan Crawford has explained, the Act “has not been a success; many sites have elected simply not to provide interactive services for children under thirteen rather than cope with the exacting oversight and notice requirements of the Act.”¹⁴³

Second, sites that do provide services to children and are clearly subject to the Act have chosen to either ignore the requirements of the Act or, in many cases, comply with COPPA’s facile requirements—such as posting a boilerplate privacy policy¹⁴⁴—while ignoring the more burdensome requirements such as the parental consent and notification mechanisms.¹⁴⁵ For example, in a 2002 FTC study on COPPA compliance, researchers found that only forty-seven percent of children-directed sites had any parental consent and notification mechanisms in place.¹⁴⁶

Third, other sites deflect the issue by requiring online users to simply check a box stating that they are thirteen or older before gaining access to the site.¹⁴⁷

Fourth, in a similar vein, some corporations simply deflect the issue by stating on their website that they don’t sell products or provide services to children or that they do not collect information from chil-

¹⁴¹ See 16 C.F.R. § 312.3(e) (2006).

¹⁴² In addition, entities subject to the Act must allow parents to access any personal information on their child and delete it or opt out of future collection, and such entities must limit their collection of children’s personal information to that which is reasonably necessary to participate in the activity. *Id.*

¹⁴³ Susan P. Crawford, *Shortness of Vision: Regulatory Ambition in the Digital Age*, 74 *FORDHAM L. REV.* 695, 706 n.45 (2005).

¹⁴⁴ As of 2002, ninety percent of child-directed sites posted a privacy policy. Federal Trade Commission Staff Report, *Protecting Children’s Privacy Under COPPA: A Survey on Compliance*, at 5, Apr. 2002, available at <http://www.ftc.gov/os/2002/04/coppasurvey.pdf#search=%22Protecting%20Children's%20Privacy%20Under%20COPPA%3A%20A%20Survey%20on%20Compliance%22>.

¹⁴⁵ Notably, COPPA does not require that privacy policies indicate the methods that parents can use to obtain notice and provide consent. *See id.* at 18.

¹⁴⁶ *See id.* at 12.

¹⁴⁷ *See* Complaint at 6, *United States v. Xanga.com*, No.: 06-CIV-6853 (S.D.N.Y. Sept. 7, 2006), available at http://www.ftc.gov/os/caselist/0623073/xangacomplaint_image.pdf.

dren.¹⁴⁸ For example, Amazon.com's privacy policy states that "Amazon.com does not sell products for purchase by children. We sell children's products for purchase by adults. If you are under 18, you may use Amazon.com only with the involvement of a parent or guardian."¹⁴⁹ Similarly, Target's online privacy policy states that "[w]e do not knowingly collect personally identifiable information from children under the age of 13."¹⁵⁰

Thus, corporations have responded to the Act by either: (1) not providing online services to children; (2) providing online services to children while ignoring the most meaningful yet burdensome COPPA requirements; (3) obtaining "proof" that a person is at least thirteen by merely having the person click a box before proceeding into the site; or (4) simply stating in boilerplate language that they don't provide services to children or collect information from children.

By these methods, corporations intentionally bypass the Act. The first action—actually not providing services to persons under the age of 13—is a form of benign bypassing. However, the other three actions represent something more than rogue corporate behavior; all three examples are a form of corporate governance in the field of information privacy.

As in the case of privacy policies under the GLB Act, corporations' reaction to COPPA has an effect on the market that resembles the effect of governmental authority. The manner in which COPPA actually governs children's online activity is dictated by corporations. Corporations "perform the role of authorship"¹⁵¹ by "perform[ing] as, and . . . [being] recognized as legitimate by some larger public . . . as authors of policies, of practices, of rules, and of norms"¹⁵² in the realm of online companies' privacy practices toward children.

Corporations set the governing standards of COPPA by intentionally bypassing COPPA. The Act is treated by corporations as binding only inasmuch as corporate norms define the actual practices of governing children's online privacy. In this domain, corpora-

¹⁴⁸ Joseph Turow, *Privacy Policies on Children's Websites: Do They Play by the Rules?*, at 12, March 2001, available at <http://www.asc.upenn.edu/usr/jturow/PrivacyReport.pdf#search=%22privacy%20policies%20on%20childrens'%20websites%22>.

¹⁴⁹ Amazon.com Online Privacy Policy, <http://www.amazon.com/exec/obidos/tg/browse/-/468496/104-9748931-2945530#children> (last visited Sept. 11, 2006).

¹⁵⁰ Target.com Online Privacy Policy, http://sites.target.com/site/en/spot/page.jsp?title=privacy_policy (last visited September 11, 2006).

¹⁵¹ Hall & Biersteker, *supra* note 120, at 4.

¹⁵² *Id.*

tions—not the government—have “set agendas [and] establish boundaries or limits for action.”¹⁵³ In such cases, corporations should be “understood as power sources, as part of our governance system rather than objects of it”¹⁵⁴

Unlike the GLB Act, COPPA represents a type of legislation that can be bypassed by mere words rather than conduct. In other words, COPPA is an Act that can be circumvented merely by, in effect, stating “This law does not apply to us” or “By using this website (or clicking an I Agree button), you affirm that you are not a child and thus we are legally protected.” The FTC’s own COPPA Rule encourages this behavior; it states that COPPA “applies to operators of commercial Web sites and online services directed to children under the age of 13 that collect personal information.”¹⁵⁵ For sites such as Amazon.com or Google’s Gmail, the FTC created a loophole, stating that COPPA

applies to general audience Web sites and online services that have *actual knowledge* that they are collecting information from children under the age of 13. The [COPPA] Rule requires that these Web site operators post privacy policies, provide parental notice, and get verifiable consent from a parent or guardian before collecting personal information from children.

Although the [COPPA] Rule doesn’t define the term “*actual knowledge*,” it indicates that a Web site operator is considered to have actual knowledge of a user’s age if the site asks for—and receives—information from the user from which age can be determined. For example, actual knowledge of age exists when an operator learns a child’s age by asking for date of birth on a Web site’s registration page.¹⁵⁶

This “actual knowledge” test is merely a designed loophole. This loophole is unsurprising given the key role major corporations had in the passage and language of COPPA,¹⁵⁷ which allows most sites to

¹⁵³ *Id.*

¹⁵⁴ Greenwood, *supra* note 77, at 44.

¹⁵⁵ Federal Trade Commission, *The Children’s Online Privacy Protection Rule: Not Just for Kids’ Sites*, at 1, February, 2004, available at <http://www.ftc.gov/bcp/online/pubs/alerts/coppabizalrt.pdf>.

¹⁵⁶ *Id.*

¹⁵⁷ See, e.g., *Consumer Internet Privacy: Hearing Before the S. Comm. on Commerce, Sci. & Transp.*, 106th Cong., 2000 WL 1534362 (F.D.C.H.) (2000) (testimony of George Vradenburg, America Online Senior Vice President for Global and Strategic Planning) (stating that “[w]e [at AOL] worked closely with Senator Bryan, Chairman McCain, the FTC, and key industry and public interest groups to help pass and implement the Children’s Online Privacy Protection Act. . . .”).

claim compliance because they don't ask for or receive information by which age can be determined.

The net effect of this corporate reaction to COPPA is that children's personal information is, for the most part, just as unprotected and subject to disclosure to corporations as it was before COPPA was enacted. In short, corporations' reaction to the law has defined and set the parameters of COPPA.

Moreover, corporations' authority in this area is largely unchallenged. Corporations' reactions to the Act have not been sanctioned vigilantly by enforcement actions and crippling penalties. Quite to the contrary, outside of a few COPPA enforcement actions¹⁵⁸ brought by the FTC, the standard and the governing legal regime is that COPPA is merely a harmless piece of legislation that can be completely ignored by utilizing boilerplate language that claims a lack of culpability. Indeed, "[w]hether the state actors and corporate actors are sitting in a room negotiating or dealing through a more informal dance of reciprocal signaling and expectations, it would seem odd to treat the regulatory result as anything other than a joint product."¹⁵⁹

C. *Intentional Violation of Privacy Legislation*

As noted *supra*, "corporations may choose to act in ways that openly and egregiously violate the legislative mandate because governmental deterrence is weak and ineffective."¹⁶⁰ More specifically, when penalties for violating legal rules are unsubstantial, corporations are very much incentivized to openly engage in illegal action.

The FTC is charged with enforcement of federal privacy law. Yet FTC enforcement actions are few and far between, lack effectiveness, and serve little deterrent effect. Because of this, corporations have simply chosen to intentionally violate certain privacy statutes because the benefits of doing so far outweigh the potential downside; in other words, intentional violation of legislation is beneficial because enforcement mechanisms are so weak.¹⁶¹ These intentional violations of privacy laws have engendered a society in which privacy protections are minimal and personal information is aggregated, disseminated,

¹⁵⁸ The FTC's website lists merely eleven enforcement cases under the Children's Online Privacy Protection Act. See Federal Trade Commission, *Children's Privacy*, http://www.ftc.gov/privacy/privacyinitiatives/childrens_enf.html (last visited Sept. 11, 2006).

¹⁵⁹ Daniels, *supra* note 94, at 414.

¹⁶⁰ See *supra* Part II.B.

¹⁶¹ SOLOVE, *supra* note 15, at 72.

and analyzed with impunity.¹⁶² In short, corporations' intentional violation of governmental law is yet another example of corporate governance of information privacy inasmuch as this behavior has an effect on the marketplace similar to governmental regulation and inasmuch as this behavior goes largely unchallenged and is accepted as the social norm.¹⁶³

Specifically, this behavior has gone largely unchallenged by either the public or, more significantly, by the FTC. For example, FTC enforcement actions are sporadic. In the area of credit reporting, for instance, the FTC's website lists a mere five enforcement actions since 1998.¹⁶⁴ The FTC has been most aggressive in pursuing companies for unfair and deceptive trade practices in their privacy practices and policies; the FTC's position is "that the use or dissemination of personal information in a manner contrary to a posted privacy policy is a deceptive practice under the FTC Act, 15 U.S.C. § 45."¹⁶⁵ A sum total of eighteen enforcement actions have been brought in this area under the FTC's enforcement authority under Section Five of the FTC Act.¹⁶⁶

Furthermore, FTC enforcement actions tend to focus on heavy-weight companies that bring in headlines and settlements for the government. Thus, for example, in its few enforcement actions, the FTC has gone after companies such as GeoCities, Equifax, Experian, Hershey Foods, Mrs. Field's, and Quicken Loans.¹⁶⁷ The totality of the FTC's weak enforcement activities reflects an overriding lack of adequate enforcement mechanisms in the area of individual information privacy. Therefore, the majority of companies who engage in

¹⁶² See Chris Jay Hoofnagle, *Big Brother's Little Helpers: How ChoicePoint and Other Commercial Data Brokers Collect and Package Information for Law Enforcement*, 29 N.C. J. INT'L L. & COM. REG. 595 (2004).

¹⁶³ Regulatory law is particularly susceptible to corporate influence. Writing in the nineteenth century, Karl Marx cautioned that the concentration of wealth in corporate hands would subjugate the law to private control. Writing in the early 1960s, Chicago-school free market economists reached the same conclusion, developing what has come to be called the "capture theory" of regulation.

Ostas, *supra* note 110, at 269.

¹⁶⁴ Federal Trade Commission, *Credit Reporting*, http://www.ftc.gov/privacy/privacyinitiatives/credit_enf.html (last visited September 3, 2006).

¹⁶⁵ SOLOVE & ROTENBERG, *supra* note 24, at 541.

¹⁶⁶ See Federal Trade Commission, *Unfairness & Deception*, http://www.ftc.gov/privacy/privacyinitiatives/promises_enf.html (last visited Mar. 4, 2006).

¹⁶⁷ See generally, Federal Trade Commission, <http://www.ftc.gov> (last visited Mar. 4, 2006).

privacy violations suffers no negative consequences and is aware that there is virtually no chance of being punished.

Finally, FTC privacy enforcement actions generally result in little more than a symbolic penalty.¹⁶⁸ Rather than engaging in adjudicative proceedings, the FTC generally signs settlement agreements with companies. Moreover, these settlements represent a mere pittance in comparison to the corporation's coffers. For example, in an early 2006 enforcement action that made national headlines, ChoicePoint was fined fifteen million dollars by the FTC for a leak of private data. Notably, the fine was lauded as the largest fine ever imposed on a company by the FTC for violating a privacy law: "[t]he agency declared that the company falsely assured the public about security precautions while handling personal data carelessly."¹⁶⁹ The agency argued that "the firm sold information to a purported business customer whose own ChoicePoint file identified a link to possible fraud."¹⁷⁰ But fifteen million dollars is small change for ChoicePoint; ChoicePoint currently has a market capitalization of \$3.9 billion and annual revenues of approximately \$1.1 billion.¹⁷¹ Indeed, for ChoicePoint—a company that specializes in data collection, sharing, and profiling—the fine is likely seen merely as the cost of doing business.

This toothless enforcement is typical of government enforcement efforts more generally. A 2006 Associated Press examination revealed that most financial penalties imposed by government agencies remain uncollected:

In many high-profile cases, fines are touted by authorities as proof that they are cracking down. Yet frequently those orders are quietly negotiated to just a fraction of their original amounts—as if drivers, faced with fines for speeding, offered the traffic court judge pennies on the dollar, and the judge agreed.¹⁷²

Worse, government agencies regularly issue fines that even they do not expect to collect. For example, the Department of Energy

¹⁶⁸ See Martha Mendoza & Christopher Sullivan, *Amount of Unpaid Federal Fines Soars*, THE STATE, Mar. 19, 2006, at A15.

¹⁶⁹ Joseph Menn, ChoicePoint Is Fined for Data Breach; It Will Pay \$10 Million for What the FTC Says Was Careless Handling of Consumer Information, L.A. TIMES, Jan. 27, 2006, at C1.

¹⁷⁰ *Id.*

¹⁷¹ ChoicePoint Press Release, *ChoicePoint Revenues Exceed \$1 Billion in 2005*, Jan. 26, 2006, available at <http://www.choicepoint.com/choicepoint/news.nsf/df5fe1c5a497dce38525687e006037f9/2a89e7d31152d32085257101007f8821?OpenDocument>.

¹⁷² Mendoza & Sullivan, *supra* note 168.

regularly issues fines—and coinciding press releases—for penalties that they are not even allowed to collect under federal law.¹⁷³ The Associated Press's conclusion:

The reason [the Department of Energy] issued fines it could not collect was to show what the problems were and how bad A \$1 million fine says something different than a \$10,000 fine.

Financial penalties are regularly touted by agencies and prosecutors as a strict consequence of lawbreaking. The message—that violators can expect to pay dearly—can be misleading.¹⁷⁴

In another example in the information privacy realm, in a recent action against Gateway Learning Corporation,¹⁷⁵ the FTC charged that “after collecting consumers’ information, Gateway Learning changed its privacy policy to allow it to share the information with third parties without notifying consumers or getting their consent.”¹⁷⁶ The settlement in this case was characteristically toothless: “The proposed settlement bars Gateway Learning from making deceptive claims about how it will use consumers’ information and from applying material changes in its privacy policy retroactively, without consumers’ consent. It also requires that the company give up \$4600 it earned from renting the data.”¹⁷⁷

This is just one of many examples in which the settlement amounts are grossly disproportionate to the benefit that the company

¹⁷³

Federal law exempts the national nuclear laboratories from most financial liability, but the Energy Department has issued some \$2.5 million in fines against Los Alamos, Livermore and Argonne national laboratories since 2000. The fines—*issued and waived in the same sentence*—involved 31 different workers who inhaled or touched radioactive or toxic materials.

In 2004, Energy’s National Nuclear Safety Department fined Los Alamos National Laboratory in New Mexico \$770,000 for five separate violations after two workers were exposed to dangerously high levels of plutonium. The violation notices add in parentheses: “Waived by Statute.”

“This is kind of an exercise in absurdity,” said Greg Mello, who heads the Los Alamos Study Group. . . .

Even so, the Energy Department includes the fines in its annual reports to Congress and often announces them in press releases.

Id. (emphasis added).

¹⁷⁴ *Id.* (internal quotations omitted).

¹⁷⁵ Gateway Learning is the company that markets the “Hooked on Phonics” line of products. See Press Release, Federal Trade Commission, *Gateway Learning Settles FTC Privacy Charges*, July 7, 2004) available at <http://www.ftc.gov/opa/2004/07/gateway.htm>.

¹⁷⁶ *Id.*

¹⁷⁷ *Id.* (emphasis added).

at issue received from its use of consumers' personal information and/or to the harm that the consumers at issue suffered. In addition, such small settlement amounts provide no deterrent value. The paradox here is that the FTC's enforcement practices result in little privacy protection for consumers; the "bad acts" of small companies fall under the radar and, therefore, the vast majority of companies can do as they please in regard to privacy.

Thus, large corporate offenders who are most likely to attract the attention of the FTC are not deterred by FTC enforcement actions because even the worst-case scenario—an enforcement action—does not even amount to a thorn in the side of such large entities. This reflects a more general pattern in regard to government fines:

The amount of unpaid federal fines has risen sharply in the last decade. Individuals and corporations regularly avoid large, highly publicized penalties for wrongdoing—sometimes through negotiations, sometimes because companies go bankrupt, sometimes due to officials' failure to keep close track of who owes what under a decentralized collection system.¹⁷⁸

Moreover, these large corporations are the very entities that drive privacy legislation and governmental policy.¹⁷⁹ In sum, "[i]t is . . . clear that the FTC is a paper tiger. A big company with an army of lawyers knows that it can get away with anything, and any FTC action won't hurt in the end."¹⁸⁰

Corporations therefore thwart federal privacy legislation by intentionally violating the laws. This corporate behavior affects the market in ways similar to a governmental law. In the vacuum of strong privacy enforcement, corporations shape a regime in which the federal privacy laws are virtually meaningless, and corporations'

¹⁷⁸ Mendoza & Sullivan, *supra* note 168.

¹⁷⁹ In another enforcement action outside of the privacy realm, the FTC garnered headlines but little more when it went after Experian for unfair or deceptive trade practices. The FTC's charge was that "Experian deceptively marketed free credit reports by not adequately disclosing that consumers would automatically be signed up for a credit report monitoring service costing \$79.95 if they didn't cancel within 30 days." Robert Gellman, *FTC Falls Short, Again*, DM NEWS, Nov. 11, 2005, available at http://dmnews.com/cgi-bin/artprevbot.cgi?article_id=34715&dest=article.

Experian reportedly had 9 million customers paying \$80 a year. That's \$720 million in revenue. Since some of those customers paid for more than one year of service and many are continuing customers, the total revenue probably exceeds \$1 billion. . . . What's the consequence of violating the law? A fine of less than \$1 million, plus refunds. . . . [L]et's say that the fine and refunds total \$25 million. That is a pittance relative to the revenue.

Id.

¹⁸⁰ Gellman, *supra* note 179.

actions have an effect on the market that resembles the effect of governmental authority. As Paul Schiff Berman has observed, “law is almost never ‘delivered’ on the ground in the pure form that treaties, legislation, or constitutional court decisions would indicate. Thus, . . . scholars are in danger of missing how norms actually operate if they over-emphasize the grand statements made at the highest levels of government.”¹⁸¹ The actual legal regime is one in which corporations possess virtually full license to engage in their chosen anti-privacy practices. Rather than complying with government’s law, corporations view privacy violations as the norm and any (unlikely) penalty that may result as merely the cost of doing business.

Finally, as in the first two examples, corporations’ private authority vis-à-vis the FTC has been unchallenged in any meaningful way. Thus, this corporate behavior has become the accepted social norm.

PART IV

IMPLICATIONS OF THE CORPORATE GOVERNANCE PARADIGM

*Actions, reactions, and inactions by all players in the system must be taken into account to get an accurate picture of the regime itself. Under such circumstances, if the decisions of corporate actors are indistinguishable from the decisions of state actors in terms of regulatory and social welfare effects, then treating one as “private activity” and the other as “regulatory” or “governance” activity will likely lead to more than ideological confusion. Such counterfactual characterizations may well result in . . . mistakes in policymaking.*¹⁸²

This Article began by arguing that information privacy jurisprudence is at an impasse and went on to describe the ossified state of domestic information privacy law. The Article then proffered that our information privacy quandaries have not and cannot be solved by working solely within the current jurisprudential paradigm. In other words, our paradigm must take account of the reality that information privacy is not just about governmental laws and enforcement, but is also very much about corporate power and corporate governance.

Problems of information privacy cannot be solved unless their foundations and root causes are exposed and explored, including symbiotic governance by corporations and governmental entities. As Claire Cutler argues, “that which goes unrecognized is difficult to regulate.”¹⁸³

¹⁸¹ Berman, *supra* note 105, at 498.

¹⁸² Danielsens, *supra* note 94, at 415.

¹⁸³ Cutler, *supra* note 1, at 24. Similarly, James Nehf correctly argues that:

How does such an understanding alter our approaches to information privacy law? How can we utilize this new understanding? I offer preliminary thoughts that represent but the beginnings of the possible understanding of the multiple implications of this new paradigm.

A. *Beyond Market-Based and Self-Help Solutions*

The recognition that corporations govern information privacy law and policy represents a new paradigm. This paradigm is a shift from the traditional notion that information privacy law is merely the province of the government. This new paradigm is also a move away from the limited notion that solutions must focus on one of two forces: governmental law or the market. Rather, there is a third, powerful force that has heretofore gone unrecognized in the literature: governance by corporations. Folding this third force into the conceptual model of the dynamics of information privacy law and policy mandates a rethinking of possible and practical solutions.¹⁸⁴

Significantly, this recognition weakens the argument that the market should provide the proper compass for determining whether information privacy practices are sound.¹⁸⁵ Market dynamics and industry self-regulation¹⁸⁶ cannot be relied upon as correct barometers of public opinion or correct action when the market itself is dominated by the very actors that shape the law and govern the industry practices.

Arguments for approaching problems of information privacy with market-based solutions reflect the belief that informational pri-

Since there are benefits and risks associated with information collection and data sharing, policy makers must attempt to strike a balance. In doing so, they must first define the problem. This is a critical step in the formulation of public policy because the way in which a problem is defined on the public agenda will affect its ultimate resolution.

Nehf, *supra* note 2, at 5.

¹⁸⁴ Thus, for example, the importance of focusing on strengthening the lackluster enforcement efforts of the FTC pales when armed with the knowledge that FTC enforcement is but a piece of the puzzle.

¹⁸⁵ “[G]overnment actors insist that self-regulation is the American way, and [that] it is enough.” Litman, *supra* note 12, at 1287.

¹⁸⁶ Perhaps the most direct corporate influence on legal norms arises in the area of self-regulation. Advertising law provides an illustration. The Federal Trade Commission is officially charged with regulating false advertising, yet most advertising disputes are subject to industry self-regulation. It is largely left to the industry itself to set its own standards.

Ostas, *supra* note 110, at 271.

vacancy is merely a personal concern. As James Nehf has observed, information privacy has traditionally been viewed as “an individual concern rather than a general societal value or a public interest problem.”¹⁸⁷ Specifically, he argues that¹⁸⁸ “[t]his [definition of information privacy as an individual concern] has influenced the resulting public policy solutions, yet it may not be the most effective way to approach modern privacy concerns.”¹⁸⁹ Thus, solutions have tended toward individual, private, and market-based solutions.¹⁹⁰ “In contrast, when a problem is viewed as a general societal concern, and a resolution in the public interest is sought, enforcement of the legal norm is primarily through government agency oversight and regulation.”¹⁹¹

Our understanding of privacy as a private concern rather than a public concern must shift once we acknowledge that corporate governance is a force which needs to be held in check by the government. In this respect, information privacy can be seen for what it is: a public value on the most fundamental level. “If no change [in the political and legal rhetoric] occurs, we can expect to see more laws enacted periodically that purport to address privacy concerns in particular sectors, but individuals will still be expected to shoulder the burden of monitoring their own information, and market-based solutions will predominate.”¹⁹²

This view of information privacy as a personal problem rather than a public one is merely a social understanding that has engendered parallel social norms. Those entities that have a vested interest in propagating a theory of information privacy as individual and pri-

¹⁸⁷ Nehf, *supra* note 2, at 5.

¹⁸⁸ James Nehf explains the underpinnings of the viewpoint that privacy is an individual issue rather than a larger social issue:

Protecting information privacy threatened defined and influential stakeholders—government agencies, employers, marketing firms, law enforcement—all of whom were just beginning to see the advantages of information technologies. All had an interest in collecting and sharing as much information as possible. Each of these stakeholders thus had incentives to redefine the issue from the ideal of privacy as a foundational societal value to some lesser ideal that required the balancing of other societal concerns—efficiency, productivity, crime control, etc.—against the individual harms that might be caused by data collection and sharing.

Nehf, *supra* note 2, at 47 (emphasis added).

¹⁸⁹ *Id.* at 5.

¹⁹⁰ *See id.*

¹⁹¹ *Id.* at 5.

¹⁹² *Id.* at 91.

vate rather than public also have an interest in molding this theory into a widespread social norm.

If information privacy is instead viewed as a public value, and the symbiotic relationship between public governance and private governance is acknowledged, then practical solutions to problems of information privacy begin to emerge. If government and corporate actors work in symbiotic relationships to form the legal regime under which we live, then reform efforts must focus on all of the actors that are the primary power centers shaping the reigning legal regime of privacy.

In short, understanding that corporations govern the information privacy regime is of profound importance because the privacy of personal information is not “just another consumer issue,” nor is it one that ought to be solved by the individual or the market.

B. Corporate Governance and the Fallacy of Choice

Privacy scholars have noted that the concept that consumers have a “choice” about privacy is misguided¹⁹³ because if there is any choice, it is a Hobson’s choice: “an apparently free choice when there is no real alternative; the necessity of accepting one of two or more equally objectionable alternatives.”¹⁹⁴ This point is even more salient once the private governance paradigm is conceded. In regard to personal “choice” in information privacy:¹⁹⁵

¹⁹³ Moreover, on the consumer front, this privacy problem presents the ubiquitous problem of lack of choice. As Julie Cohen argues,

the rhetoric of “choice” obfuscates the political choice that current data privacy policy represents. The data privacy debate is not merely, or even mostly, about the satisfaction of consumer preferences as expressed in the direct market for goods and services. Like the rhetoric of “transaction costs,” the emphasis on “choice” conceals the degree to which the model predetermines who chooses. In particular, with respect to secondary uses of personally-identified data, the “choice” that the model protects is not choice by individuals. It is the choice of data processors about how to classify individuals, and for what purposes.

Cohen, *supra* note 40, at 1399.

¹⁹⁴ M-W.com dictionary definition, <http://www.m-w.com/dictionary/hobson's> (last visited September 7, 2006).

¹⁹⁵

Consumers are faced with the Hobson’s choice of surrendering their private information, being unable to participate in large segments of the commercial economy or to lie.

Now, there are three ways of approaching this problem. First, one may stridently protest and walk out the door. Second, one may approach the sales clerk and decline to provide the information risking delay or that the transaction will not occur. Third, one could tell a white-lie. . . .

legal consciousness regarding contracts is likely to contain much of the same multivocality that characterizes legal consciousness on other kindred topics. When, in order to purchase a needed product, the consumer must accept the retailer's standard-form contract, the symbolism may evoke hierarchy and oppression more than it evokes mutualism, voluntarism, or equality. Or, more likely, it may evoke both at once, leaving the consumer with a Hobson's choice between a narrative of disempowerment ("I had no say in the matter") and a narrative of self-blame ("I brought it on myself").¹⁹⁶

In other words, consumers can either consent to a company's privacy policy or not do business with that particular company at all; either action represents consumer powerlessness.¹⁹⁷ In fact, privacy policies among industries are generally significantly similar—hence, the realistic "choice" of the consumer is often to consent to a privacy policy or not do business with an entire *industry* at all. This Hobson's choice, in fact, amounts to coercion. We cannot live in the modern world and refrain from consenting to the ubiquitous, company-biased privacy policies and stances. As Paul Schwartz has noted, this is an "autonomy trap."¹⁹⁸

True contractual consent requires meaningful choice. For example, there often exists no meaningful choice on the part of the shopping consumer, as the marketplace is filled with industry leaders who have a firm stranglehold on the industry and who have adopted virtually the same pro-business privacy policies. Thus, the American world of contracts is one in which consent is meaningless and "agreements" are but a farce. When corporate actors shape the rules (in confluence with the government) in such a way that the rules not only heavily favor those corporate actors but also leave consumers with an extremely limited set of choices, the notion that individuals truly "consent" to corporate privacy practices becomes farcical.

The phrase "knowledge is power" is almost a truism, as is the claim that power resides in the hands of those who control the information. But this truism has real meaning in our twenty-first cen-

Llewellyn Joseph Gibbons, *It's Nobody's Business, But You Still Cannot Lie About It: Criminalizing Innocent Attempts to Maintain Cyber-Privacy*, 30 OHIO N.U. L. REV. 377, 378 (2004).

¹⁹⁶ Mark Suchman, *The Contract as Social Artifact*, 37 LAW & SOC'Y REV. 91, 112 n.27 (2003).

¹⁹⁷ Larry Magid, *It Pays to Read License Agreements*, <http://www.pcpitstop.com/spycheck/eula.asp> (last visited Sept. 8, 2006) (discussing lack of choice in end-user license agreements).

¹⁹⁸ Paul M. Schwartz, *Internet Privacy and the State*, 32 CONN. L. REV. 815, 825 (2000).

tury society. Understood at its base level, consumers' "free will" is at the behest of corporate decision-making. In short, the ceding of our personal information to corporations has engendered a society that is controlled by corporations. This realization is of profound significance because we cannot solve the problems of domestic information privacy unless we address this underlying power dynamic.

Moreover, corporate governance has an effect on social norms. When corporate governance is part of the legal regime, consumer apathy¹⁹⁹ regarding their lack of information privacy becomes less surprising. Outside of the problem of identity theft, the vast majority of consumers seem disinterested in privacy violations. Even more seriously, as discussed *supra*, many legal scholars treat the problem as one that merits attention but is obviously less "important" than matters of human rights or environmental law. This phenomenon is not insignificant. When both laypersons and legal scholars dismiss a social problem as trivial or, at the most, important but less deserving of attention than "real" social justice issues, that problem becomes relegated to the backwaters of social and legal thought. In turn, the social problem is virtually ignored by policymakers and the government. Yet consumer attitudes are shaped and guided not only by the government and the mass media, but also by private actors such as corporations via shared governance of information privacy law.

C. *Bringing the Individual Back into Information Privacy*

The stripping away of political façade, legitimization, and hidden sources of power is necessary to bring individual citizens' concerns to the forefront. While it may be true that we are living in a time of rapid transition from governmental authority to symbiotic governance both domestically and globally, this does not force the

¹⁹⁹ One commentator has observed that:

[C]onsumers are not as concerned about financial privacy as surveys suggest. A June 2001 study found that many survey questions "distort or manipulate" the answers. The study went on to note that surveys "cannot effectively replicate the choices that consumers make in the real world, where they must choose among competing desires and where nothing comes for free." The authors of the survey also point out that consumers are continuing to shop online in record numbers despite early forecasts that privacy concerns would keep them away. The study notes that other surveys show that when people are asked to name their top concerns without being given a list of possible responses, privacy is not listed as one of their top concerns. The authors of the study also indicate that consumers may not always report their actual behavior accurately.

Eric Poggemiller, Note, *The Consumer Response to Privacy Provisions in Gramm-Leach-Bliley: Much Ado About Nothing?*, 6 N.C. BANKING INST. 617, 633-34 (2002).

conclusion that individuals must simply accept this fact and consent to being governed by private actors without democratic accountability.

Rather, the recognition that private governance is occurring in the field of information privacy is a powerful one that can unlock a vault of realistic solutions to seemingly intractable problems.

For instance, the understanding that the illusion of “choice” in privacy negotiations is merely a Hobson’s choice constructed by governing corporations undermines arguments for industry self-regulation and menu-based privacy options between consumers and corporations. Such “true” contractual arrangements are unlikely to exist between powerful corporations that govern consumer “privacy” contracts and relatively powerless consumers.

Similarly, calls for robust privacy legislation appear quixotic when viewed through the lens of corporate governance of information privacy. This is also true of arguments for more robust and frequent FTC enforcement actions because the state is complicit—whether through action or inaction—in governance by corporations. Indeed, “in its manifestation as market authority, private authority transforms both the state and state sovereignty. However, the state participates in this transformation.”²⁰⁰ Once we understand and accept that information privacy is governed not just by our federal, state, and local governments, but also by corporations, our legal and policy strategies should be rethought.

Clearly, the “enforcement” model of protecting information privacy is woefully inadequate. The FTC should be understood as merely a weak enforcement mechanism that ultimately operates in the interest of corporations. As argued *supra*, with few exceptions, even the few FTC settlement actions that are brought to closure do not involve the individuals whose privacy has been violated, nor do the individuals share in the spoils of the settlement funds.

Individuals must be brought back into the privacy picture.²⁰¹ Looking to the market or to governmental agencies to enforce pri-

²⁰⁰ Thomas J. Biersteker & Rodney Bruce Hall, *Private Authority as Global Governance*, in *THE EMERGENCE OF PRIVATE AUTHORITY IN GLOBAL GOVERNANCE* 203, 209 (Rodney Bruce Hall & Thomas J. Biersteker eds., 2002).

²⁰¹ One commentator argues that:
the federal courts, and the Supreme Court in particular, have bestowed the equivalent of human rights on these artificial entities. They now have the protection of law and the Constitution, which means the protection of the police and the military, to interfere in our elections and in our lawmaking. . . . They’re able to field fifty or a thousand lobbyists. . . . What’s happened is, we’ve been channeled into regulatory

vacy rights is a largely futile effort likely to produce few victories. The privacy problem is fundamentally one wherein the players are corporations and government, and individuals are distant spectators equipped with foggy, distorting binoculars.

Significantly, this lockout of consumers from their own information privacy matters²⁰² has been accomplished via a steering of such matters away from the judicial system and into legislative and regulatory backwaters. A pessimist might argue that calls for common law remedies to privacy wrongs—based in tort, property, and contract law—are unlikely to succeed when the status quo is governed by the very entities that have a stake in minimizing our personal information privacy. But the jurisprudential glass is actually half full. Exposing the underlying power structures that dictate privacy practices and leave the individual out of the equation almost entirely might well cause a rethinking of possible common law solutions.

For example, many privacy wrongs arise out of the farce of privacy policies. Consumers “agree” to what are, in fact, anti-privacy policies, and are forced to live with that “agreement” because they consented. Yet once it is understood that there is no true “choice” or “consent” taking place on the part of the consumer due to corporate power and governance by corporations, the underutilized defense that such “agreements” are in fact unconscionable becomes a meaningful possibility. The seminal unconscionability case of *Williams v. Walker-Thomas Furniture Co.*²⁰³ was decided in a context of one retailer wielding significant power over a neighborhood of consumers with few options. Yet *Williams v. Walker Furniture Co.* could serve as the small-scale model for a more sophisticated case against corporations and forced privacy agreements on a wide-scale basis. Douglas Baird

administrative agencies, like the Federal Communications Commission, the Environmental Protection Agency, the Securities Exchange Commission and the National Labor Relations Board, where we try to make the best of the worst of a bad situation. . . .

David Barsamian, *Challenging Corporate Power: An Interview with Richard Grossman*, Z MAG., Jan. 2000, available at <http://www.thirdworldtraveler.com/Corporations/ChallengingCorpPower.html>.

²⁰² For example, consumers generally receive no part of any FTC monetary settlement. In the few cases in which they have received some redress, it has been paltry at best and grossly disproportionate to the harm consumers may have suffered because of the privacy violation. As one commentator has noted, “[t]oo often, the FTC’s principal interest is in being able to pat itself on the back through a trophy press release. The commission rarely seeks to obtain recovery for consumers.” Gellman, *supra* note 179.

²⁰³ 350 F.2d 445 (D.C. Cir. 1965).

argues that such boilerplate agreements between companies and consumers often reflect a deeper, profound social problem:

When boilerplate appears troublesome, some other mischief is often afoot. Boilerplate, while not a vice itself, is frequently the symptom of a problem that the law should appropriately address [T]roublesome boilerplate can emerge from anticompetitive behavior. Legal intervention, however, must aim at the underlying anticompetitive conduct itself, not the boilerplate.²⁰⁴

Although I do not agree with Baird's assertion that boilerplate contracts should not be analyzed under the doctrine of adhesion, but rather under some underlying "bad actor" conduct, I do agree that boilerplate "privacy" agreements reflect an underlying power imbalance that is troublesome and should be accounted for when deciding the legal validity of a contract.

On the property front, some proponents of individuals' informational privacy have argued that personal information should be deemed as property of the individual. This argument has, to date, been unsuccessful. Yet judicial attitudes toward information privacy might be swayed if the information privacy problem were understood as one engendered by the power imbalance between corporations and individuals. In other words, if corporations govern information privacy and individuals' personal data is considered to be public, the question of the role of power and powerlessness in property struggles comes into play. As K.J. Greene notes:

When we think of private property, we think of three characteristics: the right to exclude others, title (ownership), and the right to collect income or rent off the property It has been noted that: intellectual property law can ameliorate but not eliminate underlying disparities in bargaining power [and accordingly] economic need might induce [a person] to part with control over her [private property], and even give up liberty to use it, perhaps in return for fairly small rewards.²⁰⁵

Thus, the dismissal of the "personal information as property" argument is significantly weakened when confronted with the reality of appropriation of personal property by the dominant entities that govern the information privacy landscape.

These two examples represent possible means of reviving common law theories by exposing the underlying power structures at work in information privacy law and enforcement. The notion of

²⁰⁴ Douglas G. Baird, *The Boilerplate Puzzle*, 104 MICH. L. REV. 933, 934 (2006).

²⁰⁵ K.J. Greene, *Copyright, Culture & Black Music: A Legacy of Unequal Protection*, 21 HASTINGS COMM. & ENT. L.J. 339, 375-76 (1999).

2006]

INFORMATION PRIVACY

169

governance by corporations is one that can and should engender a myriad of imaginative resistance models—whether via the judiciary or other, less traditional mechanisms.

CONCLUSION

The democratic implications of corporate governance are profound. As one scholar notes:

[A]s firms begin to function like governments, this raises major issues for democratic and representative theories of governance [P]rivate entities are not normatively entitled to act authoritatively for the public, because they are not subject to mechanisms of political accountability, but rather are only subject to the accountability of their private members.²⁰⁶

Although an examination of the implications for democracy posed by corporate governance is beyond the scope of this Article, it is crucial to begin to raise questions regarding democracy, accountability, and legitimacy in the realm of information privacy. And the antecedent requirement of such questioning is to expose governance by corporations in this and other fields, for wrongs that are rooted in invisible systems of authority cannot be remedied.

²⁰⁶ Biersteker & Hall, *supra* note 200, at 211.