Journal of Criminal Law and Criminology

Volume 103 | Issue 3 Article 2

Summer 2013

Privacy Versus Security

Derek E. Bambauer

0091-4169/13/10303-0667
THE JOURNAL OF CRIMINAL LAW & CRIMINOLOGY Vol. 103, No. 3

Printed in U.S.A.

PRIVACY VERSUS SECURITY

DEREK E. BAMBAUER*

Legal scholarship tends to conflate privacy and security. However, security and privacy can, and should, be treated as distinct concerns. Privacy discourse involves difficult normative decisions about competing claims to legitimate access to, use of, and alteration of information. It is about selecting among different philosophies and choosing how various rights and entitlements ought to be ordered. Security implements those choices—it mediates between information and privacy selections. This Article argues that separating privacy from security has important practical consequences. Security failings should be penalized more readily and more heavily than privacy ones, both because there are no competing moral claims to resolve and because security flaws make all parties worse off. Currently, security flaws are penalized too rarely, and privacy ones too readily. The Article closes with a set of policy questions highlighted by the privacy-versus-security distinction that deserve further research.

I. PRIVACY VERSUS SECURITY

Acxiom is one of the world's foremost data mining companies. The company's databases contain information on over half a billion consumers, with an average of 1,500 transactions or data points per consumer.[1] It processes one billion such records each day.[2] Each consumer receives a unique numeric identifier, allowing Acxiom to track and classify them by location, credit card usage history, and even interests.[3] Acxiom earns over a billion dollars annually by selling this data to companies that want to

* Associate Professor of Law, University of Arizona James E. Rogers College of Law. Thanks for helpful suggestions and discussion are owed to Jane Bambauer, Danielle Citron, Dan Hunter, Margo Kaplan, Thinh Nguyen, Paul Ohm, and Tal Zarsky. The author welcomes comments at: derekbambauer@email.arizona.edu.

[1] Natasha Singer, *You for Sale: A Data Giant Is Mapping, and Sharing, the Consumer Genome*, N.Y. TIMES, June 17, 2012, at B1.

[2] Richard Behar, *Never Heard of Acxiom? Chances Are It's Heard of You*, FORTUNE, Feb. 23, 2004, at 140.

[3] *Id.* at 144.

market their wares more effectively.[4] If Big Data has an epicenter, it is likely located in Conway, Arkansas, where Acxiom's server farm can be found.[5]

Even giants make mistakes. In February 2003, Acxiom provided a defense contractor with the Social Security numbers of passengers who flew on JetBlue flights.[6] The contractor used one of those Social Security numbers in a PowerPoint presentation, and that passenger's information quickly became public.[7] The disclosure led to intense criticism of the company and to a complaint to the Federal Trade Commission.[8]

And, in 2002 and 2003, hackers penetrated Acxiom's computers, accessing records on millions of American consumers. Acxiom failed to detect the breaches; rather, the attacks were noticed first by local law enforcement and then by the Federal Bureau of Investigation (FBI).[9] Indeed, in the 2003 case, Acxiom had no idea its systems had been compromised until a Cincinnati sheriff turned up compact discs filled with the company's records while searching the home of a systems administrator for a marketing firm.[10] It was only while the FBI was investigating the case that agents stumbled upon a second group of hackers who had broken into Acxiom's server three times the prior year.[11] The Cincinnati systems administrator captured the sensitive data while it was being transferred via File Transfer Protocol (FTP), without encryption, from a server outside Acxiom's firewall—the equivalent, in security terms, of writing it on a postcard sent through regular mail.[12]

Thus, Acxiom exposed sensitive consumer data three times—once through a deliberate choice and twice through incompetence. Privacy advocates were outraged in each instance. This Article argues, though, that these cases—the disclosure, and the hacks—should be treated differently. The disclosure is a privacy problem, and the hacks are a security problem. While legal scholars tend to conflate privacy and security, they are distinct

---

[4] *Id.* at 140.

[5] Singer, *supra* note 1, at B1.

[6] *See* Behar, *supra* note 2, at 140.

[7] *Id.* at 146.

[8] Marilyn Adams & Dan Reed, *Passengers Sue JetBlue for Sharing Their Data*, USA TODAY, Sept. 24, 2003, at 3B.

[9] Behar, *supra* note 2, at 142; Linda Rosencrance, *Acxiom Database Hacked: Sensitive Information Was Downloaded but Apparently Not Distributed*, COMPUTERWORLD (Aug. 8, 2003, 12:00 PM), http://www.computerworld.com/s/article/83854/Acxiom_database_hacked.

[10] Behar, *supra* note 2, at 140.

[11] *Id.* at 142.

[12] *Id.* at 148; Rosencrance, *supra* note 9.

concerns. Privacy establishes a normative framework for deciding who should legitimately have the capability to access and alter information. Security implements those choices. A counterintuitive consequence of this distinction is that law should punish security failures more readily and harshly than privacy ones. Incompetence is worse than malice.

Security, in contrast to privacy, is the set of technological mechanisms (including, at times, physical ones) that mediates requests for access or control.[13] If someone wants access to your online banking site, he needs your username, password, and personal identification number (your credentials).[14] The security of your online banking is determined by the software on the bank's server and by who knows your credentials. If someone wants access to your paper health records, they need physical access to your physician's file room. The security of your health records is determined by the physical configuration of the office and by who holds a copy of the key to it. As a privacy matter, you might want only your doctor and her medical staff to have access to your records. As a security matter, the office's cleaning staff might have a key that lets them into the file room.[15]

The differences between privacy and security matter. Security defines which privacy choices can be implemented. For example, if your entire electronic medical record is secured by a single mechanism (such as a password), it is not possible to enforce selective access, so that your dermatologist can see information about your sunscreen use but not about your antidepressant use. And privacy dictates how security's options should be implemented, the circumstances under which they are appropriate, and the directions in which they ought to develop.

Distinguishing between privacy and security is unusual in legal scholarship. Most academics and advocates treat the two concerns as interchangeable or as inextricably intertwined. Jon Mills, for example, treats encryption and authentication—classic security technologies—as methods of protecting privacy.[16] For Mills, any "disclosure without consent

---

[13] Leslie P. Francis & John G. Francis, *Informatics and Public-Health Surveillance*, *in* BIOINFORMATICS LAW: LEGAL ISSUES FOR COMPUTATIONAL BIOLOGY IN THE POST-GENOME ERA 191 (Jorge L. Contreras & Jamie Cuticchia eds., 2013) ("'[S]ecurity' [refers] to means for assuring adherence to specified data protections.").

[14] *See generally* Patco Constr. Co., Inc. v. People's United Bank, 684 F.3d 197 (1st Cir. 2012) (reversing summary judgment for defendant bank, which approved suspicious, fraudulent transfers after attackers correctly supplied customers' credentials).

[15] *See, e.g.*, Molly Hennessy-Fiske, *Jackson Files Said Breached*, L.A. TIMES, June 11, 2010, at AA1; Chris Dimick, *Reports Pour in Under CA's New Privacy Laws*, J. AHIMA (July 7, 2009, 1:40 PM), http://journal.ahima.org/2009/07/07/cas-new-privacy-laws.

[16] JON L. MILLS, PRIVACY: THE LOST RIGHT 301–02 (2008).

gives rise to privacy concerns."[17] Similarly, Viktor Mayer-Schönberger takes up the possibilities of digital rights management (DRM) technology as a privacy solution.[18] Mayer-Schönberger contemplates using the locks and keys of DRM as a mechanism to implement restrictions on who can access personal information.[19] Yet the difficulties he rightly recognizes in his proposal, such as comprehensiveness, resistance to circumvention, and granularity, are those of security, not privacy.[20] DRM is not privacy at all: it is security. Placing it in the wrong category causes nearly insurmountable conceptual difficulties. In assessing privacy protections on social networking services, such as Facebook and Orkut, Ruben Rodrigues focuses on privacy controls (which enable users to limit access to information), and distinguishes data security mechanisms (which protect users from inadvertent breaches or deliberate hacks).[21] Yet both, in fact, are aspects of security, not privacy. Here, too, the wrong classification creates problems. Rodrigues grapples with problems of access by third-party programs, which could be malware or a competitor's migration tool; user practices of sharing login information; and authentication standards.[22] Each issue is made clearer when realigned as a security matter.

While some privacy scholarship has recognized the privacy–security distinction rather murkily, it has not yet been explored rigorously or systematically. For example, Charles Sykes treats cryptography as conferring privacy, but then later quotes cypherpunk Eric Hughes, who writes, "Privacy in an open society requires cryptography. If I say something, I want it heard only by those for whom I intend it."[23] This correctly recognizes that privacy and security (as implemented through cryptography) are different, though complementary. Ira Rubenstein,

---

[17] *Id.* at 58.

[18] VIKTOR MAYER-SCHÖNBERGER, DELETE: THE VIRTUE OF FORGETTING IN THE DIGITAL AGE 144–54 (2009). Digital rights management systems manage what actions a user can take with digital information (e.g., whether she can open, copy, or print material), such as an e-book. *See generally Digital Rights Management (DRM) & Libraries*, AM. LIBR. ASS'N, http://www.ala.org/advocacy/copyright/digitalrights (last visited Mar. 16, 2013) (explaining DRM).

[19] MAYER-SCHÖNBERGER, *supra* note 18, at 144–54.

[20] *Id.* at 148–54.

[21] Ruben Rodrigues, *Privacy on Social Networks: Norms, Markets, and Natural Monopoly*, *in* THE OFFENSIVE INTERNET: SPEECH, PRIVACY, AND REPUTATION 237, 242 (Saul Levmore & Martha C. Nussbaum eds., 2010).

[22] *Id.* at 248–54.

[23] CHARLES J. SYKES, THE END OF PRIVACY 167–69 & n.* (1999). Cypherpunks advocate the use of technological self-help, such as through encryption, as a check on government and corporate power. *See, e.g.*, Eric Hughes, A Cypherpunk's Manifesto (Mar. 9, 1993) (unpublished manuscript), *available at* http://w2.eff.org/Privacy/Crypto/Crypto_misc/cypherpunk.manifesto.

Ronald Lee, and Paul Schwartz seem implicitly to understand the distinction, though they do not leverage it, in their analysis of privacy-enhancing technologies.[24] Thus, in assessing why users have not embraced anonymization tools, they concentrate principally on security risks, such as the possibility of attacks against these tools or of drawing attention from government surveillance. Peter Swire and Lauren Steinfeld formally treat security and privacy separately, but conflate the roles of the two concepts.[25] For example, Swire and Steinfeld discuss the Health Insurance Portability and Accountability Act's (HIPAA) Privacy Rule but lump in security considerations.[26] And Paul Schwartz and Ted Janger see analogous functioning by information privacy norms, which "insulate personal data from different kinds of observation by different parties."[27] That is exactly what security does, but unlike norms, security restrictions have real bite. Norms can be violated; security must be hacked. Rudeness is far easier to accomplish than decryption.

The one privacy scholar who comes closest to recognizing the distinction between security and privacy is Daniel Solove. In his article on identity theft, Solove analyzes the interaction (along the lines of work by Joel Reidenberg[28] and Larry Lessig[29] exploring how code can operate as law) between architecture and privacy.[30] Solove's view of architecture is a holistic one, incorporating analysis of physical architecture, code, communications media, information flow, and law. Solove assesses the way architecture shapes privacy. This is similar to, but distinct from, this Article's argument, which is that security implements privacy. Moreover, the security concept is less holistic: it assesses precautions against a determined attacker, one unlikely to be swayed by social norms or even the

---

[24] Ira S. Rubinstein et al., *Data Mining and Internet Profiling: Emerging Regulatory and Technological Approaches*, 75 U. CHI. L. REV. 261, 276–80 (2008) (discussing why users have not embraced privacy-protecting technologies such as anonymizers and pseudonyms).

[25] Peter P. Swire & Lauren B. Steinfeld, *Security and Privacy After September 11: The Health Care Example*, 86 MINN. L. REV. 1515, 1522 (2002) ("Both privacy and security share a complementary goal—stopping unauthorized access, use, and disclosure of personal information."). Security's goal is stopping unauthorized access. Privacy's goal is to define what is treated as "unauthorized."

[26] *Id.* at 1524–25.

[27] Edward J. Janger & Paul M. Schwartz, *The Gramm-Leach-Bliley Act, Information Privacy, and the Limits of Default Rules*, 86 MINN. L. REV. 1219, 1251–52 (2002).

[28] Joel R. Reidenberg, *Lex Informatica: The Formulation of Information Policy Rules Through Technology*, 76 TEX. L. REV. 553, 568–76 (1998).

[29] Lawrence Lessig, *The New Chicago School*, 27 J. LEGAL STUD. 661, 662–65 (1998).

[30] Daniel J. Solove, *Identity Theft, Privacy, and the Architecture of Vulnerability*, 54 HASTINGS L.J. 1227, 1238–43 (2003).

threat of ex post punishment.[31]

Finally, Helen Nissenbaum's recent work is instructive about the differences between these two concepts, although it is not a distinction she draws directly. She argues that standard theories of privacy devolve, both descriptively and normatively, into focusing upon either constraints upon access to, or forms of control over, personal information.[32] This encapsulation points out the problems inherent in failing to recognize how privacy differs from security. An individual may put forth a set of claims about who should be able to access her personal information or what level of control she should have over it.[33] Those claims describe a desired end state—the world as she wants it to be regarding privacy. However, those claims are unrelated to who can access her personal information or what level of control she has over it at present. More important, those normative claims are unrelated to overall access and control, not only now, but into the future, and perhaps in the past. A given state of privacy may be desirable even if it is not achievable.

This Article next explores how privacy involves making normative choices.

II. PRIVACY

At base, privacy issues are arguments about values. Privacy debates are some of the most contentious in information law. Scholars and courts disagree about virtually everything: the theoretical bases and contours of privacy rights;[34] the relative merits of free-expression rights versus privacy;[35] the risks posed by de-identified data;[36] the virtues of a "right to

---

[31] *See, e.g.*, Ebenezer A. Oladimeji et al., Security Threat Modeling and Analysis: A Goal-Oriented Approach 1, 4–5 (Nov. 13–15, 2006) (paper presented at the 10th IASTED International Conference on Software Engineering and Applications).

[32] HELEN NISSENBAUM, PRIVACY IN CONTEXT: TECHNOLOGY, POLICY, AND THE INTEGRITY OF SOCIAL LIFE 69–71 (2010).

[33] *Id.*

[34] *See, e.g.*, AMITAI ETZIONI, THE LIMITS OF PRIVACY (1999); DANIEL J. SOLOVE, UNDERSTANDING PRIVACY (2008); ALAN F. WESTIN, PRIVACY AND FREEDOM (1967); Richard A. Posner, *The Economics of Privacy*, 71 AM. ECON. REV. 405 (1981).

[35] *See, e.g.*, Sorrell v. IMS Health Inc., 131 S. Ct. 2653, 2672 (2011) (striking down a Vermont statute forbidding drug detailers from obtaining prescription data); Snyder v. Phelps, 131 S. Ct. 1207, 1220 (2011) (rejecting tort liability for infliction of emotional distress for protests at a military funeral).

[36] *Compare* Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. REV. 1701 (2010) (critiquing release of de-identified data as risky), *with* Jane Yakowitz, *Tragedy of the Data Commons*, 25 HARV. J.L. & TECH. 1 (2011) (criticizing Ohm's analysis and lauding the benefits of de-identified data).

be forgotten";[37] and the benefits of ad-supported media versus Internet users' interests in not being tracked online.[38] What makes these debates so important, and heated, is that they embody a clash between values and policies that have legitimate claims for our attention.[39]

The answers to those arguments can rarely be resolved empirically; rather, they depend upon one's prior normative commitments. Privacy, as scholars such as Daniel Solove,[40] Danielle Citron,[41] Anita Allen,[42] and Helen Nissenbaum[43] remind us, is no longer about a binary division between data revealed and data concealed. It is about competing claims to information. Put crudely, privacy theory supplies an account of who should be permitted to access, use, and alter data, and why those particular actors should be viewed as having legitimate entitlements thereto.

Privacy is about power.[44] It is about how law allocates power over information. Consider one's banking habits. Federal banking regulations (implemented pursuant to the Gramm–Leach–Bliley Act) require that firms safeguard consumers' data[45] and that they provide those consumers with annual descriptions of their privacy practices related to that data.[46] The mandates are geared almost entirely to notification, however. Consumers have no legal entitlement to their data; their only right is to opt out of having it shared with non-affiliated third parties.[47] (Even this entitlement has exceptions, such as for joint marketing programs.[48]) Customers have no

---

[37] *See, e.g.*, Norberto Nuno Gomes de Andrade, *Oblivion: The Right to Be Different . . . from Oneself: Reproposing the Right to Be Forgotten*, 13 REVISTA DE INTERNET, DERECHO Y POLITICA [J. INTERNET L. & POL.] 122, 134 (2012) (Spain) (arguing for the individual right to removal of old or obsolescent personal information). *But see, e.g.*, Jeffrey Rosen, *The Right to Be Forgotten*, 64 STAN. L. REV. ONLINE 88 (2012) (criticizing proposal on free speech grounds); Jane Yakowitz, *More Bad Ideas from the E.U.*, FORBES (Jan. 25, 2012, 3:57 PM), http://www.forbes.com/sites/kashmirhill/2012/01/25/more-bad-ideas-from-the-e-u/ (criticizing proposal on accuracy and free speech grounds).

[38] Natasha Singer, *Mediator Joins Contentious Effort to Add a 'Do Not Track' Option to Web Browsing*, N.Y. TIMES, Nov. 29, 2012, at B2 (describing efforts to forge an Internet standard that balances ad-supported media with individual claims to privacy).

[39] *See, e.g.*, James Q. Whitman, *The Two Western Cultures of Privacy: Dignity Versus Liberty*, 113 YALE L.J. 1151 (2004).

[40] SOLOVE, *supra* note 34.

[41] Danielle Keats Citron, *Reservoirs of Danger: The Evolution of Public and Private Law at the Dawn of the Information Age*, 80 S. CAL. L. REV. 241 (2007).

[42] ANITA L. ALLEN, UNPOPULAR PRIVACY: WHAT MUST WE HIDE? (2011).

[43] NISSENBAUM, *supra* note 32.

[44] *Cf.* Robert M. Cover, *Violence and the Word*, 95 YALE L.J. 1601 (1986).

[45] 16 C.F.R. § 314 (2012) (implementing 15 U.S.C. §§ 6801(b), 6805(b)(2) (2006)).

[46] *Id.* §§ 313.5–313.18.

[47] *Id.* § 313.10(a).

[48] *Id.* § 313.13(a); *see also id.* §§ 313.14–313.15 (noting other exceptions).

capability to prevent data sharing with third parties affiliated with their banks. Their sole recourse—which is rarely, if ever, exercised for privacy reasons—is to switch financial providers.

Firms record and trade in consumers' financial data. That means it holds value. And the law confers that value upon the provider rather than upon the consumer. This has two effects. Most immediately, it makes the financial firm relatively richer and the individual consumer relatively poorer. Second, and more subtly, it impedes development of a consumer-side market for financial data.[49] A recurring puzzle of privacy law is why markets for consumers' information, where the consumer accepts bids for her data, have failed to develop.[50] Here, the puzzle likely arises from information asymmetry: the consumer does not know what data the bank holds about her, what it is worth to the bank, or what it is worth to her.[51] Comparing the privacy policies of various providers imposes some cost; moreover, such policies tend to be vague (because the law permits them to be)[52] and largely invariant (because there is little competitive advantage to offering heterogeneous terms and because banks rationally set their defaults to maximize their information returns).[53]

Regardless of how well financial privacy regulation actually functions, it inarguably implements a set of normative choices. This allocation of value might be optimal. It could represent either an efficient set of defaults or an efficient societal outcome.[54] Providing consumers greater control over their information might impose unacceptable costs, or perhaps financial data simply does not seem sensitive enough to require greater protections. This regulatory architecture could result from public choice considerations: financial firms hold a concentrated pecuniary interest in the

---

[49] *See* Tony Vila et al., *Why We Can't Be Bothered to Read Privacy Policies: Models of Privacy Economics as a Lemons Market*, *in* ECONOMICS OF INFORMATION SECURITY 143, 143–52 (L. Jean Camp & Stephen Lewis eds., 2004).

[50] *See, e.g.*, Julie E. Cohen, *Irrational Privacy?*, 10 J. ON TELECOMM. & HIGH TECH. L. 241 (2012); Aleecia M. McDonald & Lorrie Faith Cranor, *The Cost of Reading Privacy Policies*, 4 I/S: J.L. & POL'Y FOR INFO. SOC'Y 543 (2008); Jan Whittington & Chris Jay Hoofnagle, *Unpacking Privacy's Price*, 90 N.C. L. REV. 1327 (2012).

[51] *See* JAMES P. NEHF, OPEN BOOK: THE FAILED PROMISE OF INFORMATION PRIVACY IN AMERICA 134–36 (2012); NISSENBAUM, *supra* note 32, at 105–06; Paul Schwartz, *Property, Privacy, and Personal Data*, 117 HARV. L. REV. 2055, 2097 (2004).

[52] 16 C.F.R. § 313.6.

[53] *See* Woodrow Hartzog, *Website Design as Contract*, 60 AM. U. L. REV. 1635, 1639 (2011) (stating that other than design and interactive features, "the only other contractual terms on virtually every website are standard-form").

[54] *See generally* RICHARD H. THALER & CASS R. SUNSTEIN, NUDGE: IMPROVING DECISIONS ABOUT HEALTH, WEALTH, AND HAPPINESS 85–87 (2008) (noting the importance of well-chosen default settings, especially where consumers rarely change default settings).

data, while consumers' interests are diffuse.[55] Financial firms have experience lobbying regulators; consumers do not.[56] Default entitlement settings along with disclosure, alienability, and liability rules all operate to confer the value of consumer financial data to banks rather than customers.

Privacy allocations occur outside the commercial context as well. Records of gun ownership often have stringent privacy safeguards: in many states, they are not accessible to the public,[57] and even government actors face limits[58]—the Bureau of Alcohol, Tobacco, Firearms and Explosives is the only federal agency empowered to trace firearms in criminal investigations.[59] These rules may be sensible on a number of grounds: they could safeguard important constitutional values inherent in the Second Amendment, protect gun owners from being targeted for theft, or ensure that government does not treat citizens who own guns differently from those who do not.[60] But, counternarratives are possible. Privacy in gun ownership records prevents an estranged spouse from learning that her husband has purchased a gun.[61] It keeps parents from knowing which of their children's friends live in households where a firearm is present and, therefore, from deciding whether to let them visit those friends.[62] Information about firearm ownership is power, as concealed carry laws make plain.[63] The privacy rules regarding that ownership allocate power to the gun owner and away from those who interact with her. That choice may be appropriate or not, but it is definitely a choice.

---

[55] Lynn A. Stout, *Uncertainty, Dangerous Optimism, and Speculation: An Inquiry into Some Limits of Democratic Governance*, 97 CORNELL L. REV. 1177, 1195–96 (2012).

[56] *See generally* Richard L. Hasen, *Lobbying, Rent-Seeking, and the Constitution*, 64 STAN. L. REV. 191 (2012).

[57] Kelsey M. Swanson, Comment, *The Right to Know: An Approach to Gun Licenses and Public Access to Government Records*, 56 UCLA L. REV. 1579, 1583–88 (2009).

[58] *See* 18 U.S.C. § 926(a) (2006).

[59] *National Tracing Center*, BUREAU OF ALCOHOL, TOBACCO, FIREARMS & EXPLOSIVES, http://www.atf.gov/publications/factsheets/factsheet-national-tracing-center.html (last visited Mar. 17, 2013).

[60] Elaine Vullmahn, Comment, *Firearm Transaction Disclosure in the Digital Age: Should the Government Know What Is in Your Home?*, 27 J. MARSHALL J. COMPUTER & INFO. L. 497, 518–26 (2010).

[61] James A. Mercy & Linda E. Saltzman, *Fatal Violence Among Spouses in the United States, 1976–85*, 79 AM. J. PUB. HEALTH 595, 596 (1989) ("Firearms were used in the perpetration of 71.5[%] of spouse homicides from 1976 to 1986.").

[62] *See, e.g.*, Mathew Miller et al., *Firearm Availability and Unintentional Firearm Deaths*, 33 ACCIDENT ANALYSIS & PREVENTION 477 (2001).

[63] *See, e.g.*, M. Alex Johnson, *In Florida and Illinois, Concealed-Weapons Debate Lays Bare the Politics of Gun Control*, NBC NEWS (Dec. 13, 2012, 5:58 PM), http://usnews.nbcnews.com/_news/2012/12/13/15889808-in-florida-and-illinois-concealed-weapons-debate-lays-bare-the-politics-of-gun-control?lite.

Privacy, as these two examples demonstrate, is about clashing interests and values, and about the difficult task of choosing among them. Shifts in privacy rules nearly always burden some stakeholders while benefiting others. Rule configurations are justified by recourse to value frameworks: efficiency, distributive justice, or religious prohibitions.[64] And these configurations describe how privacy ought to function. Security, by contrast, describes how privacy *does* function.

III. SECURITY

Security implements privacy's choices. Security determines who actually can access, use, and alter data.[65] When security settings permit an actor without a legitimate claim to data to engage in one of these activities, we do not view that fact as altering the normative calculus. The actor's moral claim does not change. The access or use is simply error. Security, therefore, is the interface layer between information and privacy. It mediates privacy rights, putting them into effect. Security is the bridge between data and those who consume it.[66] Security's debates are more cold-blooded and technical—they are about relative informational advantages, the ability to bear costs, and the magnitude and probability of harm.[67] Like precautions against civil harms (the domain of tort law), security measures exist along a continuum.[68] Perfection is generally unattainable or unaffordable.[69] Where there are normative choices—such as who should bear residual risk—they tend to be more deeply buried, or subsumed in utilitarian methodologies.

Formally, then, security is agnostic about how privacy rules dictate selection of who may interact with data. The capability to access or alter

---

[64] Privacy discourse often fails to make these normative commitments explicit. However, the best privacy scholarship sets forth clearly its bases for favoring a particular regime. *See, e.g.*, NISSENBAUM, *supra* note 32, at 129–57.

[65] *See* Derek E. Bambauer, *Conundrum*, 96 MINN. L. REV. 584, 628–32 (2011) (discussing access and alteration).

[66] On this account, the absence of security may well reflect a normative choice, and perhaps that should be the default assumption.

[67] *See, e.g.*, Derek E. Bambauer, *Rules, Standards, and Geeks*, 5 BROOK. J. CORP. FIN. & COM. L. 49 (2010); Hans Brechbühl et al., *Protecting Critical Information Infrastructure: Developing Cybersecurity Policy*, 16 INFO. TECH. FOR DEV. 83, 85–87 (2010); Michel van Eeten & Johannes M. Bauer, *Emerging Threats to Internet Security: Incentives, Externalities and Policy Implications*, 17 J. CONTINGENCIES & CRISIS MGMT. 221, 225–29 (2009); Vincent R. Johnson, *Cybersecurity, Identity Theft, and the Limits of Tort Liability*, 57 S.C. L. REV. 255, 299–303 (2005).

[68] *See, e.g.*, Steven Shavell, *Individual Precautions to Prevent Theft: Private Versus Socially Optimal Behavior*, 11 INT'L REV. L. & ECON. 123 (1991).

[69] Derek E. Bambauer, *The Myth of Perfection*, 2 WAKE FOREST L. REV. 22 (2012).

data can be granted to all users or none, it can be added or revoked, and it can even be bifurcated.[70] A particular technology may provide for more or less robust, granular, or transparent choices for security. That limits how effectively security can implement privacy. It does not, however, challenge the legitimacy of privacy choices in selecting the desired end state.

Informally, though, there are two interactions between security and privacy. The first parallels how Lawrence Lessig's New Chicago School anticipates interplay between law and code.[71] Different security architectures make privacy regimes more or less tenable, thereby influencing their development and adoption. Multiuser operating systems such as Unix offered greater granularity of control, and hence more finely tuned privacy in their data, than operating systems such as the early variants of Windows, which did not segregate information, even if they formally allowed users to log on with different credentials.[72] Moreover, systems where data has a temporally defined existence, such as with Vanish's self-destructing documents, make it possible to envision privacy models where data transfers are of limited duration rather than complete transfers.[73] Similarly, privacy theories will generate development of technologies that make their implementation possible. Worries about data aggregation in a time of near-costless storage and indexing helped drive firms offering Web browsers to implement anonymous surfing options, such as Google Chrome's incognito mode.[74]

The second interaction occurs with the selection of the security precautions to be taken. For example, regulation of medical records may require that only those treating a patient or covering her care via insurance have the capability to access her protected health information.[75] However, a hospital may put in place a security mechanism that fails to enforce this mandate—or, at least, fails to do so rigorously.[76] The hospital may do so innocently or deliberately. It may have incompetent information technology staff, or it may be shirking the cost of putting a more capable

---

[70] Bambauer, *supra* note 65, at 630.

[71] *See* Lessig, *supra* note 29, at 662–66.

[72] STUART MCCLURE ET AL., HACKING EXPOSED: NETWORK SECURITY SECRETS & SOLUTIONS 90, 121 (4th ed. 2003) (explaining that more granular control includes more options, for example, the option to allow a user to access information, but not to alter it).

[73] *See Overview*, VANISH: SELF-DESTRUCTING DIGITAL DATA, http://vanish.cs.washington.edu/ (last visited Mar. 17, 2013).

[74] *See Incognito Mode (Browse in Private)*, CHROME, http://support.google.com/chrome/bin/answer.py?hl=en&answer=95464 (last visited Mar. 17, 2013).

[75] *See* 45 C.F.R. § 164.502(a)(1) (2012).

[76] *See, e.g.*, News Release, U.S. Dep't of Health & Human Servs., Massachusetts Provider Settles HIPAA Case for $1.5 Million (Sept. 17, 2012), *available at* http://www.hhs.gov/news/press/2012pres/09/20120917a.html.

system in place. Yet even when the hospital is knowingly shortchanging privacy safeguards, this is a problem of implementation, not of guiding values. The hospital does not object to the level of privacy protection for health information. It simply does not want to bear the cost of providing it.[77] Presumably, if its security costs were completely covered (say, if a per-patient assessment for the new system were levied), the hospital would be entirely willing, or at least indifferent towards, implementing more robust security.

The question of security costs is one about system design: burdened parties will be tempted to shirk costly responsibilities. To counteract the lure of evading these burdens, the system must supply resources to the burdened party, monitor its behavior, threaten it with ex post sanctions, or impose some other constraint.[78] These problems are challenging, but they are standard questions of regulatory theory.

The harder question regarding cost is that it may point out a disjunction between normative choices in the abstract and burdens in reality. While privacy policy is not made in a vacuum, it is also difficult to treat it as part of a comprehensive menu of choices. Funds spent on protecting consumer financial information cannot be spent on additional customer service personnel, or on improving banks' website usability for disabled users. And enforcement efforts to ensure banks are meeting their privacy obligations cannot be employed to monitor their workplace safety or compliance with antidiscrimination rules in employment. Thus, structural features of policymaking, along perhaps with cognitive biases in decisionmaking, may lead to privacy choices that we like in theory but are unwilling to pay for in practice.[79]

Privacy determines who ought to be able to access, use, and alter information. It justifies these choices with reference to larger values—values that compete for priority and attention. Security implements that set of choices. While entities may contest who should cover the costs of security, that fight is separate from the negotiations over how access and

---

[77] *See generally* Peter Kilbridge, *The Cost of HIPAA Compliance*, 348 NEW ENG. J. MED. 1423 (2003) (quantifying the costs of HIPAA compliance for hospitals).

[78] On monitoring, see 15 U.S.C. § 80b-4 (2006 & Supp. 2012) (implementing § 404 of the Dodd–Frank Wall Street Reform and Consumer Protection Act, Pub. L. No. 111-203, 124 Stat. 1376, 1571 (2010)); on sanctions, see 45 C.F.R. § 160.402 (2012) (imposing civil penalties for violations of HIPAA); on subsidies, see Amitai Aviram, *Network Responses to Network Threats: The Evolution into Private Cybersecurity Associations*, *in* THE LAW AND ECONOMICS OF CYBERSECURITY 143, 149 (Mark F. Grady & Francesco Parisi eds., 2006) ("Public subsidies of private network security efforts may be appropriate in some cases because of the significant positive externalities network security confers on people who are not network members . . . .").

[79] THALER & SUNSTEIN, *supra* note 54, at 31–33 (discussing optimism bias).

alteration rights ought to be allocated; rather, it is simply over who pays for making those decisions a reality.

IV. KEEP 'EM SEPARATED

Paying attention to the distinction between privacy and security has important consequences. At a theoretical level, it concentrates attention on issues where normative models differ versus instances that demonstrate failures of implementation. To borrow an example from computer science researcher Christopher Soghoian, whether the California company Biofilm should ask for, and then retain, customers' e-mail addresses as the price of a sample of the personal lubricant Astroglide is a privacy question.[80] It was a security problem when Biofilm accidentally made those addresses available on its Web server.[81] When customers submitted their information to Biofilm, both parties wanted to keep that data between them. Customers gained no benefit from the inadvertent disclosure. And Biofilm's goals did not change—it did not release the information in pursuit of greater revenue or more targeted marketing. It was simply a mistake.

From a utilitarian perspective, privacy issues are a zero-sum game. If firms can track users' activities on their own websites (and perhaps other ones) and retain that data, they gain relative to a "do-not-track" regime where they cannot do so.[82] Users' gains are inversely correlated: they benefit more from a regime where they can elect to reveal information to websites versus one where they cannot. Security issues, by contrast, result in an outcome that is worse for both sides.[83] After the breach above, Biofilm is worse off, and its consumers are worse off.[84] That difference

---

[80] *See* Ryan Singel, *Security Researcher Wants Lube Maker Fined for Privacy Slip*, WIRED (July 10, 2007, 5:35 PM), http://www.wired.com/threatlevel/2007/07/security-resear/; Christopher Soghoian, *Astroglide Data Loss Could Result in $18 Million Fine*, SLIGHT PARANOIA (July 9, 2007), http://paranoia.dubfire.net/2007/07/astroglide-data-loss-could-result-in-18.html.

[81] *See* Singel, *supra* note 80; Soghoian, *supra* note 80.

[82] Robert N. Charette, *Online Advertisers Turning up the Heat Against Making "Do Not Track" Browsers' Default Setting*, IEEE SPECTRUM (Oct. 15, 2012, 3:43 PM), http://spectrum.ieee.org/riskfactor/computing/it/online-advertisers-turning-up-the-heat-against-defaulting-browsers-to-do-not-track-setting.

[83] *See* Alessandro Acquisti et al., Is There a Cost to Privacy Breaches? An Event Study 2–4 (2006) (paper prepared for Twenty-Seventh International Conference on Information Systems and Workshop on the Economics of Information Security), *available at* http://www.heinz.cmu.edu/~acquisti/papers/acquisti-friedman-telang-privacy-breaches.pdf (documenting negative effects of data breaches on stock prices).

[84] Those who access the data without permission gain a benefit. In the Biofilm case, security researcher Soghoian discovered the mistake (and also the list of users who received free Astroglide). While this problem of unauthorized third-party benefits is one that is theoretically challenging for utilitarianism, in practice it is conventional to discount or

between security and privacy has important ramifications for regulation.

At a practical level, this approach suggests that when disputes involve security flaws, rather than privacy debates, courts should permit liability at a much lower threshold of harm and fault or blameworthiness. Security might be conceptualized as akin to a contractual bargain between those who supply data and those who hold it.[85] And contract, unlike tort, is a doctrine of strict liability.[86] Courts do not care whether a breaching party is blameworthy, or whether the harm resulting from a breach is weighty or small. Merely showing breach is sufficient.[87]

Alternatively, one might envision security within tort law's framework.[88] Firms could be held to owe a duty to the subjects of the information they possess, or even to society generally, to securely store and handle data.[89] Security failures could be evaluated under strict liability (firms bear the entire cost of the harm their insecurity creates), under a negligence standard (firms only bear costs when they have failed to meet some criterion for security), or both (such as strict liability for data leaks and negligence for hacking).[90] Tort law may be preferable since it offers the possibility of compensating those harmed by security failures, even if only nominally, and of imposing greater deterrence ex ante through the threat of punitive damages.[91]

Finally, one might approach security from the perspective of criminal law, by conditioning liability upon a blameworthy mental state. As with scienter in tort, the level of mens rea could be reduced, such as to

---

exclude altogether that utility from the calculus. A principled reason for this approach is that it forces would-be attackers to enter the privacy market: they should bargain with Biofilm rather than trying to pry data from its servers. A more problematic reason is to deprecate certain types of utility for moral reasons; however, this requires importing an external normative framework into the putatively neutral utilitarian calculus.

[85] The analogy only runs so far. Society should not countenance blanket waivers of security by entities that hold data, particularly given that self-help—in the form of reading terms of service and selecting among competing firms—is infeasible at best. *See, e.g.*, McDonald & Cranor, *supra* note 50, at 565–68.

[86] Robert D. Cooter, *Economic Theories of Legal Liability*, 5 J. ECON. PERSP. 11, 12 (1991).

[87] Curtis Bridgeman, *Reconciling Strict Liability with Corrective Justice in Contract Law*, 75 FORDHAM L. REV. 3013, 3017 (2007).

[88] *See, e.g.*, Vincent R. Johnson, *Credit-Monitoring Damages in Cybersecurity Tort Litigation*, 19 GEO. MASON L. REV. 113 (2011).

[89] *See* Michael D. Scott, *Tort Liability for Vendors of Insecure Software: Has the Time Finally Come?*, 67 MD. L. REV. 425, 442–50 (2008).

[90] *See id.* at 441–50 (discussing negligence).

[91] *See* A. Mitchell Polinsky & Steven Shavell, *Punitive Damages: An Economic Analysis*, 111 HARV. L. REV. 869, 896–900 (1998).

negligence, or even eliminated, as with strict liability.[92] And as with strict liability crimes generally, security failures might be punished without the traditional requirement of blameworthiness because these violations are seen as less morally culpable.[93] Security breaches will less typically involve situations where the defendant benefits directly. Society is more likely to condemn actions where a defendant gains from his crimes than where his benefit may be minimal (the cost of some precautions not taken) or even negative (such as market harm from breaches).[94]

Thus, security failures generally leave everyone involved (except for the attacker) worse off. Privacy failures, by contrast, typically involve a transfer of utility between parties: if Biofilm sold the e-mail addresses rather than losing them, it would be enriched, and the Astroglide samplers would be worse off. Thus, privacy disputes involve courts or regulators deciding whether such transfers should be sanctioned. Security problems destroy utility. Society should have less hesitation about imposing liability for actions (or inactions) that only reduce utility.

This framework also suggests that current approaches to security problems are misguided, and even harmful. Even insecure data controllers rarely face significant liability to the subjects of the information.[95] Courts typically dispose of tort-based claims by the subjects on one or both of two grounds: duty and causation.[96] They hold that the data controller bears no duty towards the data subjects, and hence there is a lack of a prima facie cause of action.[97] (Courts are often dishonest in their analyses: lack of duty is a legal conclusion, not a factual state that compels a legal conclusion.) Second, courts typically find either that the data subjects have not suffered any harm or that harm is not attributable to the breach.[98] Even from a compensation perspective, this seems faulty: data subjects must bear the risk of harm until it materializes, rather than the data controller, which likely can avoid spills at lower cost and probably has better access to

---

[92] *See generally* Darryl K. Brown, *Criminal Law Reform and the Persistence of Strict Liability*, 62 DUKE L.J. 285 (2012) (describing rationales for states' implementation of strict-liability crimes).

[93] *See* Staples v. United States, 511 U.S. 600, 616–18 (1994); Darryl K. Brown, *Criminal Law's Unfortunate Triumph over Administrative Law*, 7 J.L. ECON. & POL'Y 657, 671 (2011).

[94] *See, e.g.*, Meghan J. Ryan, *Proximate Retribution*, 48 HOUS. L. REV. 1049 (2012).

[95] *See* Bambauer, *supra* note 67, at 58.

[96] Sasha Romanosky & Alessandro Acquisti, *Privacy Costs and Personal Data Protection: Economic and Legal Perspectives*, 24 BERKELEY TECH. L.J. 1061, 1078–81 (2009).

[97] *See, e.g.*, Katz v. Pershing, LLC, 672 F.3d 64 (1st Cir. 2012).

[98] *See, e.g.*, Reilly v. Ceridian Corp., 664 F.3d 38, 41–44 (3d Cir. 2011); Romanosky & Acquisti, *supra* note 96, at 1078–79.

insurance markets.[99] And from a deterrence perspective, this outcome is entirely wrong: it enables data holders to evade liability regardless of the level of precautions that they take, since an adjudicating court will never reach even a negligence analysis. While public enforcement occurs irregularly, such as through the Federal Trade Commission, this is insufficient to create a realistic threat of costs to press data controllers to take proper security measures.[100] Imposing something akin to strict liability for data spills is preferable: holding them liable for all proved harm would at least give data subjects the opportunity to prove loss, and the risk of punitive damages (even cabined by recent Supreme Court jurisprudence[101]) would foster deterrence.

In contrast, pure privacy claims should be treated with far more caution. An example is the litigation—and, in European countries, potential prosecution—over Google Street View.[102] As part of Google's mapping of streets and roads, the company has captured imagery of private homes, people entering bars, and even people in states of undress.[103] Google has faced potential civil and criminal liability for its actions, along with some level of opprobrium. Here, though, there are competing normative claims. Google is engaged in an activity that creates significant social benefit. The people whose travels, nakedness, and homes are made more public than expected have been relying on practical obscurity to protect their privacy. It is not obvious that Google's claims must yield pride of place.

There are important policy questions embedded in this Article's

---

[99] *See, e.g.*, Pamela Lewis Dolan, *Thinking of Buying Data Breach Insurance? Here Are Some Things to Consider*, AMEDNEWS.COM (Jan. 31, 2011), http://www.ama-assn.org/amednews/2011/01/31/bica0131.htm.

[100] *See* Andrew Serwin, *The Federal Trade Commission and Privacy: Defining Enforcement and Encouraging the Adoption of Best Practices*, 48 SAN DIEGO L. REV. 809, 854–56 (2011).

[101] *See, e.g.*, State Farm Mut. Auto. Ins. Co. v. Campbell, 538 U.S. 408, 429 (2003) (holding that a ratio of punitive damages to compensatory damages of 145 to 1 was excessive).

[102] W.J. Hennigan, *Google Pays Pennsylvania Couple $1 in Street View Lawsuit*, L.A. TIMES (Dec. 2, 2010, 12:13 PM), http://latimesblogs.latimes.com/technology/2010/12/google-lawsuit-street.html; Seth Weintraub, *Google's Streetview Victorious in European Courts*, CNNMONEY (Mar. 21, 2011, 6:36 PM), http://tech.fortune.cnn.com/2011/03/21/googles-streetview-victorious-in-european-courts/.

[103] Matt Hickman, *9 Things You Probably Shouldn't Do in the Presence of a Google Street View Vehicle*, MOTHER NATURE NETWORK (Oct. 4, 2012, 7:05 PM), http://www.mnn.com/lifestyle/arts-culture/stories/9-things-you-probably-shouldnt-do-in-the-presence-of-a-google-street-; *Artist Captures Bizarre Images Shot by Google's Street View Cameras*, N.Y. DAILY NEWS (Dec. 6, 2012, 3:31 PM), http://www.nydailynews.com/entertainment/bizarre-images-captured-google-street-view-cameras-gallery-1.1214757.

approach. For example, at what level of fault or intent should liability be imposed for security breaches? The correct answer is likely to vary by industry, and perhaps even more granularly than that. There are at least two important factors. First, what fraction of the implementation costs does the potential defendant bear? Is it able to pass these expenses through to its customers at low transaction cost? A lower liability threshold might be appropriate where the holder of the data has a pecuniary incentive to shirk its duties. Second, is there any risk that this security problem is, in fact, a privacy problem? The data owner, for example, might have neglected security because doing so better enabled it to exploit the data. Here, too, liability at a lower threshold of fault or blameworthiness is useful as a channeling function: data owners should take up privacy fights directly, rather than using security as indirect means to attain their goals.[104] These questions, while critical to successful implementation, are technical ones. They bear not on what ends are to be achieved, but rather on the mechanisms to achieve them.

V. CONCLUSION

Security and privacy can, and should, be treated as distinct concerns. Privacy discourse involves difficult normative decisions about competing claims to legitimate access to, use of, and alteration of information. It is about selecting among different philosophies and choosing how various rights and entitlements ought to be ordered. Security implements those choices—it mediates between information and privacy selections. Importantly, this approach argues that security failings should be penalized more readily, and more heavily, than privacy ones, because there are no competing moral claims to resolve and because security flaws make all parties worse off.

---

[104] As one example, in 2011, Google began encrypting searches by users signed in to its services. The new search encryption prevents websites that users visited by clicking on a result from obtaining referrer data that reveal the terms that the users searched. However, Google still transmits referrer data when a user clicks an ad. Search engine optimization (SEO) firms objected to the first change, and some privacy advocates objected to continued transmission of referrer data with ads. The critique of Google was that it guised the change in security terms, while the major effect was to drive website owners onto the company's search optimization tools and away from competing SEO firms. *See* Danny Sullivan, *Google to Begin Encrypting Searches & Outbound Clicks by Default with SSL Search*, SEARCH ENGINE LAND (Oct. 18, 2011, 2:09 PM), http://searchengineland.com/google-to-begin-encrypting-searches-outbound-clicks-by-default-97435.