Fall 2010

Locating the Regulation of Data Privacy and Data Security

Edward J. Janger
Brooklyn Law School, edward.janger@brooklaw.edu

LOCATING THE REGULATION OF DATA PRIVACY AND DATA SECURITY

Edward J. Janger[*]

In our 2007 Article on notification of security breaches, Paul Schwartz and I explored the concept of a centralized response agent to help coordinate private and public efforts to respond to data spills.[1] In that Article, we were agnostic about whether the coordinated response agent should be public or private, and if public where, institutionally, it should be situated.[2] An important element of that agnosticism was our retrospective focus. We were concerned with response to breaches that had already occurred. The question of regulating data security and privacy is, of course, broader, encompassing the formulation of norms for appropriate data use, data protection, and breach response.[3] In this essay, I will briefly address my agnosticism, and ask, more broadly, which institutions might best handle the generation and enforcement of legal entitlements regarding invasions of privacy and data security breaches.

The occasion for asking this question is the recent enactment of the Wall Street Reform and Consumer Protection Act, which creates, as a crucial component of efforts to reregulate the banking industry, a Consumer Financial Protection Bureau (CFPB or the Bureau).[4] The principal goal of the new Bureau will be to examine consumer credit instruments as products to ensure that they are "safe" for consumers to "use."[5] The proposal for such an agency, made initially by Elizabeth Warren and Oren Bar-Gill, was

---

[*] David M. Barse Professor, Brooklyn Law School and Anne Urowsky Visiting Professor, Yale Law School. The author would like to thank Lisa Baldesweiler for able research assistance, and Joan Wexler and the Dean's Research Fund for generous support of this project. Mistakes are, of course, mine alone.

1. Paul M. Schwartz & Edward J. Janger, *Notification of Data Security Breaches*, 105 MICH. L. REV. 913 (2007) [hereinafter Schwartz & Janger, *Data Security Breaches*].

2. *See id.* at 961.

3. We have addressed these questions as well in earlier work, both together and separately. *See generally* Edward J. Janger & Paul M. Schwartz, *The Gramm-Leach-Bliley Act, Information Privacy, and the Limits of Default Rules*, 86 MINN. L. REV. 1219 (2002) [hereinafter Janger & Schwartz, *Limits on Default Rules*]; Edward J. Janger, *Privacy Property, Information Costs and the Anticommons*, 54 HASTINGS L.J. 899 (2003) [hereinafter Janger, *Anticommons*]; Edward J. Janger, *Muddy Property: Generating and Protecting Information Privacy Norms in Bankruptcy*, 44 WM. & MARY L. REV. 1801 (2003) [hereinafter Janger, *Muddy Property*].

4. At the time of the Symposium, the proposal for the "Bureau" was embodied in the Consumer Financial Protection Agency Act of 2009, H.R. 3126, 111th Cong. § 111 (2009). In July, President Obama signed the Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010, Pub. L. No. 111-203, 124 Stat. 1376 (2010). Title X of that Act was called the Consumer Financial Protection Act of 2010. *Id.* Instead of creating a separate agency, that Act created a Consumer Financial Protection Bureau within the Federal Reserve Bank. *Id.*

5. *Id.*

based on two linked insights.[6] First, that modern consumer credit instruments—be they mortgages, credit cards, or debit cards—are just as much products as a toaster.[7] And second, that while there is a consumer products safety commission that is tasked with ensuring the safety of toasters, there is no similar agency tasked with ensuring that financial products are safe.[8] Warren and Bar-Gill note that there is a congeries of agencies that have some jurisdiction over consumer financial protection—the Federal Reserve, the Office of the Comptroller of the Currency (OCC), the Federal Trade Commission (FTC), the Federal Deposit Insurance Corporation (FDIC), and so on.[9] Most of these agencies have as their focus the regulation of the banking system, rather than the protection of a bank's customers.[10] The FTC alone focuses on consumer protection, but its jurisdiction is spread across the market generally.[11]

The discussion of the CFPB might not, at first glance, seem relevant to questions of data privacy in the payment system. Indeed, much of the discussion of the safety of consumer financial products has focused on the credit and repayment terms associated with credit cards and mortgages.[12] But the use and security of data gathered and transferred in credit and payment card transactions is every bit as much a danger of these products as over-indebtedness.[13] Identity theft and invasion of privacy are harms associated with these products. Moreover, the contracting process associated with such non-price terms is particularly prone to lemons equilibria, and hence even more problematic than that relating to the price of credit.[14] Therefore, it is fair to ask whether data privacy and data security ought to be included in the mission of the CFPB.

In this essay, I will explore whether locating regulation of data privacy and data security in the CFPB would be beneficial, or whether jurisdiction would be better left to the existing regulators. I argue that responsibility for protecting personal information would best be split in two. The generation of privacy and data security norms can—and probably should—be situated

---

6. Oren Bar-Gill & Elizabeth Warren, *Making Credit Safer*, 157 U. PA. L. REV. 1, 98–100 (2008).

7. *See id.* at 3–6.

8. *See id.* at 4–5.

9. *See id.* at 86.

10. *See id.* at 85.

11. *See id.* at 86.

12. Susan Block-Lieb & Edward J. Janger, *The Myth of the Rational Borrower: Rationality, Behaviorism, and the Misguided "Reform" of Bankruptcy Law*, 84 TEX. L. REV. 1481, 1513 (2006).

13. *See infra* Part I.C (discussion on Hannaford Brothers and TJX Companies).

14. *See, e.g.*, ROBERT COOTER & THOMAS ULEN, LAW AND ECONOMICS 41 (2d ed. 1997); George A. Akerlof, *The Market for "Lemons": Quality Uncertainty and the Market Mechanism*, 84 Q.J. ECON. 488, 489–90 (1970); Richard Craswell, *Property Rules and Liability Rules in Unconscionability and Related Doctrines*, 60 U. CHI. L. REV. 1, 49 (1993); Janger & Schwartz, *Limits on Default Rules*, *supra* note 3, at 1240–41; Michael Spence, *Consumer Misperceptions, Product Failure and Producer Liability*, 44 REV. ECON. STUD. 561, 561 (1977).

in an agency like the CFPB. By contrast, measures for responding to data spills might best be coordinated by the existing banking-focused agencies. Finally, regulation of data security precautions should be shared between the consumer protection agency and the bank regulatory agency.

This Article will proceed in three steps. First, I will explain the differences between data privacy and data security, and describe the existing regulatory architecture. In the second part, I will explore the various ways in which data privacy and data security norms can be fashioned, starting with contract, then self-regulation, and finally methods of public regulation. Third, I will discuss the possibility that, while the CFPB has a role to play in regulating data privacy and data security, there are important differences between norm generation for data privacy, data security, and loss mitigation that suggest different locations for regulatory authority. I will argue that the proposed CFPB has an important role to play in the formulation of the data privacy and data security norms that govern consumer relationships with their banks. By contrast, loss mitigation may be more appropriately handled through industry self-regulation, or through the regulatory institutions that are focused on systemic risk.

I. DATA PRIVACY AND DATA SECURITY

Data privacy and data security are closely related concepts, but they are not the same. Data privacy requires that data be kept secure, but data may be kept secure for reasons other than privacy.[15] Entities that wish to hold their data secure may not care at all about the privacy of those who disclosed the data.[16] So first, it is important to define terms. If data privacy is viewed as the power to keep data secluded and safe from view, then data privacy and data security *are* the same. This conflation turns, however, on the mistaken view that data privacy is purely about concealment. This is only partially true. In all contexts that matter, data privacy involves a bilateral or multilateral relationship between a discloser and a recipient, or recipients, of information.[17] Privacy is not usually about data concealment, it is about enforcing norms and expectations with regard to data sharing.[18]

---

15. Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1609, 1663 (2001) (describing the "data seclusion deception"). The conflation of privacy and security arises from the mistaken impression that data privacy is actually about keeping data private. *Id.*

16. For example, data aggregators such as Choice Point or credit reporting agencies gather personal information, and keep it secure, not because they care particularly about consumer expectations of privacy, but because information is their stock-in-trade. Schwartz & Janger, *Data Security Breaches*, *supra* note 1, at 922–23.

17. *See* Schwartz, *supra* note 15, at 1660 ("We can refer to these ideas as . . . the 'autonomy trap' and . . . the 'data seclusion deception.'"); *see also* ROBERT C. POST, CONSTITUTIONAL DOMAINS: DEMOCRACY, COMMUNITY, MANAGEMENT 51–88 (1995). *See generally* Robert C. Post, *The Social Foundations Of Privacy: Community and Self in the Common Law Tort*, 77 CAL. L. REV. 957 (1989).

18. *See* Janger, *Anticommons*, *supra* note 3, at 904–08.

In the payment system, for example, a purchaser reveals his or her identity and account information to a merchant, the merchant passes that information through a data conduit to the clearance network, the availability of funds or credit is verified, and the transaction is processed.[19] Along the way, at least four entities are given access to potentially sensitive personal information. The merchant learns the customer's name, credit card number, and purchasing preferences. Some or all of that information is also passed to the merchant's bank, the clearance network (i.e., Visa, MasterCard, Amex), and to the customer's bank.[20] All of these disclosures may be fairly characterized as consistent with the primary purpose of the discloser—accomplishing payment.

Data privacy refers to the norms which govern information sharing and the permitted secondary uses of disclosed information by each of the entities that handle or come into possession of personal information.[21] The touchstone is the discloser's reasonable expectations of privacy.[22] Privacy norms govern what happens once these various entities have identifiable personal information about the discloser. What may they do with that information? With whom may they share it? What secondary uses of personal information are permitted to the recipients of that information? Data security, by contrast, regulates the procedures for ensuring that the disclosed information remains where the parties to the transaction intend and may be accessed only by people who are authorized.[23] Thus, a privacy violation usually involves an intentional act by the information recipient

---

19. LYNN M. LOPUCKI, ELIZABETH WARREN, DANIEL KEATING & RONALD J. MANN, COMMERCIAL TRANSACTIONS: A SYSTEMS APPROACH 317 (4th ed. 2009).

20. *Id.*

21. *See, e.g.*, Joel R. Reidenberg, *Privacy Wrongs in Search of Remedies*, 54 HASTINGS L.J. 877 *passim* (2003); Joel R. Reidenberg, *E-Commerce and Trans-Atlantic Privacy*, 38 HOUS. L. REV. 717, 720 (2001); Joel R. Reidenberg, *Resolving Conflicting International Data Privacy Rules in Cyberspace*, 52 STAN. L. REV. 1315, 1347 (2000); Joel R. Reidenberg, *Restoring Americans' Privacy in Electronic Commerce*, 14 BERKELEY TECH. L.J. 771, 773 (1999). *See also* Daniel J. Solove, *Data Mining and the Security-Liberty Debate*, 75 U. CHI. L. REV. 343 *passim* (2008); Daniel J. Solove, *"I've Got Nothing to Hide" and Other Misunderstanding of Privacy*, 44 SAN DIEGO L. REV. 745, 754–60, 767–70 (2007). *See generally* Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477 (2006) (developing a new taxonomy for privacy, focusing on activities that invade privacy); Daniel J. Solove, *Identity Theft, Privacy, and the Architecture of Vulnerability*, 54 HASTINGS L.J. 1227 (2003) (conceptualizing privacy and advocating for protections that shape this concept).

22. *See, e.g.*, Joel R. Reidenberg, *Privacy in the Information Economy: A Fortress or Frontier for Individual Rights?*, 44 FED. COMM. L.J. 195, 221–27 (1992) (discussing various types of actionable invasions of privacy in the common law and the general requirement that there be a reasonable expectation of privacy in the appropriated information) [hereinafter Reidenberg, *Frontier for Individual Rights*].

23. *Compare* Gramm-Leach-Bliley Financial Modernization Act of 1999 § 501, 15 U.S.C. § 6801 (2006) (stating that a financial institution "shall establish appropriate standards . . . (3) to protect against unauthorized access"), *with id.* § 6802 (stating that a financial institution "may not . . . disclose . . . to a nonaffiliated third party any nonpublic personal information").

that violates the expectations of the receiver.[24] A security violation, by contrast, may involve a violation of a duty of care,[25] but it rarely—if ever—involves an intentional disclosure of information.[26] These differences suggest that different approaches may be necessary for generating and enforcing data security and data privacy norms.

A. DATA PRIVACY AND GLB

Until recently, the principal regulation governing data privacy in the payment system was the Graham-Leach-Bliley Act[27] (GLB).[28] Section 501 of the Act creates an obligation to protect the privacy of customer data.[29] Section 502 gives some limited heft to that obligation, requiring notice and an opportunity to opt out of any sharing of data with a non-affiliate, and limiting the reuse of that information by non-affiliates.[30] This regime has been criticized for killing trees with relatively useless privacy notices, for providing precious little data privacy protection because affiliate sharing is permitted, and because the opt-out rule sets the default in favor of non-affiliate sharing.[31]

As a result, the onus for developing privacy standards, and establishing enforceable privacy rights, rests on consumers' willingness and ability to contract for protection. In other words, if a consumer wishes to limit the sharing of her data, she must affirmatively opt out of data sharing, and, to the extent she wishes to limit affiliate sharing, she will have to negotiate for it.[32] In most cases this will mean foregoing the commercial relationship with the financial institution. The limits of consumer contracting and the problem of contracts of adhesion have been well discussed elsewhere.[33] Paul Schwartz and I have discussed it specifically in the context of GLB,

---

24. Reidenberg, *Frontier for Individual Rights*, *supra* note 22, at 222–23.

25. *Id.* at 223–24.

26. *Id.*

27. 15 U.S.C. § 6801.

28. *See generally* Schwartz & Janger, *Data Security Breaches*, *supra* note 1.

29. 15 U.S.C. § 6801(a) ("It is the policy of the Congress that each financial institution has an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers' nonpublic personal information.").

30. *Id.* § 6802.

31. Timothy J. Muris, Chairman, Fed. Trade Comm'n, Remarks at the 2001 Privacy Conference: Protecting Consumers' Privacy: 2002 and Beyond (Oct. 4, 2001), http://ftc.gov/speeches/muris/privisp1002.shtm.

32. Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 STAN. L. REV. 1193, 1246–67 (1998); Richard S. Murphy, *Property Rights in Personal Information: An Economic Defense of Privacy*, 84 GEO. L.J. 2381, 2402–04 (1996); Paul M. Schwartz, *Privacy and the Economics of Personal Health Care Information*, 76 TEX. L. REV. 1, 53–67 (1997) [hereinafter Schwartz, *Privacy Economics*]; Jeff Sovern, *Opting In, Opting Out, or No Options at All: The Fight for Control of Personal Information*, 74 WASH. L. REV. 1033, 1101–13 (1999); *see also* Janger & Schwartz, *Limits on Default Rules*, *supra* note 3, at 1221.

33. C & J Fertilizer. Inc. v. Allied Mutual Ins. Co., 227 N.W.2d 169, 174 (Iowa 1975); *see generally* Todd D. Rakoff, *Contracts of Adhesion: An Essay in Reconstruction*, 96 HARV. L. REV. 1173 (1983).

and found the result unsatisfactory.[34] We concluded that the likely product of GLB's notice and opt-out regime is a lemons equilibrium in which bad privacy practices prevail.[35] We raised these issues in 2002, and nothing that has happened since then has led us to question these conclusions. Instead the focus of regulatory concern has been identity theft, which is really not a "privacy" problem at all. The reasons for this shift of focus are discussed below.

B. DATA SECURITY AND GLB § 501(B)

GLB has relatively little to say on the subject of data security, but curiously, that is where the action has been.[36] Section 501 of GLB consists principally of a delegation to the agencies that govern financial institutions.[37] It provides in full:

> **(b) Financial institutions safeguards**
>
> In furtherance of the policy in subsection (a) of this section, each agency or authority described in section 505(a) of this title shall establish appropriate standards for the financial institutions subject to their jurisdiction relating to administrative, technical, and physical safeguards—
>
> (1) to insure the security and confidentiality of customer records and information;
>
> (2) to protect against any anticipated threats or hazards to the security or integrity of such records; and
>
> (3) to protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer.[38]

It instructs the various bank supervisory agencies to develop regulations for handling customer data, such as PIN numbers, social security numbers, and other data that might create a risk of, among other things, identity

---

34. Janger & Schwartz, *Limits on Default Rules*, *supra* note 3, at 1230–32.

35. Craswell, *supra* note 14, at 49. Richard Craswell states:

> Because terms that are good for buyers are generally more expensive for sellers, any seller that offers better terms will charge a higher price to make the same level of profits she could make by offering less favorable terms at a lower price. However, if most buyers have good information about prices but only poor information about non-price terms, they may not notice an improvement in non-price terms, while they will definitely notice the higher price. As a result, many buyers may stop purchasing from this seller.

Id.

36. *See* Gramm-Leach-Bliley Financial Modernization Act of 1999, 15 U.S.C. § 6801 (2006).

37. *Id.* § 6801(b).

38. *Id.*

theft.[39] In response, the various bank supervisory agencies promulgated the Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice that mandates risk assessments and the creation of a response program by financial institutions.[40] In addition, the regulations contemplate a two-tier system of reporting security breaches.[41] Any security breach must be reported to the financial institution's supervising agency.[42] If, after an investigation, it appears that there is risk to the consumer, then notice of the security breach must also be given to the consumer.[43] While the Interagency Guidance is not perfect, it does mandate a relatively comprehensive architecture for managing sensitive personal financial data.[44] The delegation contained in § 501(b) could have been exercised in any number of ways. But, unlike privacy, the task of regulating data security has not been left to contract. Data security has been regulated more robustly than secondary use.

C. SELF REGULATION AND STANDARD SETTING—PCI DSS

The regulation of data security has not been limited to government agencies. The payment card industry has taken it upon itself to engage in self regulation in this area through the creation of the Payment Card Industry Security Standards Council (PCI SSC).[45] The PCI SSC consists of the entities responsible for clearing payment card transactions—Visa, MasterCard, American Express. This group has promulgated a series of protocols called the Payment Card Industry Data Security Standard or PCI DSS.[46] This standard is intended to form the basis for auditing the security practices of participants in the payment card clearance system.[47] The PCI DSS standard requires participants in the payment system, in broad outline, to:

---

39. *Id.* §§ 6801(a), 6804(a)(1); Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice, 70 Fed. Reg. 15,736, 15,752 (Mar. 29, 2005), *available at* http://edocket.access.gpo.gov/2005/pdf/05-5980.pdf.

40. Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Notice, 70 Fed. Reg. at 15,751–54.

41. *Id.* at 15,752; *see also* Edward J. Janger & Paul M. Schwartz, *Anonymous Disclosure of Security Breaches: Mitigating Harm and Facilitating Coordinated Response, in* SECURING PRIVACY IN THE INTERNET AGE 223, 227 (Anum Chander, et al. eds., 2008).

42. Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice, 70 Fed. Reg. at 15,752.

43. *Id.*

44. Schwartz & Janger, *Data Security Breaches*, *supra* note 1, at 920.

45. PCI SECURITY STANDARDS COUNCIL, http://www.pcisecuritystandards.org (last visited Dec. 30, 2010).

46. PCI SSC Data Security Standards Overview, PCI SECURITY STANDARDS COUNCIL, https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml (last visited Dec. 30, 2010).

47. Doug Drew & Sushila Nair, *Payment Card Industry Data Security Standard in the Real World*, INFO. SYS. CONTROL J., 1 (Sept./Oct. 2008), http://www.isaca.org/Journal/Past-Issues/2008/Volume-5/Documents/jpdf0805-payment-card-industry.pdf.

1. Install and maintain a firewall configuration to protect cardholder data.

2. [N]ot use vendor-supplied defaults for system passwords and other security parameters.

3. Protect stored cardholder data.

4. Encrypt transmission of cardholder data across open, public networks.

5. Use and regularly update anti-virus software [on all systems commonly affected by malware].

6. Develop and maintain secure systems and applications.

7. Restrict access to cardholder data by business need-to-know basis.

8. Assign a unique ID to each person with computer access.

9. Restrict physical access to cardholder data.

10. Track and monitor all access to network resources and cardholder data.

11. Regularly test security systems and processes.

12. Maintain a policy that addresses information security. [48]

Notwithstanding the implementation of PCI DSS, there have been numerous data spills. Indeed, Hannaford Brothers and TJX Companies were both hacked in 2008.[49] Ironically, Hannaford received its certification one day after being made aware of a two-month compromise of its internal system.[50] The proponents of PCI DSS point out that PCI DSS compliance is assessed at a specific moment in time, and that none of the entities that have been breached was actually complying with the PCI DSS protocol at the time of its breach.[51] They lay the blame, not on the protocols, but on the implementation of compliance validation procedures.[52]

---

48. *Id.* at 2.

49. Brian Krebs, *Three Alleged Hackers Indicted in Large Identity-Theft Case*, WASH. POST, Aug. 18, 2009, at A11; Dan Goodin, *TJX Suspect Indicted in Heartland, Hannaford Breaches*, THE REGISTER (Aug. 17, 2009, 8:49 PM), http://www.theregister.co.uk/2009/08/17/heartland_payment_suspect.

50. *Middleware Audits and Remediation for PCI Compliance: The New Frontier of PCI*, EVANS RES. GRP., 1 (2009), http://www.evansresourcegroup.com/partners.html (follow "Read our Whitepaper: Middleware Audits and Remediation for PCI Compliance: The new frontier of PCI" hyperlink at bottom of page).

51. Jaikumar Vijayan, *Post-Breach Criticism of PCI Security Standard Misplaced, Visa Exec Says*, COMPUTERWORLD (Mar. 19, 2009, 12:00 PM), http://www.computerworld.com/s/article/9130073/Post_breach_criticism_of_PCI_security_standard_misplaced_Visa_exec_says. *See also* Goodin, *supra* note 49; Kim Zetter, *TJX Hacker Charged with Heartland, Hannaford Breaches*, WIRED (Aug. 17, 2009, 2:34 PM), http://www.wired.com/threatlevel/2009/08/tjx-hacker-charged-with-heartland/.

52. Andrew Conry Murray, *PCI and the Circle of Blame*, NETWORK COMPUTING (Feb. 23, 2008), http://networkcomputing.com/data-protection/pci-and-the-circle-of-blame.php.

Interestingly, the payment card industry has proven much more interested in creating norms and an architecture for protecting data security than in articulating data sharing norms.[53] One might point to the emergence of private issuers of "privacy seals," such as Trust-E and Secure Scan, but the recent FTC settlement with ControlScan suggests that this market solution is far from perfect.[54] In that case, a privacy seal provider was shown to have regularly failed to verify the privacy practices of the merchants it endorsed.[55]

D. CONCLUSIONS AND QUESTIONS

This brief review of the regulatory architecture raises a number of questions. First, why do the regulating agencies seem inclined to leave the creation and enforcement of data privacy norms to the law of contracts, while taking a more proactive approach to protecting data security? Second, why hasn't the market responded through competition over privacy practices? And third, what does this tell us about the appropriate government approach to regulating data privacy as compared to data security?

II. SOURCES OF REGULATION: COMMON LAW, CONTRACT AND REGULATION

To decide whether public regulation is necessary one starts by asking whether there is a market failure.[56] That question further turns on whether, left to themselves, the combination of private contracting behavior, contract law, and tort law will produce optimal regulation. The answer to this question in the context of data privacy and security may be too obvious to bear discussion. To the extent that contract is involved, Susan Block-Lieb and I, as well as Oren Bar-Gill, have written at length about the extent to which consumers make cognitive and heuristic errors in deciding whether to enter into consumer credit transactions.[57] Consumers, it turns out, are notoriously bad at figuring out how much it is going to cost them to borrow money; they are also relatively bad at making inter-temporal comparisons between consumption in the present and consumption in the future.[58] There is, moreover, a considerable literature on the extent to which consumers are

53. Evan Schuman, *FTC: Web Site Security Seals are Lies*, CBSNEWS.com, Mar. 5, 2010, http://www.cbsnews.com/stories/2010/03/05/opinion/main6270104.shtml.

54. *Id.* (discussing the "bogus" security verification supplied by ControlScan in the context of the FTC settlement).

55. *Id.*

56. RICHARD A. POSNER, ECONOMIC ANALYSIS OF LAW 389 (7th ed. 2007).

57. Bar-Gill & Warren, *supra* note 6, at 12–13; Block-Lieb & Janger, *supra* note 12, at 1489–90.

58. Bar-Gill & Warren, *supra* note 6, at 29–33.

even worse at negotiating over the non-price terms of contracts.[59] What is clear is that consumers are not good at bargaining over either privacy or data security. As such, relying on contract to establish data privacy and security norms will place all of the power in the hands of the financial institutions that receive the information.[60]

While comparing bad to worse may not be profitable, it is possible that consumers' ability to bargain over data security is even worse than their ability to bargain over privacy terms. Consumers may be able to articulate their expectations about how their information might be used in broad terms.[61] This failure of imagination and lack of information is even worse for data security. Consumers cannot be expected to understand or monitor the data security practices of their banks. And, while, from time to time, banks compete on the basis of data security,[62] as far as consumers are concerned, their claims are entirely unverifiable. Indeed, the time when most financial institutions spend the most advertising about data security is after they have been subject to a breach.[63]

Where bargaining is impossible, as with data security, the natural common law substitute is tort law.[64] The law of negligence might be expected to step in to establish data security norms. The problem with relying on common law enforcement through private litigation is that even when consumers discover that they have been the victims of identity theft it is virtually impossible for the consumer to discover the source of the breached data.[65] Thus, most data security breaches are likely to escape detection, and hence financial institutions are unlikely to fully internalize the costs associated with lax security practices.

For these reasons, it is not surprising that contract and tort have not provided adequate protection of either data privacy or data security. Thus, it would appear that some form of regulatory response would be appropriate for determining what data privacy terms should be embodied in consumer credit and consumer payment contracts. Similarly, the nature of the obligation to prevent data theft, fraud, or identity theft will have to be created by public processes. Finally, the architecture for responding to data spills will likely require some degree of public coordination.

---

59. Richard Craswell, *Contract Law, Default Rules, and the Philosophy of Promising*, 88 MICH. L. REV. 489, 505–08 (1989).

60. Schwartz & Janger, *Data Security Breaches*, *supra* note 1, at 927; Joseph Turow et al., *The Federal Trade Commission and Consumer Privacy in the Coming Decade*, 3 I/S: J.L. & POL'Y FOR INFO. SOC'Y 723, 730–32 (2007).

61. But even here there may be a failure of imagination. Few consumers realize how many hands information passes through in completing a transaction.

62. Schwartz & Janger, *Data Security Breaches*, *supra* note 1, at 948.

63. *Id.*

64. GUIDO CALABRESI, THE COSTS OF ACCIDENTS: A LEGAL AND ECONOMIC ANALYSIS 125–26 (1970).

65. Schwartz & Janger, *Data Security Breaches*, *supra* note 1, at 962–63.

III. THE CONSUMER FINANCIAL PROTECTION BUREAU AS A REGULATOR OF PRIVACY AND SECURITY

As noted above, in their 2008 article, Elizabeth Warren and Oren Bar-Gill proposed the creation of an independent consumer financial protection agency.[66] The tasks of such an agency would be to review the various consumer credit products offered to consumers to ensure that they were safe.[67] A CFPB is part of the financial reform bill that was enacted this year.[68] The financial reform bill is over 1300 pages long, but the key provisions are §§ 1031 and 1032. Section 1031 grants power to the Bureau to promulgate regulations that prohibit unfair, abusive, or deceptive acts or practices.[69] Section 1032 authorizes the Bureau to mandate certain disclosures, and to create loan forms that, if used, provide a safe harbor from liability.[70]

The principal focus in discussion of these sections has been the financial terms associated with such consumer credit products. Modern products, including credit cards and home mortgages, have often been designed expressly to hide their true costs.[71] Back end fees, teaser rates, default rates, negative amortization, and balloon payments are just a few of what Warren describes as the "tricks and traps" that have become standard practices in the consumer credit market and, in particular, the subprime market.[72] Warren and Bar-Gill proposed an agency that would examine such products for transparency and would examine marketing practices to ensure that loans were only extended to people for whom they were appropriate.[73] The absence of such regulation played an important role in the financial meltdown of the last few years.

Institutional competence is at the heart of Warren and Bar-Gill's argument for a CFPB.[74] It is not that statutory protections did not exist for consumers in credit transactions. Their concerns were the related problems of regulatory capture and diffusion of responsibility.[75] Warren and Bar-Gill were concerned instead that too many agencies had jurisdiction over consumer protection, but none had it as its core purpose.[76] The FDIC, the

---

66. Bar-Gill & Warren, *supra* note 6, at 98.

67. *Id.* at 98–99.

68. Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010, Pub. L. No. 111-203, § 1011, 124 Stat. 1376, 1964–65 (2010).

69. *Id.* § 1031.

70. *Id.* § 1032.

71. Bar-Gill & Warren, *supra* note 6, at 54–55.

72. *Id.* at 56.

73. *Id.* at 98–100; *see also* Susan Block-Lieb & Edward Janger, *Demand-Side Gatekeepers in the Market for Home Loans*, 82 TEMP. L. REV. 465, 495 (2009).

74. Bar-Gill & Warren, *supra* note 6, at 74.

75. *Id.* at 99–100, nn. 323, 325.

76. Bar-Gill & Warren state:

OCC, and the Federal Reserve all had some responsibility for consumer protection, but their core function was protecting the safety and soundness of the banking system.[77] By contrast, the FTC had consumer protection as a core function, but little expertise with financial products.[78]

While the CFPB's intended focus is on lending products, and on the credit function associated with payment cards, the use of credit cards as payment devices raises a different set of safety issues that might be handled similarly by such an agency. Data privacy and data security are just as much terms of the credit/payment card contract as is the interest rate. And, if anything, they are less transparent. The question therefore is not, could the CFPB mandate include data privacy and data security; the question is whether it should, as a matter of comparative institutional competence.

In considering whether the CFPB would be an appropriate regulator of financial privacy and security, the divide between data privacy and data security is instructive. While legislation and regulation at the federal level have not been perfect in either category, the regulations promulgated under § 501(b) relating to data security are far more thoughtful than those relating to data privacy.[79] Similarly, to the extent that self regulation has had any impact whatsoever, it has had influence on the data security side.[80]

This discrepancy may be traceable to the intrinsic difference between data privacy and data security. Where data privacy is involved, there is an inherent conflict of interest between consumers and banks. Consumers expect their data to be kept confidential, and expect secondary use to be narrowly cabined. The financial institutions would like to have as much discretion as possible in how they use personal information. They have every incentive to contract for broad discretion, and to ensure that legislation does not interfere with their ability to use information as they desire.

By contrast, where data security is involved, the conflict of interest between consumer and financial institution has a different contour. While financial institutions do have an incentive to limit the extent to which contracts or legal regulations might lead to the imposition of liability, they

---

> This litany of agencies, limits on rulemaking authority, and divided enforcement powers results in inaction. No single agency is charged with supervision over any single credit product that is sold to the public. No single agency is charged with the task of developing expertise or is given the resources to devote to enforcement of consumer protection. No single agency has an institutional history of protecting consumers and assuring the safety of products sold to them.

Id. at 97 (citations omitted).

77. *Id.* at 93–95.

78. *Id.* at 95–96.

79. *See supra* Part I.B.

80. *See supra* Part I.C.

also have a relatively strong interest in ensuring that personal data remains secure.

This interest is not a product of their particular interest in data security. Instead, it is a product of the risk of loss rules that govern parties in the payment system. One can go as far back as the rule in *Price v. Neal*,[81] and the properly payable rule under 4-401 of the Uniform Commercial Code (UCC) to see that the risk of fraud is placed, in the first instance, on the bank that fails to detect it.[82] If a financial institution honors an unauthorized check, it must re-credit the account.[83] Similarly, under the Truth in Lending Act (TILA), the credit card bank must re-credit the account if an unauthorized charge is made on a credit card.[84] While, in both cases, it may be possible for the paying bank to push liability down to the merchant who initially took the check or accepted the card, the loss is going to rest on a bank, not on the consumer. In this regard, banks have every incentive to make sure that data remains secure. This interest is reflected in the self regulation that produced a program like PCI DSS. Here, the alignment between the banking industry and the bank regulatory agencies may be a plus rather than a minus.

This alignment of interest between consumers and financial institutions appears to be reflected as an alignment of interest between regulators and the regulated. There are types of coordination and response that cannot be handled by one firm alone. Neither can a consortium of private actors accomplish such coordination without public assistance.

PCI DSS and the Hannaford data spill offer an example of both the promise of self regulation and its limits. PCI DSS may be a well considered and effective standard for protecting data security, but the standard setting body has limited power to enforce the standards it sets.[85] It can audit participants in the payment system.[86] It can deprive victims of data spills membership going forward, but it cannot, in any meaningful way, punish, and it has limited power to exclude members.[87]

By contrast, the existence of a standard such as PCI DSS may work effectively in conjunction with tort law to set the standard by which negligence might be judged, after the fact. PCI DSS could provide a framework for regulatory agencies to include or exclude participants from the payment system.

---

81. Price v. Neal, (1762) 97 Eng. Rep. 871 (K.B.) 871–72; 3 Burr. 1354, 1357. The rule in *Price v. Neal* places the risk of loss for a forged check on the depositors' bank that pays the instrument without noticing that the signature is forged. *Id.*

82. *See* U.C.C. § 4-401 (2002).

83. *Id.*

84. Truth in Lending Act of 1968 § 133, 15 U.S.C. 1643 (2006); Truth in Lending (Regulation Z), 12 C.F.R. § 226.13 (2007).

85. Drew & Nair, *supra* note 47, at 1.

86. *Id.* at 1–2.

87. *Id.*

Note here, however, that the pattern I am describing for data security is very different from the one the CFPB would establish for defining terms. This pattern involves cooperation among a self-regulatory organization, the industry, and the agency. This is the sort of cooperation that might best be accomplished through the OCC or Federal Reserve where the goal is the safety and soundness of the financial system, and protection (for better or worse) of the industry itself. By contrast, where data privacy is involved, such a cooperative relationship is anathema to the function of protecting consumers.

CONCLUSION

As such, and in conclusion, it appears that it may be desirable to split the regulation of data privacy and data security in two. The articulation of data security and data privacy norms might properly be entrusted to the CFPB. An agency focused on consumer protection is in the best position to generate and impose the default terms relating to privacy and security that will find their way into consumer credit and payment contracts. However, the regulation of data protection procedures, and the development of programs for mitigating the harm caused by security breaches would best be handled by the bank regulatory agencies themselves.