The Gramm-Leach-Bliley Act, Information Privacy, and the Limits of Default Rules

Edward J. Janger† & Paul M. Schwartz††

CONTENTS

INTRODUCTION

The Gramm-Leach-Bliley Act (GLB Act) of 1999 removed legal barriers that had existed between different kinds of financial institutions.[1] Where legal walls once blocked mergers among banks, brokerage houses, insurance companies, and other financial entities, the GLB Act permits the creation of

† Associate Professor of Law, Brooklyn Law School.
†† Professor of Law, Brooklyn Law School.

1. Gramm-Leach-Bliley Act of 1999, Pub. L. No. 106-102, 113 Stat. 1338 (1999) (codified in scattered sections of 12 and 15 U.S.C.).

new kinds of "financial supermarkets." This law also sought to provide new rules for financial privacy.[2] To limit the possible negative results of data processing by the financial supermarkets, the GLB Act sought to provide "the most comprehensive federal privacy legislation in history."[3]

Only a few years after the GLB Act's enactment, however, it appears to have failed as far as privacy protection is concerned. The Act has pleased neither privacy advocates nor the financial industry. The Privacy Rights Clearinghouse, for example, has stated of the mandatory privacy notices under the GLB Act, "Industry, government agencies, and consumer education organizations . . . would all do well to view the year 2001 as a costly experiment that resulted in little effective education of the public about the rights to privacy of personal financial information under GLB."[4] This conclusion has been echoed by Federal Trade Commission Chairman Timothy Muris, who summarized the net result of GLB privacy notices in these terms: "Acres of trees died to produce a blizzard of barely comprehensible privacy notices."[5] It may, in fact, be a rare legislative feat to have a single statute create so many diverse critics so quickly.

This Article examines the roots of the unhappiness with the GLB Act. It explores the GLB Act and its shortcomings through reference to and refinement of theoretical work regarding the law of incomplete contracts. The key scholarship concerns information sharing and "defaults," or background rules, for filling gaps in agreements.[6] We explore three possible kinds

2. These protections are found in Title V of the GLB Act. 15 U.S.C. §§ 501-509, 521-527 (2000).

3. L. Richard Fischer & Clarke Dryden Camper, *Reform Law and Privacy: A Road Map*, AM. BANKER, Nov. 19, 1999, at 6.

4. Tena Friery & Beth Givens, *2001: The GLB Odyssey—We're Not There Yet*, *at* http://www.privacyrights.org/ar/fp-glb-ftc.htm (Dec. 4, 2001).

5. Timothy J. Muris, *Protecting Consumers' Privacy: 2002 and Beyond*, *at* http://www.ftc.gov/speeches/muris/privisp1002.htm (Oct. 4, 2001) [hereinafter Muris, *Protecting Privacy*].

6. Privacy scholars have already begun to make use of the concept of default and mandatory rules. *See* Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 STAN. L. REV. 1193, 1246-67 (1998); Richard 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).

of defaults: majoritarian, information forcing, and norm enforcing. Our chief focus is on the GLB Act's requirements of notice plus "opt-out" before data sharing with non-affiliates.[7] As a result of the GLB Act's *opt-out* default, information may be shared with non-affiliates unless consumers, after notice, object to the practice. In contrast, under a privacy *opt-in*, information would not be shared with third parties unless consumers agreed to the practice.

This Article finds that the GLB Act's privacy safeguards are highly problematic as examples of either a majoritarian or information forcing default. The GLB Act also raises difficulties if evaluated as a background rule that seeks to enforce norms. In our judgment, information privacy should be conceptualized as a norm constitutive of a democratic society.[8] The access to personal information and limits on it help form the nature of the society in which we live and shape our individual identities. For example, the structure of access to personal information can have a decisive impact on the extent to which certain actions or expressions of identity are encouraged or discouraged.

Our concept of "constitutive privacy" suggests that information privacy is a kind of commons that requires some degree of social control to construct and preserve. Default rules, when viewed from this normative perspective, should have a limited role in norm enforcement because of the current poor functioning of the privacy market between consumers and financial institutions. In particular, the presence of bounded rationality along with coordination problems makes default rules a risky choice in this context of information privacy. Under such conditions, the law should generally seek to minimize harms that flow from reliance on bargaining among consumers and data processors.

In this Article's final section, we explore a manner in which to make the GLB Act's mandatory rules more flexible, and we propose possible revisions to the existing "notice and opt-out" default in the GLB Act.[9] Mandatory rules can avoid the flaws of command and control regulations through the use of negotiated "safe harbor" agreements between oversight agencies and industry. We look to the Children's Online Privacy Protection

7. *See* Gramm-Leach-Bliley Act § 502(a)-(b). Section (a) deals with notice while section (b) deals with opt-out provisions.

8. *See infra* Part II.B.

9. *See infra* Part II.C.

Act of 1998 as providing a model in this regard.[10] Finally, we revisit the GLB Act's opt-out requirement. We propose to improve upon this requirement by using social science research concerning the power of "frames." We also discuss the possible merits of a shift to an opt-in requirement.

I. THE GRAMM-LEACH-BLILEY ACT

In this Part, we describe the GLB Act in both its non-privacy dimensions and its Title V's privacy-protective aspects. We then explore the current grounds for widespread discontent with the GLB Act's information privacy safeguards.

A. NON-PRIVACY ASPECTS TO THE STATUTE

The GLB Act overturned legal barriers that existed among different kinds of financial institutions. In particular, it repealed essential elements of the Glass-Steagall Act, enacted during the Great Depression, and the later Bank Holding Company Act, first enacted in 1956 and amended significantly in 1982.[11] The Glass-Steagall Act prevented banks that were members of the Federal Reserve System from affiliating with companies that underwrote, sold, or distributed securities. The Bank Holding Act generally blocked a bank from controlling a non-bank company. Amendments to it in 1982 prevented banks from conducting insurance underwriting or insurance agency activities.[12] These statutes erected legal barriers between the commercial banking, securities, and insurance industries.

---

10. Children's Online Privacy Protection Act of 1998, 15 U.S.C. §§ 6501-6506 (2000).

11. The GLB Act repeals sections of the Banking (Glass-Steagall Act) Act of 1933. Gramm-Leach-Bliley Act § 101. The critical sections of the Glass-Steagall Act, sections 20 and 32, restricted banks and security firms from affiliating with each other. Neal R. Pandozzi, *Beware of Banks Bearing Gifts: Gramm-Leach-Bliley and the Constitutionality of Federal Financial Privacy Legislation*, 55 U. MIAMI L. REV. 163, 171 (2001). Section 4 of the Bank Holding Act had generally prevented a bank from controlling a non-bank company without a finding by the Federal Reserve Board of a close relation of the activities of the non-bank company to banking. Gramm-Leach-Bliley Act §§ 102-103; *see also* Pandozzi, *supra*, at 171.

12. *See* Gramm-Leach-Bliley Act §§ 102-103 (amending section 4(c)(8) of the Bank Holding Company Act by adding section 4(k) to it). On the complex relationship of the GLB Act to the typical role of the states in regulating the insurance industry, see Scott A. Sinder, *The Gramm-Leach-Bliley Act and State Regulation of the Business of Insurance—Past, Present and . . . Future?*, 5 N.C. BANKING INST. 49 (2001).

By the end of the 1990s, such limitations were widely considered undesirable.[13] The enactment of the GLB Act in 1999 sought to benefit consumers by enhancing competition in the domestic financial service industries. It also sought to assist U.S. financial service companies by heightening their ability to compete internationally.[14] The GLB Act did so by sweeping away legal restrictions that had prevented mergers among different kinds of financial entities. As one commentator noted, the GLB Act allows the creation of new financial supermarkets that are capable of offering "the consumer one-stop financial shopping."[15] This statute permits banks, securities firms, and insurance companies to combine within a new structure termed a "financial holding company."[16] With enactment of the GLB Act, a wave of mergers began among different kinds of financial service entities—a round of far-reaching corporate consolidations that is still underway.

The GLB Act also responds to information privacy issues. Our initial, process-oriented definition of this term is as follows: Information privacy is the *creation and maintenance of rules that structure and limit access to and use of personal data.*[17] These rules are sometimes found in social norms, such as the idea of limits on sharing information ("gossip") about one

13. Citigroup provides a good example of the kind of financial entity blocked by the legal barriers between different kinds of financial entities. Citigroup was formed by the merger of Citicorp and Travelers Group. As the *Value Line* explains, Citigroup "is a diversified financial services company with operations in consumer and corporate banking, insurance, investment banking, and asset management." *Citigroup,* THE VALUE LINE INVESTMENT SURVEY, 2142 (Nov. 2001). Among Citigroup's businesses are Citibank, Salomon Smith Barney Holdings, CitiFinancial, SSB Citi Asset Management Group, Primerica Financial Services, Travelers Life & Annuity, and Travelers Property Casualty. *Id.* Recently, however, Citigroup has considered a spin-off of the property-casualty part of its insurance operations. *See* Paul Beckett, *Citigroup May Split Off a Travelers Unit, Property-Casualty Division Appears Headed for IPO, Partial Spinoff Next Year*, WALL ST. J., Dec. 19, 2001, at A3.

14. David Constantino, *Developments in Banking Law: 1999 X. Insurance and Annuities*, 19 ANN. REV. BANKING L. 100, 100 ("After failing to pass a similar act last year, Congress acknowledged that passing Gramm-Leach-Bliley was necessary to ensure that the domestic financial services industry remained competitive with foreign financial services industries."). For a general discussion of the Gramm-Leach-Bliley Act, see Pandozzi, *supra* note 11, at 170-71.

15. Pandozzi, *supra* note 11, at 166.

16. Gramm-Leach-Bliley Act § 103 (amending section 4 of the Bank Holding Company Act of 1956, 12 U.S.C. § 1843).

17. For a discussion of this definition, see PAUL M. SCHWARTZ & JOEL R. REIDENBERG, DATA PRIVACY LAW 5-6 (1996).

family member with non-family members.[18] Statutory law, such as the GLB Act, provides another source for information privacy rules.

Before the GLB Act, functional barriers between different companies may have limited some collection and sharing of personal data. In contrast, mergers in the aftermath of the GLB Act necessarily would lead to creation of new kinds of detailed stores of personal information. Anticipating this result of the new financial supermarkets, Congress responded with the privacy protections of the GLB Act's Title V. As a result of Title V, the GLB Act was regarded, at least initially, and at least by some observers, as among the most significant pieces of privacy legislation of the 1990s. During the debates over the statute, one Congressman promised that the GLB Act would "represent the most comprehensive federal privacy protections ever enacted by Congress."[19] Another congressman stated that the Act would "provide some of the strongest privacy provisions to ever be enacted into any federal law."[20] Despite this initial enthusiasm, the GLB Act has already managed to disappoint both industry leaders and privacy advocates alike.

B. THE PRIVACY PROVISIONS OF THE GLB ACT

The GLB Act's privacy provisions have four important aspects. These provisions are briefly stated and then examined in more detail. First, the GLB Act requires that financial entities under its regulation provide annual "privacy notices" that inform their customers of their privacy practices.[21] Second, the GLB Act requires that financial institutions permit consumers to prevent their personal information from being shared with non-affiliated companies.[22] The GLB Act does so through an opt-out requirement.[23] Third, the GLB Act requires financial institutions to develop policies to promote data security.[24]

---

18. In contrast to our view, most norm theorists see privacy as merely an obstacle to norm formation. *See, e.g.*, ROBERT C. ELLICKSON, ORDER WITHOUT LAW 285 (1991) (calling for "improved circulation of accurate reputational information").

19. 145 CONG. REC. H11,544 (daily ed. Nov. 4, 1999) (statement of Rep. Sandlin).

20. *Id.* H11,539-40 (daily ed. Nov. 4, 1999) (statement of Rep. Vento).

21. Gramm-Leach-Bliley Act § 502(a).

22. § 502(b).

23. *Id.*

24. § 501(b).

Fourth, the GLB Act creates a right of enforcement, which it assigns not to individuals, but to different federal agencies, including the Federal Trade Commission, the Board of Governors of the Federal Reserve System, the Office of the Comptroller of the Currency, and the Securities and Exchange Commission.[25]

We begin with the requirement that financial institutions provide "notice" of their information practices. The notice provision is perhaps the most commented upon of the Act's privacy requirements, which is unsurprising due to the mandate's high cost. As an article in the *New York Times* explained, "Financial services companies and their supporters . . . say the notices cost the companies too much."[26] The cost of the privacy notices is directly tied to the magnitude of the required mailings. A single company, Citigroup, mailed more than ninety million privacy notices to its credit card customers.[27] The *New York Times* also mentioned the likelihood of each United States household receiving dozens of privacy notices by the initial GLB Act deadline for notices on July 1, 2001.[28]

The GLB Act's notice requirements in section 503 subsections (a) and (b) address both the *process* by which to provide the notices and their *substance* or content. The process and substance requirements both attempt to ensure that the regulated entities provide "clear and conspicuous" disclosure to each consumer of the institution's policies and practices with regard to the processing of personal data.[29] The idea of notice under the GLB Act is to convey information that is critical to an individual's decisionmaking about the use of her personal data. Thus, section 503(a) requires that privacy notices be provided to a consumer "[a]t the time of establishing a customer relationship . . . and not less than annually during the continuation of such relationship."[30] As a further mandated process element, entities must provide the notices by mail, in electronic

25. § 505.

26. John Schwartz, *Privacy Policy Notices Are Called Too Common and Too Confusing*, N.Y. TIMES, May 7, 2001, at A1. As a reflection of the overall frustration with the notice requirement, the FTC held a workshop on December 4, 2001 to allow discussion of problems with the GLB Act privacy notices. Papers from the workshop are posted at http://www.ftc.gov/bcp/workshops/glb/index.html.

27. Schwartz, *supra* note 26, at A1.

28. *Id.*

29. *See* Gramm-Leach-Bliley Act § 503(a).

30. *Id.*

form, "or other form" as permitted by regulations.[31]

Beyond these process elements, the GLB Act also sets out the required substance of the privacy notices. Section 503(a) of the GLB Act establishes three initial substantive requirements. It calls for notices that explain a financial institution's policies and practices with respect to its (1) disclosure of personal data to affiliates and nonaffiliated third parties; (2) disclosure of personal data of persons who have ceased to be its customers; and (3) protection of personal data of "consumers."[32] The GLB Act broadly defines the term "consumer."[33] Finally, section 503(b) of the GLB Act provides two more elements regarding the substance of the mandated privacy notices. Privacy notices must explain a financial institution's policies and practices with regard to (4) confidentiality "of nonpublic personal information" and (5) categories of personal data collected by the financial institution.[34]

If the core of the GLB Act's requirement concerning notice is that adequate information be provided for individual decisionmaking, the second important aspect of the GLB Act concerns the individual's ability to prevent personal information from being shared with non-affiliated companies. The GLB Act protects this interest through an opt-out requirement.[35] As an initial matter, one must observe that the GLB Act creates no such individual interest regarding the sharing of personal financial data among affiliated entities. In other words, the GLB Act creates no ability for consumers to block data sharing *inside* a financial supermarket. It is for this reason that the Privacy Rights Clearinghouse continues to advise those concerned

31. *Id.*

32. § 503(a)(1)-(3).

33. The term "'consumer' means an individual who obtains, from a financial institution, financial products or services which are to be used primarily for personal, family, or household purposes, and also means the legal representative of such an individual." § 509(9). The rights of consumers to disclosures regarding the information practices are triggered when a consumer becomes a "customer," § 503(a), and some obligations continue after a "person" has stopped being a "customer."

34. § 503(b). The form of these notices is to be further specified in regulations issued by the GLB Act oversight agencies. § 503(a). The FTC has already issued its regulations regarding the GLB Act. FTC Privacy of Consumer Financial Information Final Rule, 16 C.F.R. § 313 (2001). These regulations and those of other GLB oversight agencies were upheld against various challenges in *Individual Reference Services Group v. FTC*, 145 F. Supp. 2d 6, 46 (D. D.C. 2001).

35. Gramm-Leach-Bliley Act § 502(b).

about their privacy to consider maintaining different accounts with different companies.[36]

When information is to be shared *outside* the financial entity, however, the GLB Act offers more choices to the individual. It requires that customers of the financial entity be informed of this practice and "given the opportunity, before the time that such information is initially disclosed, to direct that such information not be disclosed to such third party."[37] The mandated privacy notices discussed above are to inform individuals both of planned data sharing with non-affiliates and their ability to refuse these data transfers.[38]

Thus, the GLB Act sets an *opt-out* privacy default. Information may be shared with non-affiliates unless consumers, after notice, object to the practice. In contrast, the Clinton Administration backed a financial privacy bill that would have altered this aspect of the GLB Act for one subset of information.[39] The Clinton proposal would have prevented financial institutions from sharing health information among affiliated firms or third parties unless consumers explicitly agreed to this practice.[40] Here, the default would have been set as a privacy *opt-in*—information would not be shared with third parties unless consumers agreed to the practice.

A privacy opt-in does exist, however, for personal financial information in Vermont. The GLB Act generally allows states to offer more stringent privacy protections; its standards serve as a floor, not as a ceiling.[41] Vermont is now attempting to make use of the GLB Act's statutory opening for states. In

36. As the Clearinghouse summarizes: "So, if you are concerned about affiliate sharing and the ability of these 'financial supermarkets' to compile extensive dossiers about you, you must take extra care to conduct your banking with one corporation, keep your insurance accounts with another unaffiliated corporation, and your investments with yet another." Privacy Rights Clearinghouse, *Fact Sheet 24: Protecting Financial Privacy*, *at* http://www.privacyrights.org/fs/fs24-finpriv.htm (Sept. 2001) [hereinafter *Fact Sheet 24*].

37. Gramm-Leach-Bliley Act § 502(b)(1)(B).

38. § 502(b).

39. Consumer Financial Privacy Act, H.R. 4380, 106th Cong. (2000). For details on the Clinton Administration's views regarding financial privacy, see White House, *Proclamation: Plan to Enhance Consumers' Financial Privacy*, *at* http://clinton4.nara.gov/WH/New/html/20000501_4.html (May 1, 2000).

40. H.R. 4380, § 3(b)(2). This bill also required that an opt-out be provided before financial institutions shared data with both affiliated and non-affiliated parties. § 2(a).

41. Gramm-Leach-Bliley Act § 507(b).

February 2002, Elizabeth Costle, the Vermont Commissioner of Banking, Insurance, Securities, and Health Care Administration, issued regulations that require affirmative customer consent before information may be shared with non-affiliated parties.[42] These regulations are now under legal attack;[43] should the Vermont approach be upheld in court, it will offer useful evidence in answering some of the questions regarding the merits of opt-in versus opt-out. We explore this issue in more detail later in this Article.

To return to the GLB Act, beyond its provision allowing limited individual "choice" through an opt-out requirement, the Act generally lacks substantive restrictions regarding transfers of information by a financial institution, whether to affiliated or non-affiliated companies.[44] All told then, the success of the statutory provisions concerning the sharing of personal information with non-affiliated third parties will likely turn on the effectiveness of (1) privacy notices in actually conveying information reasonably designed to promote the exercise of choice and (2) opt-out in actually providing a mechanism reasonably designed to promote the exercise of choice. We return to these important points later.

Beyond notice and choice, the third aspect of the GLB Act requires financial institutions to develop policies to prevent

---

42. Privacy of Consumer Financial and Health Information Regulation, VT. CODE R. 21 020 053 Reg. IH-2001-01 (2002). For background on the regulation, see State of Vermont, Dep't of Banking, Ins., Sec. & Health Care Admin., Banking Div., *In Wake of Federal Law, Vermont Passes Own Stricter Financial Privacy Regulations*, *at* http://www.bishca.state.vt.us/news_releases/FinancialPrivacyRegs.htm (Nov. 2001) [hereinafter *Vermont Privacy Regulations*].

As an international example, Canada has adopted an opt-in regime for financial information. *See* Michael Geist, *Canadian Privacy Law's Ins and Outs*, THE GLOBE AND MAIL, April 4, 2002, at B13 ("Financial or health data, for example, are generally viewed as highly sensitive, and thus require opt-in consent [under Canadian privacy law]."), *available at* http://www.globeandmail.com/servlet/ArticleNews/printarticle/gam/20020404/TWGEISY.

43. Patrick Thiboudeau, *New Vermont 'Opt-in' Privacy Law Faces Legal Challenge*, COMPUTERWORLD, http://www.computerworld.com/storyba/0,4125,NAV47_STO68104,00.html (Feb. 7, 2002).

44. In one substantive restriction regarding transfers, the GLB Act prevents financial institutions from disclosing an individual's account number or access code to a non-affiliated company for use in telemarketing, direct mail marketing, or marketing through e-mail to the consumer. Gramm-Leach-Bliley Act § 502(d). A financial institution, however, can still disclose personal data to these parties—the GLB Act prevents it only from disclosing the *means* by which one's account can be accessed.

fraudulent access to confidential financial information. This aspect of the GLB Act addresses the distinct issues of data security. Data security involves a cluster of concerns, including the prevention of unauthorized access to personal information and the processing of only accurate personal information.

The GLB Act spells out three requirements for data security. It calls for financial institutions to (1) protect the security and confidentiality of customer records and information; (2) prevent any anticipated threats or hazards to the security or integrity of such records; and (3) prevent unauthorized access to use of records that could result in "substantial harm or inconvenience to any customer."[45] The question of unauthorized access to records is further addressed in a section of Title V concerning "pretexting" or the obtaining of customer information by false pretenses.[46] One way that pretexting occurs is when false statements are made to an employee of a financial institution. As Timothy Muris, the Chairman of the FTC, has explained, "[f]or a price, some so-called 'information brokers' call banks and other financial institutions under the 'pretext' of being a customer to obtain the customer's account numbers and balances, as well as other personal information."[47] Among the priorities that Muris has announced as part of the FTC's new "ambitious, positive, pro-privacy agenda" is an increase in the agency's prosecutions of pretexting.[48]

Finally, the fourth critical aspect of the GLB Act concerns its assignment of an enforcement right, not to individuals, but to seven different federal agencies, including the Federal Trade Commission, Federal Reserve, and Securities and Exchange Commission.[49] The enforcement powers of these "GLB oversight agencies" include assessing criminal penalties.[50] In "aggravated cases," the penalties allow doubling of statutory fines and imprisonment for up to ten years.[51] The GLB Act also permits the oversight agencies to exercise "for the purpose of enforcing compliance . . . any other authority conferred on such

45. § 501(b)(1)-(3). The Act also requires the GLB Act oversight agencies to establish "appropriate standards" for data security and integrity. § 501(b). For a discussion of this provision, see *infra* Part II.C.

46. Gramm-Leach-Bliley Act § 521 Subtit. B.

47. Muris, *Protecting Privacy*, *supra* note 5.

48. *Id.* Muris has also called for the FTC to increase its resources devoted to protecting privacy by fifty percent. *Id.*

49. Gramm-Leach-Bliley Act § 505.

50. § 523.

51. § 523(b).

agency by law."[52] Thus, the FTC in enforcing the GLB Act can use its traditional injunctive power and order parties to "cease and desist" from prohibited behavior.[53] As a final matter regarding enforcement, the FTC and the Attorney General are required to submit to Congress an annual report on the number and disposition of any enforcement actions taken pursuant to the GLB Act.[54] This requirement will increase the visibility of enforcement actions carried out by the GLB Act oversight agencies.

C. UNHAPPINESS WITH THE GLB ACT

The GLB Act has managed to disappoint both industry leaders and privacy advocates alike. Why are so many observers currently frustrated with the GLB Act? We have already noted the complaint of financial services companies regarding the expense of privacy notices. These organizations also argue that there has been scant pay-off from the costly mailings—and strong evidence backs up this claim. For example, a survey from the American Banker's Association found that 22% of banking customers said that they received a privacy notice but did not read it, and 41% could not even recall receiving a notice.[55] Another survey found only 0.5% of banking customers had exercised their opt-out rights.[56]

Privacy advocates also have complaints about the GLB Act. Their objections begin with the lack of comprehensibility of some of the GLB Act notices. As we have noted, the GLB Act requires privacy notices and the disclosure of opt-out to be made "clearly and conspicuously."[57] A readability study of pri-

52. § 522(b)(2).

53. *See* Federal Trade Commission Act, 15 U.S.C. § 45(g) (2000). For a news report on a FTC enforcement action in a different context of privacy, see Daniel Golden, *FTC Investigates Group that Sells Student Data*, WALL ST. J., Dec. 11, 2001, at B1. According to this report, the FTC is now investigating the National Research Center for College and University Admissions, an organization that helps school recruiters find promising students. *Id.* This organization also is said to have supplied the names and other personal information of high school students to commercial marketers and made only vague disclosures to students about how their data would be used. *Id.*

54. Gramm-Leach-Bliley Act § 526(b).

55. *ABA Survey Shows Nearly One Out of Three Consumers Read Their Banks' Privacy Notices*, *at* http://www.aba.com/press+room/bankfee060701.htm (June 15, 2001).

56. John Martin, *Opting Out—or Not*, *at* http://more.abcnews.go.com/sections/wnt/dailynews/privacy_notices_010621.html (June 21, 2001).

57. Gramm-Leach-Bliley Act § 502(b)(1)(A).

vacy notices, however, by Mark Hochhauser for the Privacy Rights Clearinghouse, found these notices to be often difficult to understand.[58] Hochhauser found that, on average, the GLB Act privacy notices were written at a third or fourth year college reading level.[59] Literacy experts generally recommend that documents intended for the general public be written at a junior high school level.[60] As Hochhauser argues, "Consumers will have a hard time understanding the notices because the writing style uses too many complicated sentences and too many uncommon words."[61] The Privacy Rights Clearinghouse made a related finding concerning the failings of the GLB Act notices when it analyzed the consumer contacts it had received about the Act.[62] In the judgment of this organization, only about 10% of the individuals that contacted it for help regarding financial privacy under the GLB Act showed anything approaching a high level of understanding about privacy notices.[63] Indeed, most consumers that contacted this organization had been alerted to privacy protections under the GLB Act by media reports and not by the numerous privacy notices that they had received.[64] In many cases, individuals had simply assumed that these forms were additional telemarketing offers from financial institutions and neglected to read the privacy notices.[65]

Not only are privacy notices difficult to understand, but they are written in a fashion that makes it hard to exercise the opt-out rights that the GLB Act mandates. For example, opt-out provisions are sometimes buried in privacy notices. As the Public Citizen Litigation Group has found, "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 . . . ."[66] Public Citizen also

58. Mark Hochhauser, *Lost in the Fine Print: Readability of Financial Privacy Notices*, *at* http://www.privacyrights.org/ar/GLB-Reading.htm (July 2001).

59. *Id.*

60. *Id.*

61. *Id.*

62. Tena Friery & Beth Givens, *2001: The GLB Odyssey—We're Not There Yet: How Consumers Responded to Financial Privacy Notices and Recommendations for Improving Them*, *at* http://www.privacy rights.org/ar/fp-glb-ftc.htm (Dec. 4, 2001).

63. *Id.*

64. *Id.*

65. *Id.*

66. Public Citizen Litigation Group, *Petition for Rulemaking* 5,

identified many passages regarding opt-out that "are obviously designed to discourage consumers from exercising their rights under the statute."[67] For example, some financial institutions include an opt-out box only "in a thicket of misleading statements . . . ."[68] 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."[69]

As Public Citizen concludes regarding the GLB Act privacy notices, "[i]t seems that these notices were written by lawyers trained in the art of obfuscation, not by communication experts trained to express ideas clearly."[70] Another explanation is possible: Later in this Article, we argue that the GLB Act notices can "frame" options, so as to discourage or encourage opting out.[71] We make this argument with reference to the social science literature regarding "framing effects." Specifically, we suggest that GLB Act notices are currently being designed to discourage opting out. Before reaching this argument, however, we wish first to consider and refine existing theoretical work about information sharing and "defaults" (or background rules) for filling gaps in agreements. In our view, this scholarship can help us understand where the GLB Act went wrong—and how it might be set right.

II. INCOMPLETE CONTRACTS AND NORM ENFORCING DEFAULTS

The GLB Act provides default terms for the use of personal data by financial institutions. By "default terms," we mean the background rules that govern an agreement unless individual action is taken to customize the terms. As Ian Ayres and Robert Gertner explain, "[d]efault rules fill the gaps in incomplete contracts; they govern unless the parties contract around them."[72] In this Part, we begin by looking at three characteris-

---

http://www.epic.org/privacy/consumer/glbpetition.pdf (July 26, 2001).

67. *Id.*

68. *Id.*

69. *Id.* at 5-6.

70. *Id.* at 4.

71. *See infra* Part II.A.

72. Ian Ayres & Robert Gertner, *Filling Gaps in Incomplete Contracts: An Economic Theory of Default Rules*, 99 YALE L.J. 87, 87 (1989) [hereinafter Ayres & Gertner, *Filling Gaps*]; *see also* Ian Ayres & Robert Gertner, *Majori-*

tics of default rules. We present these aspects of default rules as distinct, ideal types, although in practice a default rule may have more or less of these different characteristics. In our view, default rules can be majoritarian, information forcing, and norm enforcing.[73]

After defining and exploring each of these default rules in Section A below, we conclude that the GLB Act does not create successful majoritarian or information forcing defaults. As for norm enforcing defaults, the extent to which a background rule actually encourages certain behavior can only be evaluated once an underlying normative function is specified. What then should be the normative role of an information privacy law, such as the GLB Act's Title V? We turn to this question in section B of this Part. Finally, Section C concludes by proposing possible improvements to existing mandatory opt-out default rules in the GLB Act.

A. MAJORITARIAN DEFAULTS, INFORMATION FORCING DEFAULTS AND BEHAVIOR FORCING DEFAULTS

This section examines the law of incomplete contracts. This area of law is of particular interest to us because prior to the GLB Act parties involved in most consumer relationships with financial institutions did not explicitly negotiate regarding information privacy. Where gaps might once have existed, the GLB Act has now spoken and provided rules for information privacy. The question remains, however, as to the nature of its gap closing terms.

The law of incomplete contracts recognizes that parties to a broad range of ordinary commercial transactions cannot be expected to specify the terms of their agreement in full and com-

---

tarian vs. Minoritarian Defaults, 51 STAN. L. REV. 1591 (1999); Ian Ayres & Robert Gertner, *Strategic Contractual Inefficiency and the Optimal Choice of Legal Rules*, 101 YALE L.J. 729 (1992).

73. On majoritarian default terms, see Ayres & Gertner, *Filling Gaps*, *supra* note 72, at 89 ("Few academics have gone beyond one-sentence theories stipulating that default terms should be set at what the parties would have wanted."). Regarding information forcing defaults, Ayres and Gertner state that these defaults

> are designed to give at least one party to the contract an incentive to contract around the default rule and therefore to choose affirmatively the contract provision they prefer. In contrast to the received wisdom, penalty defaults are purposefully set at what the parties would not want—in order to encourage the parties to reveal information to each other or to third parties (especially the courts).

Id. at 91. The term "norm enforcing default" is our own.

plete fashion.[74] When a consumer purchases a candy bar from a convenience store, for example, the law does not expect her to bargain with the seller over contingencies such as her unexpected dislike for the brand of candy or the chocolate turning out to be an inedible lump. Indeed, the law accepts that parties will not be foresighted even in complex contracting arrangements among sophisticated parties.[75] Try as they might, even

74. Douglas G. Baird & Thomas H. Jackson, *Fraudulent Conveyance Law and Its Proper Domain*, 38 VAND. L. REV. 829, 835-36 (1985) ("[Default rules] should provide all the parties with the type of contract that they would have agreed to if they had had the time and money to bargain over all aspects of their deal."); *see also* Charles J. Goetz & Robert Scott, *The Mitigation Principle: Toward a General Theory of Contractual Obligation*, 69 VA. L. REV. 967, 971 (1983) ("Ideally, the preformulated rules supplied by the state should mimic the agreements contracting parties would reach were they costlessly to bargain out each detail of the transaction.").

75. The law of sales provides off the shelf warranties. *See* U.C.C. §§ 2-313 (1989) (express warranties), 2-314 (implied warranty of merchantability), 2-315 (implied warranty of fitness for a particular purpose). The law of sales also provides for remedies that determine, for example, what will happen if the chocolate proves inedible. *See* U.C.C. § 2-714 (1989). Note that even for sophisticated parties single transactions involving small sums of money may not merit the expense of generating a fully specified agreement. Moreover, sophisticated parties may recognize that limitations on foresight may lead them to use open-ended defaults to align incentives *ex post*. *See, e.g.*, Gillian K. Hadfield, *Judicial Comptence and the Interpretation of Incomplete Contracts*, 23 J. LEGAL STUD. 159, 166 (1994).

One context where the debate about the capacity of parties to specify obligations *ex ante* has been hotly contested is in the literature on "contract bankruptcy." One group of scholars argues that bankruptcy law should be treated as a waivable default term. *See* Barry E. Adler, *Financial and Political Theories of American Corporate Bankruptcy*, 45 STAN. L. REV. 311, 313–14 (1993) ("Bankruptcy's solution to the common pool problem, however, rests on a faulty premise: that there *is* a common pool problem. . . . In theory, each creditor could appoint management as its agent to enforce a mutual and irrevocable agreement among creditors to accept only a collective default remedy."); Barry E. Adler, *A World Without Debt*, 72 WASH. U. L.Q. 811, 816–18 (1994) ("[I]n principle, a world without debt or bankruptcy, and with contractual solutions to the collective action problem, seems an efficient world."); Michael Bradley & Michael Rosenzweig, *The Untenable Case for Chapter 11*, 101 YALE L.J. 1043, 1078–79 (1992) ("Chapter 11 should be repealed, abolishing court-supervised corporate reorganizations and, in effect, precluding residual claimants from participating in any reorganization of the firm."); Robert K. Rasmussen, *Debtor's Choice: A Menu Approach to Corporate Bankruptcy*, 71 TEX. L. REV. 51, 53–54 (1992) ("Contrary to the prevailing wisdom, this Article argues that bankruptcy law should be treated as a default rule."); Alan Schwartz, *Bankruptcy Contracting Reviewed*, 109 YALE L.J. 343, 363 (1999) (arguing that bankruptcy law should be the default rule); Alan Schwartz, *A Contract Theory Approach to Business Bankruptcy*, 107 YALE L.J. 1807, 1821–22 (1998) (advocating the *ex ante* perspective).

Other scholars argue that Bankruptcy Code protection should be non-

sophisticated individuals will not be able to draft contractual terms that cover every possible eventuality. Indeed, the economics of many transactions make customized bargaining inefficient. For example, the consumer buying the candy bar is rationally more likely to opt for the shortest possible waiting time before her chocolate experience rather than negotiating an explicit agreement concerning all aspects of the sale in question. It may be efficient to not spend any time on the terms of contracts concerning a wide variety of matters.[76]

---

waivable. *See* Susan Block-Lieb, *The Logic and Limits of Contract Bankruptcy*, 2001 U. ILL. L. REV. 503, 508 (2001); Lynn M. LoPucki, *Contract Bankruptcy: A Reply to Alan Schwartz*, 109 YALE L.J. 317, 342 (1999). It is striking, however, that scholars on both sides of the debate agree that federal bankruptcy law should remain available as a default where the parties choose not to generate a customized insolvency regime.

76. Contract scholars have noted that one of the benefits of standardized contracts is to provide so-called "network externalities." Marcel Kahan & Michael Klausner, *Standardization and Innovation in Corporate Contracting (or "The Economics of Boilerplate")*, 83 VA. L. REV. 713, 760 (1997); Michael Klausner, *Corporations, Corporate Law, and Networks of Contracts*, 81 VA. L. REV. 757, 763-64 (1995). Network externalities arise when one contracting party invests time and effort into figuring out how to accomplish a complex transaction. Once a set of forms exists, the second deal is much less costly to do than the first. The first deal will have a positive external effect by reducing the cost of doing similar deals for all subsequent parties. To the extent that the first party is a repeat player, it may capture some of the benefit, but the benefit also extends to other members of the contracting network.

Edward Rubin recognizes that contractual default rules can provide the same network externality as that provided by form contracts. *See* Edward L. Rubin, *Types of Contracts, Interventions of Law*, 45 WAYNE L. REV. 1903, 1919-20 (2000) ("[T]he optimal level of standardization for adaptable contracts might not be produced by the market, and that legal intervention might secure the use of standard forms more reliably than the market does.").

Duncan Kennedy takes a different approach to explaining consumers' failure to engage in scrutiny of standardized contracts. He writes,

> [C]onsumers have only limited knowledge of the probabilities that apply to them at the time of making the contract. There are many other unexpected disasters that might also afflict them, and they may *rationally* decide that spending even a little time on the terms of legal protection from each would be a waste of effort. Assume that buyers also suspect that sellers in general tend to lie about the contract terms they offer, and that even when they have legally assumed an obligation to buyers, they tend to resist honoring it if it falls due, so that the consumer may have to pay more in legal fees than the value of the injury if he wants to enforce a contract clause covering anything less than a major catastrophe.

Duncan Kennedy, *Distributive and Paternalist Motives in Contract and Tort Law with Special Reference to Compulsory Terms and Unequal Bargaining Power*, 41 MD. L. REV. 563, 599-601 (1982). In Kennedy's view, it will be rational for consumers simply to ignore contractual terms. *Id.* at 603. As a result, Kennedy ends with the same view as those who argue in favor of "net-

Fortunately, contractual default rules come to the rescue where parties to a contract fail to specify a term.[77] Contract law scholarship speaks of both majoritarian defaults and information forcing defaults. Later in this Article, we develop the concept of a "norm enforcing" default, but we begin with these two other terms. A *majoritarian default* seeks to approximate the term most parties would have agreed to had they taken the time to bargain. Majoritarian default rules are quite common in commercial law. When Karl Llewellyn drafted the Uniform Commercial Code (U.C.C.), he expressly sought to adopt defaults that ratified existing commercial practice.[78] Indeed, the U.C.C. expressly provides for majoritarian defaults in section 1-205, which requires courts to fill gaps in the express terms of contracts by drawing on course of performance, course of dealing, and usage of trade. Perhaps more importantly, U.C.C. section 2-208 requires courts to use commercial practice to explicate express terms of contracts should they prove ambiguous. These sections of the U.C.C. put courts squarely in the role of interpreting contracts in terms of the hypothetical majoritarian bargain whenever gaps or ambiguities appear.[79]

To identify the GLB Act as drawing on majoritarian defaults, one might attempt to demonstrate that most individuals

---

work externalities": It can be desirable for the law to provide compulsory terms for contracts. *Id.* at 597.

77. *Cf.* Rubin, *supra* note 76, at 1914-16.

78. Robert E. Scott, *Is Article 2 the Best We Can Do?*, 52 HASTINGS L.J. 677, 685 n.26 (2001) ("Llewellyn believed that a major purpose of the Code was to resolve disputes according to the 'best' commercial norms. In his view, the task of the courts was to identify and select the best commercial prototypes that were revealed in a particular commercial environment.").

79. This so-called "incorporation strategy" has been the subject of heated debate among commercial scholars. *Compare* Jody S. Kraus & Steven D. Walt, *In Defense of the Incorporation Strategy*, *in* THE JURISPRUDENTIAL FOUNDATIONS OF CORPORATE AND COMMERCIAL LAW 193, 193 (Cambridge Univ. Press 2000), *with* Robert E. Scott, *The Case for Formalism in Relational Contract*, 94 NW. U. L. REV. 847, 871-74 (2000), *and* Lisa Bernstein, *The Questionable Empirical Basis of Article 2's Incorporation Strategy: A Preliminary Study*, 66 U. CHI. L. REV. 710, 714-15 (1999). Bernstein notes,

> The debates surrounding these codification efforts suggest that there was not widespread agreement among merchants as to either the meaning of common terms of trade or the content of many basic commercial practices. Rules committee debates sometimes went on for years, customs relating to important aspects of transactions were left uncodified because consensus could not be achieved, and in most industries drafting committees eventually engaged in only selective codification.

Id. at 714-15.

would in fact bargain for its terms. This approach to majoritarian defaults views the topic as an empirical matter. Either most consumers would want the default terms of the GLB Act, or they would not. This path requires answering questions regarding whether most individuals desire (1) privacy notices; (2) an opt-out obligation before data sharing with non-affiliated parties; (3) an inability to block data sharing with affiliated entities; or (4) an absence of any private right of action should their interests be violated.

As a further twist, we should also point out that the requirement of sending privacy notices under the GLB Act is not, strictly speaking, a "default" in the terminology of the law of incomplete contracts. Rather, the GLB Act creates an "immutable" rule for privacy notices—a mandatory obligation that the parties cannot change.[80] Customers of a financial institution are to be supplied with privacy notices on a yearly basis; the customers and the financial entity cannot negotiate around this requirement.[81] Although it cannot be changed, this immutable rule might still reach a majoritarian result. So, once again, we might decide to approach this matter as a simple empirical question.

A flight to empiricism is not unproblematic. In drafting the GLB Act, Congress does not appear to have engaged in empirical research or drawn upon an outside body of findings regarding majoritarian wishes.[82] Additionally, the GLB Act, whether through its defaults or its mandatory rules, does not appear to have reached de facto majoritarian results. One can plausibly argue, for example, that most customers, at least as the privacy market is currently constituted, (1) would *not* demand privacy notices; (2) would want an opt-in, or affirmative consent, before data sharing among non-affiliates; (3) would

80. *See generally* Ayres & Gertner, *Filling Gaps*, *supra* note 72, at 88 (discussing the origins and basis for immutable rules); John C. Coffee, Jr., *The Mandatory/Enabling Balance in Corporate Law: An Essay on the Judicial Role*, 89 COLUM. L. REV. 1618, 1624 (1989) (discussing mandatory fiduciary duties); Jeffrey N. Gordon, *The Mandatory Structure of Corporate Law*, 89 COLUM. L. REV. 1549, 1555-85 (1989) (describing the role that mandatory rules play in a contractual system).

81. Gramm-Leach-Bliley Act of 1999, Pub. L. No. 106-102, § 502, 113 Stat. 1338 (1999) (codified in scattered sections of 12 and 15 U.S.C.). For the FTC's rule regarding § 502 of the GLB Act, see FTC Privacy of Consumer Financial Information Final Rule, 16 C.F.R. § 313.5(a)(1) (2001).

82. *Financial Privacy: Hearings on H.R. 10 the Financial Services Act of 1999, Before the Subcomm. on Fin. Inst. and Consumer Credit, Comm. on Banking and Fin. Serv.*, H.R. 106-32, 106th Cong. (1999).

want to be able to block data sharing even among *affiliated* entities; and (4) would want to have a private right of action against financial entities for violation of their privacy interests.[83] The GLB Act supplies the first rule (which consumers arguably do not want) and does not reach the second, third, or fourth outcomes (which consumers arguably desire). These results appear counter-majoritarian.

The presence or absence of majoritarian defaults in the GLB Act may therefore seem to turn on a simple issue—does the GLB Act reflect majoritarian desires? At this point, we wish to refine this question and our analysis because majority wishes regarding contractual defaults (or mandatory contractual elements) can be quite intractable. Empiricism is, as it turns out, an elusive matter when it comes to contractual majoritarianism.

As Richard Craswell has persuasively argued, majoritarian defaults are difficult to derive from empirical data.[84] Craswell has identified a number of "difficulties involved in interpreting the sociological data about a society's practices."[85] He has pointed to issues regarding "the number of people who must follow any set of rules for those rules to be accepted as a legally relevant practice"; "the problem of conflicting expectations at different levels of generality"; and "the potential for circularity that arises when people's expectations are themselves affected by existing legal rules."[86] The last point is of particular impor-

83. The polling data is incomplete, but suggestive. Thus, the newsletter *Privacy Times* has reported on a survey that found 57% of respondents "very" or "somewhat" concerned that their "primary financial institution" was sharing "their personal or financial data with its partners or third parties." *Not-So-Private Banking*, Privacy Times, Jan. 7, 2002, at 3. The survey was sponsored by Star Systems, Inc., an ATM company. More specifically, the poll found an even higher percentage (62%) concerned that their financial institution was sharing information with "affiliated companies." *Id.* at 3-4. This percentage of concerned consumers even exceeded those who were concerned about data sharing with "government agencies" (59%). *Id.*

Another survey focused solely on Californians. This survey, sponsored by E-Loan, an online lender, "found that 66% of respondents favored an opt-in [approach to financial privacy] bill, 8% favored opt-out, 13% preferred neither and 6% didn't know." 22 Privacy Times, *Poll: Californians Want Speier Bill*, Feb. 27, 2002, at 6. In addition, 80% of respondents said that they were "not at all comfortable" with financial institutions selling their data to other financial firms. *Id.* at 7.

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

85. *Id.* at 506.

86. *Id.* at 506-07.

tance in the area of information privacy. Prior to the GLB Act, individual financial privacy expectations, to the extent that they were at all formed, could only be based on existing law, including judicial decisions, and the practices imposed upon consumers by financial institutions. The circularity that Craswell warns about arises if these expectations are used to set majoritarian defaults.

A second approach to contract defaults is the idea of *information forcing* defaults. These are also known as "penalty defaults" for reasons that will become evident shortly. As developed by Ian Ayres and Robert Gertner, such defaults are to be a helpful response to information asymmetries. The idea is to "inform the relatively uninformed contracting party" by setting a penalty as a default against the better informed party.[87] Through this penalizing effect, information forcing defaults are intended to obligate the party with better information to disclose it and thereby encourage parties to bargain about the terms. These default rules are by definition non-majoritarian; it is expected that parties will frequently, if not inevitably, alter the default. The key is that the information default disfavors the party with better information.

As an example of an information forcing default, Ayres and Gertner point to the treatment of real estate brokerage commissions for a buyer breaching a purchase contract.[88] The applicable contracts typically include a clause obligating the purchaser to forfeit a specific amount of "earnest" money if she breaches the agreement. If the contract is silent on how to divide this money between the real estate broker and the seller, Ayres and Gertner propose that the default rule be set in favor of the uninformed party, who is likely to be the seller. As a result, in the case of buyer breach, the earnest money should go to the seller, not the real estate broker. This default rule prevents the broker from taking advantage of a seller's ignorance by setting the information forcing default as a *penalty* for the better informed party. Ayres and Gertner conclude that "[t]he real estate broker will more likely be informed about the default rule than the seller. Indeed, the seller may not even consider the issue of how to split the earnest money in case of default."[89]

87. Ayres & Gertner, *Filling Gaps*, *supra* note 72, at 98.
88. *Id.* at 98-99.
89. *Id.* at 99.

Before we return to the GLB Act, we wish to consider a further information problem, that of the "lemons equilibrium."[90] Problems with information can be systematic enough to skew an entire class of negotiations—a lesson already found in the previous example involving the earnest money and real estate broker. A lemons equilibrium occurs when one party has good information about price but bad information about non-price terms. For example, the seller of real estate may understand the commission that a broker receives but comprehend little about who receives earnest money following a purchaser's breach. As another example, lemons equilibria typically occur with used automobiles, where buyers face high transaction costs in gathering information about the most critical non-price information: whether the car is in good condition.[91]

The danger is that these information asymmetries will become entrenched. Richard Craswell explains the difficulty in overcoming a lemons equilibrium as follows:

> 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.[92]

Once a sufficiently large number of buyers cease purchasing, the seller will lose money as a result of her decision to offer more favorable terms at a higher price. Craswell concludes, "In that case, no seller has an incentive to offer the more favorable terms, and the result is an equilibrium in which only bad contract terms (or "lemons") can be obtained."[93] Craswell's parenthetical allusion to lemons suggests an unfortunate consequence when buyers and sellers are unable to signal the presence of a good product. In a lemons equilibrium, either bad

90. *See, e.g.*, George A. Akerlof, *The Market for "Lemons": Quality Uncertainty and the Market Mechanism*, 84 Q.J. ECON. 488, 489-90 (1970); Michael Spence, *Consumer Misperceptions, Product Failure and Producer Liability*, 44 REV. ECON. STUD. 561, 561 (1977).

91. As Cooter and Ulen state, "[I]t is often the case that sellers know more about the quality of goods than do buyers. For example, a person who offers his car for sale knows far more about its quirks than does a potential buyer." ROBERT COOTER & THOMAS ULEN, LAW AND ECONOMICS 41 (2d ed. 1997).

92. Richard Craswell, *Property Rules and Liability Rules in Unconscionability and Related Doctrines*, 60 U. CHI. L. REV. 1, 49 (1993).

93. *Id.*

products ("lemons") are offered for sale or bad contract terms are presented.[94]

To return to the GLB Act, does this statute successfully respond to information asymmetries, as Ayres and Gertner suggest, or to a lemons equilibrium in the privacy market? Interestingly, the GLB Act does have information forcing elements. It requires financial entities, the party with superior knowledge about the value of personal information and how it will be used, to mail privacy notices and to give individuals an opportunity to opt-out before their personal data can be shared with non-affiliated entities. Thus, the GLB Act obligates the relatively better informed parties (financial institutions) to share information with the other parties. While the GLB Act requires disclosure of information, it does not penalize the better informed parties and thereby is unlikely to encourage bargaining.

The GLB Act merely contains an opt-out requirement. As a result, information can be disclosed to non-affiliated entities unless individuals take affirmative action, namely, informing the financial entity that they refuse to share their personal data. By setting its default as an opt-out, the GLB Act fails to create any penalty on the party with superior knowledge, here the financial entity, should negotiations fail to occur. In other words, the GLB Act leaves the burden of bargaining on the less informed party, the individual consumer. These doubts about the efficacy of opt-out are supported, at least indirectly, by the evidence concerning sometimes confusing and sometimes misleading privacy notices.[95] An opt-out default creates incentives for privacy notices that lead to *inaction* by the consumer.

What then of a lemons equilibrium in the privacy market with financial institutions? In financial transactions, the consumer generally does have good information about price (such as the cost of a checking account) but bad information about non-price terms (such as the rules for information privacy). These are fertile conditions for a lemons equilibrium. Further, the current privacy market does not appear to have led financial entities to compete in offering better privacy terms. Finally, consumers today certainly would be hard pressed, amidst the clutter of confusing privacy notices, to observe any improvement in non-price terms involving personal data use. In

94. Information forcing defaults, if imposed on a class-wide basis, are intended to force a group of sellers to disclose information about non-price terms.

95. *See supra* Part I.

part, there seem to be major coordination problems among individuals—"[a]s members of large consumer blocks, individuals may have difficulty finding effective ways to express collectively their relative preferences for privacy."[96] Moreover, competition may not arise among financial service companies regarding finding more effective means to satisfy consumer preferences for privacy. A lemons equilibrium appears to exist between financial institutions and consumers.

Thus far, we have argued that the information forcing aspects of the GLB Act have proven insufficient to help the less informed party, the individual consumer, bargain for better privacy. As a final matter, we wish to note a more general difficulty with information forcing mechanisms, such as found in the GLB Act, as a means for overcoming knowledge asymmetries in a privacy market. The problem is simply stated: More information alone may fail to induce consumers to bargain for information privacy. In making this point, we wish to draw on findings by social scientists that point to the limited, or "bounded," nature of consumer rationality. In particular, these findings reveal that the parties who shape the form of offers have strong power over subsequent decisionmaking by consumers.

This power flows from the "framing effect" on decisionmaking.[97] A "framing effect" refers to the manner in which the presentation of options influences choice.[98] As Daniel Kahneman and Amos Tversky summarize, these "[f]ormulation effects can occur fortuitously, without anyone being aware of the impact of the frame on the ultimate decision. They can also be exploited deliberately to manipulate the relative attractiveness of options."[99] Since financial institutions draft the GLB Act

96. Schwartz, *Privacy Economics*, *supra* note 6, at 50-51. For a discussion of similar coordination problems in the context of health care privacy, see *id.*

97. A framing effect occurs when "the very same choice can be perceived as a gain or a loss based purely on its formal presentation." Edward J. McCaffery et al., *Framing the Jury: Cognitive Perspective on Pain and Suffering Awards*, *in* BEHAVIORAL LAW AND ECONOMICS 259, 262 (Cass R. Sunstein ed., 2000). As an example, "individuals will perceive a penalty for using credit cards as a loss and a bonus for using cash as a gain; this will lead individuals to use cash if and only if the 'penalty' tack is taken, although the two situations are, from an economic and end-state perspective, identical." *Id.*

98. Amos Tversky & Daniel Kahneman, *Advances in Prospect Theory: Cumulative Representation of Uncertainty*, *in* CHOICES, VALUES, AND FRAMES 44-45 (Daniel Kahneman & Amos Tversky eds., 2000).

99. Daniel Kahneman & Amos Tversky, *Choices, Values, and Frames*, *in* CHOICES, VALUES, AND FRAMES 1, 10 (Daniel Kahneman & Amos Tversky

statements, and thereby set the frames, they have considerable power to influence consumer decision-making. How might framing effects take place through the GLB Act notices?

According to well documented empirical findings, most people define value by focusing on changes (gains and losses) relative to some reference point. Research into frames has also found that most people react more decisively to avoid losses than to obtain gains. Put simply, the pain caused by the loss of $100 is greater than the joy caused by the gain of $100.[100] Reconsider, then, the privacy notices that imply that consumers may have already opted out or that opting out will accomplish little. These GLB Act notices present a reference point that suggests to consumers that only inaction is needed or that at best only relatively small gains are available from opting out. Finally, to raise an additional tactic of the GLB Act privacy notices, some notices state that consumers who opt-out may fail to receive "valuable offers." This notice creates a frame that points to opting out as leading only to a loss. By creating a perceived entitlement, the financial institution seeks to discourage opt-out. Due to the power of frames, a "notice plus opt-out" approach may prove unable to alter a lemons equilibrium and have virtually no information forcing effect.[101] To express this idea more completely, a law requiring notice and an opt-out default may fail to induce much bargaining so long as the better informed party still controls the language and form in which the actual data are conveyed.

In light of this critique, a notice and "opt-in" regime might at first appear to be a better choice to create an information forcing default. Because consent must be procured, the burden

---

eds., 2000).

100. Kahneman, Knetsch, and Thaler report,

> A wine-loving economist we know purchased some nice Bordeaux wines years ago at low prices. The wines have greatly appreciated in value. . . . This economist now drinks some of this wine occasionally, but would neither be willing to sell the wine at the auction price nor buy an additional bottle at that price.
>
> Thaler called this pattern—the fact that people often demand much more to give up an object than they would be willing to pay to acquire it—the *endowment effect.*

Daniel Kahneman et al., *The Endowment Effect, Loss Aversion, And Status Quo Bias, in* CHOICES, VALUES, AND FRAMES 159 (Daniel Kahneman & Amos Tversky eds., 2000).

101. *See, e.g.*, Russell Korobkin, *Inertia and Preference in Contract Negotiation: The Psychological Power of Default Rules and Form Terms*, 51 VAND. L. REV. 1583, 1587-92 (1998).

shifts to the financial institution to convince a customer to permit disclosure. The financial organization must therefore explain the benefits of action, which has the effect of flipping the frame. Opt-in creates an entitlement in the privacy of personal information, and the customer must be induced to give it up. In explaining the move to an opt-in standard for financial privacy in Vermont, the Banking Commissioner made precisely such an argument in favor of flipping the frame. Elizabeth Costle stated that "[i]nstead of waiving their right to privacy by inaction, Vermonters will be protected until they knowingly agree to the sharing of their personal information."[102] Viewed from an information forcing perspective, opt-in would appear to be an improvement over opt-out. It is, nevertheless, subject to various criticisms, some contradictory, which we wish to discuss.

First, consider the majoritarian perspective on the move to an opt-in. If most people will choose disclosure, then opt-in increases the cost of getting people where they want to go anyway. Worse yet, because of the flipping of the frame, many people will not opt-in, when perhaps many people would have wanted to do so. Here is a possible criticism that we wish to point out but not adopt. Once again, majoritarianism oversimplifies the complexity involved in setting defaults. On a different note, we will, however, argue below that the goal of opt-in may not give people precisely what they want in each transaction. Attention is also needed to the creation and preservation of a privacy commons. If we seek to create more general rules, termed "Fair Information Practices," for use of personal data, opt-in and private negotiations may not be of much help.

Second, and more troubling, financial institutions are likely to be good at getting consent when they need it. After all, they provide services that most people need or, at least, desire greatly. When faced with a choice between opting-in and not getting a credit card, the customer will likely choose to opt-in. This criticism points to the power of the stronger party to use contracts of adhesion. This point has some merit; the adjustment of frames can have an impact upon consumer choice, but decisionmaking also faces other powerful constraints. Even if the better informed party does not entirely control the language and form in which the actual information about terms is conveyed, defaults may prove unable to induce much bargain-

102. *Vermont Privacy Regulations*, *supra* note 42.

ing about critical issues.

To point to a recognition of the limits of information forcing defaults, used car "lemon laws" typically do not rely exclusively on an information forcing approach. These statutes provide some information forcing through standardized language in warranties, but also typically require, among their most important protections, that used car dealers provide a written, minimum guarantee of the used automobile for a short period of time (such as the earlier of thirty days or 1000 miles if the vehicle has 36,000 miles at the time of sale).[103] These laws also generally require that commercial used car sellers take such vehicles back from the buyer when the flaws persist after several attempts at repair.[104] Sometimes better information may not be enough to overcome market failure.

Thus far, we have discussed majoritarian and information forcing defaults. In our view, these two approaches to evaluating background rules are not the best approaches for information privacy. We now wish to set out a third classification of background rules, that of "norm enforcing" defaults.

A norm enforcing default seeks to alter, or channel, behavior of parties through reference to a non-contractual norm or policy. Rather than identifying a majoritarian position or an information forcing effect, a norm enforcing default is justified by explicit recourse to some substantive value. To be sure, once we leave the realm of ideal types, other kinds of defaults can have norm enforcing aspects. Both majoritarian and information forcing defaults, at times, have been justified because of some normative goal that they are said to reach.[105] As a sepa-

103. For an introduction to these laws, see Martha M. Post, *New York's Used-Car Lemon Law: An Evaluation*, 35 BUFF. L. REV. 971 (1986). The law itself is found at N.Y. GEN. BUS. § 198(a) (1988).

104. These statutes also provide for strong rights for the consumer when a dealer fails to fulfill his legal obligations. *See, e.g.*, N.Y. GEN. BUS. § 198-b(c)(2) (1988).

105. Some scholars have justified the use of majoritarian defaults on utilitarian grounds; these defaults are said to minimize the costs of contracting by reaching a result that most parties would desire without the parties actually having to invest in drafting the rule. Majoritarian defaults have also been defended as reflecting the parties' hypothetical consent. *See* Frank H. Easterbrook & Daniel R. Fischel, *Corporate Control Transactions*, 91 YALE L.J. 698, 702 (1982) (noting that fiduciary duties reflect the contract that shareholders would have negotiated with managers); Frank H. Easterbrook & Daniel R. Fischel, *The Proper Role of a Target's Management in Responding to a Tender Offer*, 94 HARV. L. REV. 1161, 1182 (1981) (explaining that corporate defaults supply "standard form 'contracts' of the sort shareholders would be likely to

rate category, however, the value of the norm enforcing default is that it makes explicit this characteristic of background rules. Norm enforcing defaults matter because of the impact that they have on norm-related behavior.[106]

We now face a puzzle that this Article has thus far avoided: What should be the normative role of information privacy law? Evaluating the GLB Act in terms of norm enforcing defaults requires an answer to this question. As a further complexity, and as we argue in the next section, different background rules for sharing personal data will promote different normative agendas for information privacy law.

B. TOWARD A NORMATIVE ROLE FOR INFORMATION PRIVACY–THE VIEW BEYOND DEFAULTS

Thus far, this Article has defined information privacy as involving the creation and maintenance of rules that structure

---

choose."). From this perspective, termed the "contractualist justification," a majoritarian default rule is worthwhile because it is based on what most parties would have agreed to under some greater or lesser idealized setting. For a more general introduction to the contractualist approach, see David Charny, *Hypothetical Bargains: The Normative Structure of Contract Interpretation*, 89 MICH. L. REV. 1815 (1991); Jules L. Coleman et al., *A Bargaining Theory Approach to Default Provisions and Disclosure Rules in Contract Law*, 12 HARV. J.L. & PUB. POL'Y. 639, 645-47 (1989). We can also imagine information forcing default rules that are grounded in norm enforcement; thus, information forcing may be said to overcome coordination problems to reach an economically efficient result.

106. Richard Craswell has been the most important influence on us in positing our category of "norm enforcing" defaults for privacy. He has written of the failure of "content-neutral" theories of default rules in these terms:

> ["Content neutral" default theories] give reasons why an individual who has promised to do Ø thereby incurs some form of obligation to do Ø, regardless of how Ø is filled in. The reason for this neutrality is understandable: To do anything more requires a theory that would tell people what kinds of promises they ought to make. Unfortunately, the theorists' reluctance to advise individuals as to how they ought to exercise their freedom to fill in the content of Ø leaves them equally unable to give legal systems any guidance about how to fill in the content of Ø when contracting parties fail to specify their preferred content.
>
> This other theory must be a theory that is not neutral between the different ways of filling in the exact scope of the parties' obligation—for example, it must provide some reason for preferring promises with an implied warranty to promises without an implied warranty, or vice versa. In other words, this other theory must rely on more than the value of individual autonomy or the value of telling the truth.

Craswell, *supra* note 84, at 515-16. In the next section of this Article, we attempt to develop just a theory under the title of "constitutive privacy."

access to and use of personal data. This definition is process-oriented; we wish now to examine the issue of information privacy's normative purpose. In this section, we draw contrasts between two normative views of privacy and relate these visions back to the question of default rules. The first view of privacy is concerned with individual control over personal data ("privacy-control"). The second normative vision of information privacy considers it as a value constitutive of society ("constitutive privacy").

Privacy-control. The leading paradigm of information privacy conceives of it as a right to control the use of one's data. As the Supreme Court declared in a leading Freedom of Information Act opinion, "[B]oth the common law and the literal understandings of privacy encompass the individual's control of information concerning his or her person."[107] Leading scholarship for almost a half-century contains similar definitions of information privacy.[108] The paradigm of privacy-control is a liberal autonomy principle that seeks to place the individual at the center of decisionmaking about personal information use. It seeks to achieve informational autonomy through individual stewardship of personal data and individual bargaining about data use.

Autonomy fits within the model of "privacy-control" in two ways. First, as Robert Post notes, "[a]utonomy refers to the ability of persons to create their own identity and in this way to define themselves."[109] By allowing individual stewardship of personal information, privacy-control helps people control their own identity. It does so in particular by limiting and shaping

107. United States Dep't of Justice v. Reporter's Comm., 489 U.S. 749, 763 (1988).

108. *See* Charles Fried, *Privacy*, 77 YALE L.J. 475, 482-83 (1968) ("Privacy 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."); Ken Gormley, *One Hundred Years of Privacy*, 1992 WIS. L. REV. 1335, 1356 ("[C]ontrol of information about oneself is critical in determining how and when (if ever) *others* will perceive us, which is in turn essential to maintaining our individual personalities."); Richard A. Posner, *Privacy, in* PALGRAVE DICTIONARY OF ECONOMICS 103, 104 (Peter Newman ed., Stockton Press 1998) ("[E]conomic analysis of the law of privacy . . . should focus on those aspects of privacy law that are concerned with the control by individuals of the dissemination of information about themselves."); Frederick Schauer, *Internet Privacy and the Public-Private Distinction*, 38 JURIMETRICS J. 555, 556 (1998) ("The privacy interest I address here is the power to control the facts about one's life.").

109. Robert C. Post, *Three Concepts of Privacy*, 89 GEO. L.J. 2087, 2092 (2001).

the personal information that others have about us and thereby influencing the views that they have of us. Richard Posner's skepticism about information privacy flows precisely from this aspect of it. In his view, information privacy is mostly a bad thing relating to a "right to conceal discrediting information."[110]

Second, autonomy also means making decisions about personal matters, especially ones that are important to self-definition. Thus, one's decisionmaking about important health care choices is said to promote individual autonomy.[111] Privacy-control seeks to promote autonomy by heightening individual choice about the use of personal data, including negotiating agreements about data use.

Privacy-control also encourages a commodification (through bright-line propertization and contractualization) of personal information. In the current information age, personal information is frequently considered as a new kind of intellectual property. Once it takes this form, as Pamela Samuelson has noted, individuals are "to bargain over which personal data to reveal to which firms for what purposes."[112] The transformation of personal information into property allows people to bargain over it and make binding transfers of it through contracts. In this fashion, the paradigm of privacy-control links autonomy, property, and contract.

At this point, we can also see that privacy-control fits in comfortably with the use of both majoritarian and information forcing defaults. A majoritarian default is set as the term that most parties would have reached had they bargained. Recourse to this default can be said to promote choice, or, at a minimum, *implied consent*. After all, a given course of consumer inaction at best signals acquiescence and, in that sense, implied con-

110. Posner, *supra* note 108, at 105 ("Legal protection of the right to conceal discrediting information is problematic for the further reason that it undermines social control by means of norms, an important substitute for legal control of behaviour [sic].").

111. For a discussion of informed consent in the health care setting, see CARL E. SCHNEIDER, THE PRACTICE OF AUTONOMY: PATIENTS, DOCTORS, AND MEDICAL DECISIONS 87-92 (1998); Joseph Goldstein, *For Harold Lasswell: Some Reflections on Human Dignity, Entrapment, Informed Consent and the Plea Bargain*, 84 YALE L.J. 683, 690-94 (1975); Peter H. Schuck, *Rethinking Informed Consent*, 103 YALE L.J. 899, 902-04 (1994); Aaron D. Twerski & Neil B. Cohen, *The Second Revolution in Informed Consent*, 94 NW. U. L. REV. 1, 2-5 (1999).

112. Pamela Samuelson, *Privacy as Intellectual Property?*, 52 STAN. L. REV. 1125, 1127-30 (2000).

sent.[113] Once a default is set in a majoritarian fashion, and individuals do nothing to change the default, one may assume that agreement has been reached. As for the information forcing default, the second kind of background rule, it is also highly compatible with the paradigm of privacy-control. To explore the terms of this compatibility, we first wish to adjust the actual terms of the GLB Act and then to sketch a "rosy scenario" of the impact of the revised statute.

Imagine a revised GLB Act with an *opt-in* requirement for data sharing with non-affiliates. The revised statute would now contain a true information forcing default due to its penalty—unless the financial institution obtained affirmative consent from the individual, it could not share information with a non-affiliated entity.[114] Such a result is, in fact, reached under Vermont's recent financial privacy regulations. Under the revised GLB Act or Vermont law, moreover, the following "rosy scenario" might occur: The financial institution will now have to do more to obtain assent from the individual before data sharing may occur. It would be obliged to provide more privacy, more financial services at the same price, or a lower price for the same level of services. Individual choice about data use would therefore be heightened.[115] By stimulating bargaining over terms of service, information forcing defaults would further a paradigm of privacy-control.

In our judgment, however, the rosy scenario is unlikely. Indeed, one must be wary about too great a reliance on either majoritarian or information forcing defaults as a way of promoting privacy. This Article has already questioned whether supplying more information about personal data use will induce consumers to bargain for information privacy. In making this point, we pointed to bounded consumer rationality and, specifically, to the power of frames. Related criticisms of the paradigm of privacy-control are possible. One of us has already

113. Indeed, consent also implies the possibility of refusal. If "voice," that is, bargaining about privacy terms, does not lead to change, "exit," that is, refusal, is to be possible. *See generally* ALBERT O. HIRSCHMAN, EXIT, VOICE, AND LOYALTY—RESPONSES TO DECLINE IN FIRMS, ORGANIZATIONS AND STATES (1970). Under conditions that lead to contracts of adhesion, however, such refusal is unlikely.

114. As the previous section of this Article has suggested, however, the GLB Act's opt-out requirement for data sharing with non-affiliates is information-forcing without any effective penalty.

115. For a more positive account of the possible effect of opt-in rules, see Sovern, *supra* note 6, at 1107-13.

used the term "the autonomy trap" to refer to a cluster of shortcomings of the paradigm of data control.[116] Of these, two are predominant in the context of the GLB Act: (1) the strong limitations existing on individual autonomy in the current privacy market, and (2) the shaping of individual autonomy itself through the processing of personal data.

First, self-reliant control cannot fulfill its assigned role for shaping privacy unless individuals can choose between different possibilities, and significant reasons for doubt exist on this score in the context of financial services. At present, as we have discussed, it is unlikely that consumers will be able to identify the financial institutions with better privacy practices—if they even exist. As we have argued, privacy notices provide a cornerstone only for a legal fiction of implied consent to data processing by financial institutions. Yet, the consequences of this legal fiction are apt to be quite real. As Mark Lemley concludes regarding the propertization of personal data, turning information into commodities will lead to a "right that is regularly signed away."[117] Lemley believes that this will lead to "*less* protection than we want to give individuals."[118]

Second, individual autonomy is itself shaped by the processing of personal data. In his criticism of majoritarian defaults, Richard Craswell made a similar point. In language we have already cited, Craswell noted "the potential for circularity that arises when people's expectations are themselves affected by existing legal rules."[119] In similar fashion, existing law and the practices of financial institutions shape informational self-determination in the context of financial privacy. The meaning that we attribute to individual autonomy for privacy is itself formed by the existing means by which personal data are processed. A danger of this second aspect of the "autonomy trap" is that it can lead to a reduced sense of what is possible. A dominant trend in personal data use in cyberspace can change our "is" to our "ought."

Constitutive Privacy. If privacy-control is a limited concept, what is the normative purpose of information privacy? In our judgment, information privacy should be conceptualized as

116. Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1609, 1661-64 (1999) [hereinafter Schwartz, *Privacy in Cyberspace*].

117. Mark A. Lemley, *Private Property: A Comment on Professor Samuelson's Contribution*, 52 STAN. L. REV. 1545, 1551 (2000).

118. *Id.*

119. Craswell, *supra* note 84, at 507.

a value constitutive of a democratic society.[120] Access to personal information and limits on it help form the nature of the society in which we live and shape our individual identities. For example, the structure of access to personal information can have a decisive impact on the extent to which certain actions or expressions of identity are encouraged or discouraged.[121] The importance of information privacy for both individuals and democratic community necessitates attention to boundaries about personal information.

Constitutive privacy is, therefore, a matter of line-drawing along different coordinates to shape permitted levels of scrutiny. Standards of information privacy should be considered as normatively defining "information territories."[122] These territories create patterns of knowledge and ignorance of personal data to stimulate or discourage different kinds of social expression and action.

A further point should be made about constitutive privacy. An information privacy territory should not be expected to function as a data fortress that isolates personal information in some absolute sense. Personal data often involve a social reality that is external to the individual. As a result, the optimal utilization of this information is unlikely to exist at either end of a continuum that ranges from absolute privacy to complete disclosure.[123] The proper social response to information privacy issues cannot be to maximize secrecy about individuals and their pursuits. Rather, information privacy norms should create shifting, multidimensional data preserves that insulate

120. One of us has set out this approach in a series of articles. Paul M. Schwartz, *Beyond Lessig's* Code *for Internet Privacy*, 2000 WIS. L. REV. 743, 761-62 [hereinafter Schwartz, *Lessig's Code*]; Paul M. Schwartz, *Internet Privacy and the State*, 32 CONN. L. REV. 815, 834-43 (2000) [hereinafter Schwartz, *Privacy and the State*]; Schwartz, *Privacy in Cyberspace*, *supra* note 116, at 1658-66; *see also* Robert C. Post, *The Social Foundations of Privacy: Community and Self in the Common Law Tort*, 77 CAL. L. REV. 957, 966 (1989) (stating that rather than upholding "the interests of individuals against the demands of community," information privacy creates rules that in some significant measure "constitute both individuals and community"). For an attempt to differentiate "constitutive privacy" from Post's work, see Schwartz, *Privacy in Cyberspace*, *supra*, at 1667-70.

121. *See* Julie E. Cohen, *Examined Lives: Information Privacy and the Subject as Object*, 52 STAN. L. REV. 1373, 1408 (2000) (noting that processing of personal information involves "questions of behavior modification and free will").

122. *See* Schwartz, *Privacy in Cyberspace*, *supra* note 116, at 1667.

123. For a similar conclusion regarding the use of personal medical information, see Schwartz, *Privacy Economics*, *supra* note 6, at 41.

personal data from different kinds of observation by different parties. Different kinds of "outing," that is, revelation of otherwise fully or partially hidden aspects of one's life, should be prevented before different audiences. Particular attention is needed to prevent revelation and use of data that might chill one's underlying capacity for decisionmaking.[124]

The idea of constitutive privacy suggests the necessity of involvement by democratic institutions in the creation of rules for the use of personal data. As to the content of the necessary rules, we turn to the general framework provided by "fair information practices" (FIPs).[125] FIPs are widely considered the building blocks of modern information privacy law; they have been present in information privacy law and policy since the era of mainframe computers in the 1970s.[126] Although the expressions of FIPs in different statutes and regulations vary in their details, sometimes crucially, we wish to offer a formulation of FIPs with seven elements: (1) *defined obligations*, often statutory in nature, for processors of personal information; (2) the maintenance of processing systems that the concerned individual can understand (*transparent data processing*); (3) a requirement of *notice* to the individual; (4) the provision of indi-

124. Here we gingerly re-introduce the theme of autonomy. Note, however, that we view information self-determination neither as a pre-existing quality that is independent of society and data processing nor as a quality that is protected for its own sake (which would lead us back to "privacy-control"). Rather, our view is that information self-determination is to be promoted because democratic society turns on the underlying communicative competency of individuals. *See* Schwartz, *Privacy in Cyberspace*, *supra* note 116, at 1654-55.

For influential work on this perspective regarding the interplay between self-determination, democratic society, and information privacy, see ROBERT C. POST, CONSTITUTIONAL DOMAINS: DEMOCRACY, COMMUNITY, MANAGEMENT 51-88 (1995). For a related explanation of the tie between privacy and "the practice of self-determination on the part of free and equal citizens," see JÜRGEN HABERMAS, BETWEEN FACTS AND NORMS 386, 368-70 (William Rehg trans., 1996). *See also* Spiros Simitis, *From the Market to the Polis: The EU Directive on the Protection of Personal Data*, 80 IOWA L. REV. 445, 463-66 (1995) (discussing rules on the free flow of personal data in the European Union); Spiros Simitis, *Reviewing Privacy in an Information Society*, 135 U. PA. L. REV. 707, 734-36 (1987) (discussing the connection between public and private life).

125. Schwartz, *Privacy in Cyberspace*, *supra* note 116, at 1614.

126. For a description of early proposals regarding fair information practices, see DAVID H. FLAHERTY, PROTECTING PRIVACY IN SURVEILLANCE SOCIETIES 306-07 (1989). For a more recent governmental discussion of a somewhat different set of fair information practices, see FEDERAL TRADE COMMISSION, PRIVACY ONLINE: A REPORT TO CONGRESS 7-12 (1998).

vidual *choice* regarding the use of her personal information; (5) *security* for collected and stored data; (6) *access* to personal data; (7) *enforcement* of privacy rights and standards, which can involve—often in combination—individual litigation, government oversight, or industry self-regulation.[127]

Let us return to the GLB Act and default rules. If the normative goal of this law is constitutive privacy, the rules about financial privacy must be seen as mattering both to the individual and society. What kind of information territories should we seek to create? In this regard, we should consider a warning of the Privacy Rights Clearinghouse concerning dangers in the GLB Act's aftermath:

> Consider the amount and kinds of information you supply just to a financial institution that may sell insurance, bank products, and securities. Combine this with the information available from other sources, and virtually any detail of your financial affairs, health status, spending habits, lifestyle purchases, political affiliations, religious contributions, and more can be collected by your financial institution. Unless you formally object, it can be shared, sold, rented, or otherwise disclosed with few exceptions.[128]

A financial institution knows whether a customer has recently bought running shoes or other consumer products, the name of one's physicians (as well as the nature of their speciality), and whether one has purchased orthotics or aspirin or other kinds of health care products. Some of this information might be embarrassing, and some of it might create potentially damaging labels for persons or lead to other harmful results. The cumulative impact of these disclosures can have a profound impact on the society in which we live. Regulatory attention is needed to control the resulting patterns of data accumulation and use.

Note, however, that FIPs can be crafted to be majoritarian or information forcing. Sometimes FIPs may also promote autonomy. From the list above, we might pick "transparency," "notice" and, perhaps above all, "choice" as possible majoritarian and information forcing background rules. These three examples of FIPs can also serve to enhance individual decisionmaking. FIPs, however, should *not* be justified largely on these

127. For discussion of the standards, see Paul M. Schwartz, *Privacy and Participation: Personal Information and Public Sector Regulation in the United States*, 80 IOWA L. REV. 553, 557-64 (1995). *See also* COLIN J. BENNETT, REGULATING PRIVACY: DATA PROTECTION AND PUBLIC POLICY IN EUROPE AND THE UNITED STATES 101-11 (1992).

128. *Fact Sheet 24*, *supra* note 36, at 5.

grounds, but on the idea that privacy, from a constitutive perspective, is also a "public good." Information privacy is a kind of commons that requires some degree of social control to construct and then preserve.

The problems of bounded rationality, along with ever present coordination problems, make defaults a risky choice in many contexts of information privacy. From this perspective, FIPs should carefully mix both mandatory rules and default rules. Where private bargaining about data processing is most likely to fall short, mandatory rules should set immutable standards.[129] Where potential exists for private negotiations, FIPs should only establish default rules that set a baseline for negotiations because the potential price of mandatory standards is regulatory rigidity.

The most important consequences of this approach for the GLB Act is that default rules, when viewed from a norm enforcing perspective, are likely to have a limited role. As we have argued already in this Article, the privacy market between consumers and financial institutions does not presently function well. Under these conditions, the law should generally seek to minimize harms that flow from reliance on bargaining among consumers and data processors. According to Robert Cooter and Thomas Ulen's formulation, such an approach represents the "normative Hobbes theorem" of law: "Structure the law so as to minimize the harm caused by failures in private agreements."[130]

We will conclude this Article by examining two further aspects of mandatory and default rules in the context of financial privacy. We first consider mandatory rules as found in the GLB Act's rules for data security. We then propose that the GLB Act's current opt-out be re-evaluated in light of social science literature concerning frames and that Congress consider a shift to an opt-in default.

C. MANDATORY AND DEFAULT RULES: TOWARD A REVISED GLB ACT

The rules of the GLB Act for data security are not presented as defaults, but are mandatory in nature. As this Article noted in Part I, the GLB Act spells out three requirements

129. For a further discussion in the context of cyberspace privacy, see Schwartz, *Lessig's Code*, *supra* note 120, at 781-84.

130. COOTER & ULEN, *supra* note 91, at 90.

for data security and integrity. Financial institutions are to do the following: (1) protect the security and confidentiality of customer records and information; (2) prevent any anticipated threats or hazards to the security or integrity of such records; and (3) prevent unauthorized access to use of records that "could result in substantial harm or inconvenience to any customer."[131] Title V's rules concerning "pretexting," or obtaining customer information by false pretenses, are a further response to the question of unauthorized access to records.

Recourse to mandatory rules for security standards is wise. It is unlikely that consumers will negotiate for an optimal level of data security. One difficulty here relates to information costs, which are high for consumers in this technology-driven area. Imagine the intense level of research that consumers would be forced to carry out in evaluating the information security standards of one bank versus another. A further difficulty concerns the significant market power of financial institutions, which prior to the GLB Act generally shared an incentive in having consumers bear the burden of flawed data security and "pretexting."[132] Default rules for bargaining between financial entities and consumers would not be helpful in the context of data security.

When security standards are mandatory, however, the danger is that of regulatory inflexibility. Data security may fall short if structured only as command-and-control rules, which mandate rigid outcomes and sometimes even specify the precise means—such as the type of equipment—to be used by industry.[133] As scholars have argued concerning environmental regulation, command-and-control regulation tends to freeze development of technologies and discourage recourse to less costly alternatives.[134]

---

131. Gramm-Leach-Bliley Act of 1999, Pub. L. No. 106-102, § 501(b)(3), 113 Stat. 1338 (1999). The Act also requires the GLB oversight agencies to establish "appropriate standards" for data security and integrity. § 501(b).

132. For a related discussion of how credit reporting agencies shift the problem of "identity theft" to consumers, see Lynn M. LoPucki, *Human Identification Theory and the Identity Theft Problem*, 80 TEX. L. REV. 89, 91-93 (2001).

133. *See generally* Robert N. Stavins, *Economic Incentives for Environmental Regulation*, *in* 2 DICTIONARY OF ECONOMICS & LAW 7 (1998) (discussing command-and-control rules in the context of environmental regulation).

134. *Id.*; *see also* Carol M. Rose, *The Several Futures of Property: Of Cyberspace and Folk Tales, Emission Trades and Ecosystems*, 83 MINN. L. REV. 129, 164-79 (1998).

The GLB Act provides authority to the GLB Act oversight agencies to "establish appropriate standards for the financial institutions subject to their jurisdiction relating to administrative, technical, and physical safeguards" for data security.[135] The GLB Act is silent on the kind of standards that these agencies should issue. The Children's Online Privacy Protection Act (COPPA) of 1998 provides a good model of an approach beyond command-and-control for developing technical standards.

COPPA provides comprehensive FIPs for children on the Internet. As its cornerstone, COPPA generally forbids commercial Web sites from collecting information about children without parental consent.[136] It also grants parents a right of access to any information about their children that is collected.[137] These two requirements bring with them, however, important technical questions as to how parents are to indicate their consent and authenticate their identities.[138] COPPA also contains other technical issues, including, similar to the GLB Act, a requirement of data security.[139] COPPA states that operators of a web site directed to children must "maintain reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from children."[140]

COPPA introduces flexibility in responding to these technical issues through a statutorily authorized mechanism for regulatory negotation. Parallel to the technical regulations to be developed under COPPA by the FTC, the statute authorizes the industry to formulate its own technical norms. COPPA creates a "safe harbor" for commercial web sites that follow "a set of self-regulatory guidelines, issued by representatives of the marketing or online industries" or by other approved persons.[141] Yet, industry guidelines will receive safe harbor pro-

135. Gramm-Leach-Bliley Act § 501(b).

136. 15 U.S.C.A. § 6502(b)(1)(b)(ii) (2001). For an overview of COPPA and a skepticism towards it as "paternalistic and authoritarian," see Anita L. Allen, *Minor Distractions: Children, Privacy, and E-Commerce*, 38 HOUS. L. REV. 751, 775 (2001). Interestingly enough, Professor Allen had called for non-individualistic justifications for information privacy laws in a previous article. *See generally* Anita L. Allen, *Coercing Privacy*, 40 WM. & MARY L. REV. 723 (1999) (arguing that privacy is vital for liberal democracy, and that the voluntary abrogation of privacy can become a serious problem).

137. § 6502(b)(1)(B)(iii).

138. § 6501(9).

139. § 6502(b)(1)(D).

140. *Id.*

141. § 6503.

tection under COPPA only if the FTC approves them. For such approval to be given, the FTC must find that the industry "meet the requirements" of the agency's own technical guidelines.[142] Thus, COPPA strongly seeks to channel industry norms towards certain substantive levels. Moreover, in issuing a rule regarding the COPPA Safe Harbor, the FTC has sought to make industry self-regulation effective by setting tough requirements for the industry. For example, it required all web sites making use of safe harbor self-regulation to submit to independent auditing and to provide effective enforcement requirements, including, in the alternative, "voluntary payments to the United States Treasury in connection with an industry-directed program for violators of the guidelines."[143]

FTC regulations under the GLB Act should also balance mandatory requirements for data security with regulatory flexibility. A similar provision for regulatory negotiation should be included in amendments to the GLB Act. The key to making a safe harbor effective, however, will be FTC refusal to approve any industry guidelines that provide a lesser level of data security than the FTC's own technical safeguards. Nevertheless, industry may also be able to generate insights as to how to provide an equivalent level of security at a lower cost to it.

Beyond mandatory regulations, we wish to return to defaults. We have expressed doubts that an opt-in requirement would necessarily limit much data sharing and suggest that only a limited role is suitable for defaults in financial privacy. Where less use will be made of defaults, there will be more need for FIPs. Yet, the GLB Act lacks many basic elements of FIPs.[144] At the same time, however, the GLB Act does require the Comptroller General to carry out a study of information sharing among financial affiliates.[145] The report of the Comptroller General, when issued, should provide an occasion for

142. § 6503(b)(2).

143. Children's Online Privacy Protection Rule, 64 Fed. Reg. 22,750, 22,759 (Apr. 27, 1999) (to be codified at 16 C.F.R. pt. 312).

144. For this reason, some privacy advocates have criticized it as essentially being a data sharing statute. Thus, Marc Rotenberg, head of the Electronic Privacy Information Center, views the GLB Act as performing primarily an alibi function in allowing Congress to claim it is doing something for privacy "without imposing any significant restrictions on how companies collect and use data." *Hairs Raised Over Data Privacy*, *at* http://www.privacydigest.com/2001/05/07 (May 7, 2001).

145. Gramm-Leach-Bliley Act § 526.

Congress to reconsider the GLB Act and the need for robust FIPs in it.

We can imagine, however, that Congress may decide not to provide full FIP's in a new version of the GLB Act. For that reason, we wish to offer two more modest proposals. The first concerns tweaking the current opt-out rule. The second concerns testing our "rosy scenario" by adopting an opt-in rule.

First, we believe that Congress and the GLB Act oversight agencies should reconsider the GLB's "notice and opt-out" rule in light of the social science literature regarding frames.[146] The purpose of a notice and opt-out requirement is to provide a mechanism reasonably designed to promote the exercise of choice. In our judgment, the GLB Act oversight agencies, including the FTC, must do more to make sure that opt-out notices provide choice for consumers. As an initial matter, since individuals typically devote scant resources to consumer contracts, we propose that notice and opt-out regulations require that each notice provide the opt-out information at its start and in a bold-faced format. Drawing more specifically on literature regarding frames, we also suggest that a greater number of consumers will be more likely to exercise choice if opt-out's are proposed as preventing a change of state that will lead to a loss of privacy. This latter point may seem abstract so we will make it more concrete.

We have found a proposal to the FTC from the Public Citizen Litigation Group that appears to have intuitively grasped the essence of framing effects. Public Citizen asks the FTC to issue a rule that drafts a standardized opt-out element for GLB Act privacy notices.[147] Its revised GLB out-opt, to be issued at the top of the notice "in a large, bold-faced font," would state:

> WE ARE ALLOWED TO DISCLOSE YOUR PRIVATE INFORMATION TO OTHER COMPANIES UNLESS YOU TELL US NOT TO.

146. The FTC has already issued a regulation concerning the form of privacy notices, but it speaks mostly in unhelpful generalities. For example, the FTC informs financial institutions, "[y]ou must provide a clear and conspicuous notice to each of your customers that reflects your privacy policies . . . ." FTC Privacy of Consumer Financial Information Final Rule, 16 C.F.R. § 313.5(a)(1) (2001). The FTC's regulation also provides, "You provide adequate notice that the consumer can opt out of the disclosure of nonpublic personal information to a nonaffiliated third party if you exercise an opt-in right if you . . . [d]esignate check-off boxes in a prominent position on the relevant forms with the opt out notice. . . ." *Id.* § 313.7(a)(2)(i), (ii)(A).

147. Public Citizen Litigation Group, *supra* note 66, at 1-2.

> YOU HAVE A RIGHT TO PREVENT US FROM DISCLOSING YOUR PRIVATE INFORMATION TO OTHER COMPANIES.
>
> BUT IF YOU DO NOT RESPOND WITHIN 30 DAYS, WE MAY BEGIN SHARING YOUR INFORMATION. YOU WILL STILL HAVE THE RIGHT TO TELL US TO STOP AT ANY TIME. BUT ONCE WE HAVE SHARED INFORMATION WITH OTHER COMPANIES, WE CANNOT GET IT BACK FROM THEM OR STOP THEM FROM USING IT.[148]

Note that this opt-out notice presents a frame that speaks in terms of changes of state and also identifies losses that consumers can prevent ("disclosing your private information to other companies" and "once we have shared information with other companies, we cannot get it back from them or stop them from using it."). This notice is framed in a fashion that is likely to encourage consumer consideration of the opt-out.

Finally, revising the GLB Act to contain an opt-in requirement would combine information forcing and a penalty. Despite our doubts as to the ability of this default to dislodge a lemons equilibrium in the privacy market with financial entities, an opt-in has merit as a fall back proposal to FIPs. Its benefit is to shift the burden of obtaining permission to the party who would disclose personal data. If opt-in fails to dislodge the lemons equilibrium in the privacy market, as we suspect it might, there will only be as much data disclosure as takes place at present. If, contrary to our belief, it does succeed, financial institutions will not necessarily be obliged to offer more privacy. Rather, a "successful" opt-in might lead consumers to trade their personal information for more financial services or a lower price for existing services. The shift in Vermont to an opt-in standard for financial institutions will provide interesting test results regarding the possible merits of such a revision to the GLB Act.

In a sense, then, opt-in might not lead to heightened privacy protection. Consumers may simply bargain for more services or a lower price and not for FIPs. Yet, when constitutive privacy is the goal, a default is to be used to defend the privacy commons. Given bounded rationality and the pervasiveness of coordination problems, this strategy is a risky one. We therefore end this Article by pointing once again to the limited role that defaults are likely to play in furthering information privacy for consumers.

148. *Id.* at 11-12.

CONCLUSION

In sum, the GLB Act has its failings, but ones that are instructive on a number of levels. First, it confuses notice with autonomy. Second, it uses default rules improperly by misallocating the burden of bargaining. Third, it fails to recognize the intractable nature of certain market failures in the privacy context and fails to appreciate the need to combine mandatory rules and penalty defaults to enforce privacy norms. Perhaps above all, the GLB Act does not recognize how privacy protection creates a public good. The difficulty is that private negotiations about data sharing arrangements may be insufficient to create the necessary kind of privacy commons.

The GLB Act's notice and opt-out approach is based on an attempt to link mandatory notices with a perceived majoritarian or perhaps information forcing default. This error rests on a mistaken view of privacy as the "control" of personal data. If privacy is control, one need only tell someone how their data will be used, and give them the opportunity to say "no." Yet, we have argued that "notice and opt-out" should not be equated with control. Bounded rationality, differences in negotiation strength, and coordination problems create an environment where mandatory notices obscure rather than clarify the rights of financial institution customers. "Notice and opt-out" has forced companies to incur great expense providing privacy notices while doing virtually nothing to provide strong FIPs. Indeed, if privacy protection aims to preserve autonomy, it could better serve this goal by using a penalty default, such as "notice and opt-in." This approach might force financial institutions to bargain with customers to procure the use of their personal information. This tactic might also encourage clear(er) explanation of the benefits of disclosure.

Even opt-in has its limits. "Opt-in" may well turn on unrealistic assumptions. The manner in which banks, stockbrokers, and insurance companies use information, share information with affiliates, and transfer information to third parties is complicated—too complicated to be understood by even a very smart lay person, let alone to be negotiated by each customer who opens a bank account. Individuals can be induced to bargain away their privacy by manipulating frames and exploiting collective action problems. The consequence may be that society as a whole will be left with a sub-optimal amount of pri-

vacy. Instead of overreliance on "opting," we advocate a mixed regime of mandatory and default, or waivable, background rules that are ultimately to be judged by reference to the FIPs that they put in place. FIPs are the building blocks for the multidimensional privacy spaces necessary in a democratic society.