



The attached material is posted on regulation2point0.org with permission.



J O I N T C E N T E R

AEI-BROOKINGS JOINT CENTER FOR REGULATORY STUDIES

Is More Government Regulation Needed to Promote E-commerce?

Robert W. Hahn and Anne Layne-Farrar

Related Publication 02-11

June 2002

Forthcoming Connecticut Law Review, Vol. 35, Issue 1, Fall 2002.

Mr. Hahn is director of the American Enterprise Institute-Brookings Joint Center for Regulatory Studies, a resident scholar at the American Enterprise Institute and a research associate at Harvard University. Ms. Layne-Farrar is with National Economic Research Associates (NERA). We would like to thank Alan Wiseman and Harold Furchtgott-Roth for helpful comments and Mary Beth Muething and Irina Danilkina for their excellent research assistance. Funding for this research was provided by the AEI-Brookings Joint Center for Regulatory Studies and Microsoft. The views expressed in this paper are solely those of the authors.

Is More Government Regulation Needed to Promote E-commerce?

Robert W. Hahn and Anne Layne-Farrar

E-commerce has experienced tremendous growth over the past few years. Nonetheless, senators, privacy watchdog groups, and the Federal Trade Commission have argued that e-commerce is being held back by consumer worries about online privacy and security. Some privacy advocates are calling for additional regulations—specifically new online privacy rules aimed at providing consumers with more information and customer choice. And Congress has tried to answer that call—most recently with a bill introduced by Senator Ernest Hollings. This essay examines the case for more government regulation and argues that the advocates have overstated their case. While some consumers, particularly older Americans and those new to the Internet, are clearly concerned about online privacy and security, these issues do not appear any more urgent for online shopping than offline shopping. Nor do these issues emerge as significant deterrents to e-commerce. Indeed, it is not even clear that any e-commerce has been deterred. Absent evidence of a significant market failure, the case for further government intervention is weak at best.

I. INTRODUCTION

E-commerce roughly doubled each year from 1997 to 1999.¹ Yet, there is concern in some quarters that it is not growing fast enough. For example, Senator Ernest Hollings introduced a bill in April 2002 that he claims will “accomplish the simultaneous objectives of providing better privacy protections for individuals while, at the same time, opening an untapped market of customers who are now reluctant to shop or buy online due to privacy concerns.”² Privacy watchdog groups and the Federal Trade Commission (FTC) under the last administration have echoed the argument that e-commerce is being held back by consumer worries about online

1. This statistic is based on a measure that uses credit card transactions. See Jim Harper and Solveig Singleton, *With a Grain of Salt, What Consumer Privacy Surveys Don't Tell Us*, at 8 (June 1, 2001), available at http://www.cei.org/PDFs/with_a_grain_of_salt.pdf. Citing Cyber Dialogue, *Best Practices in Online Customer Privacy Protection* (April 2001). Note that these figures are for consumer spending, not business spending. According to U.S. Census data, e-commerce retail sales increased 19% between 2000 and 2001 to reach 32.6 billion. See U.S. Census Bureau, *4th quarter 2001 release*, at <http://www.census.gov/mrts/www/current.html> (last visited April 2, 2002).

² Nicole Duran, “In Brief: Hollings Offers Privacy Preemption Bill,” *AMERICAN BANKER*, April 19, 2002.

privacy and security.³ To solve this perceived problem, privacy advocates are calling for additional regulations—specifically new online privacy rules that would improve privacy policy notifications on Web sites, provide greater customer choice in deciding to share personal information online, and beef up enforcement to identify and punish violators.⁴

This essay examines the case for more government regulation as it relates to the claim that the growth of e-commerce has been sluggish.⁵ We conclude that advocates have overstated their case. While it is difficult to know how e-commerce would have developed had tighter regulation of online privacy been in place, the evidence typically presented to bolster the case for more regulation has three problems. First, regulation advocates base many of their conclusions on surveys, which may be speculative or use data selectively. Other surveys point to traditional shopping issues like shipping fees and return hassles as bigger problems, or suggest that privacy concerns are no greater online than offline. Given that surveys do a notoriously bad job of providing objective data, using them to argue for more regulation is unconvincing. Second, there is no evidence that markets are failing to weigh consumer preferences appropriately: e-commerce Web sites have every incentive to provide protection that attracts business. Third, what little data are available demonstrates that e-commerce is growing rapidly and appears to be following a growth pattern that is typical for new technologies. In short, while hard data are difficult to obtain, the available evidence does not support the argument that e-commerce would develop more quickly and efficiently with more government regulation. In the absence of such

3. See, for example Fed. Trade Commission, *Privacy Online: Fair Information Practices in the Electronic Marketplace: A Report to Congress* (May 2000), at <http://www.ftc.gov/reports/privacy2000/privacy2000text.pdf> [hereinafter FTC (2000)]. For an example of the watchdog groups calling for additional regulation, see Sarah Andrews and Andrew Shen, Electronic Privacy Information Center, *Public Comment on Barriers to Electronic Commerce, U.S. Department of Commerce* (March 17, 2000), at http://www.epic.org/privacy/internet/Barriers_to_E-commerce.html. More recently, FTC commissioner Mozelle Thompson “citing a Forrester Research Inc. study that found that \$15 billion worth of e-commerce transactions go unrealized...said e-business is suffering from a lack of trust, both from a business-to-consumer and business-to-business standpoint.” The Commissioner added that more regulation on privacy might be needed. See Maryfran Johnson and Deborah Radcliff, *Cybersecurity Czar: Protect IT Infrastructure*, CNN.COM (November 9, 2001), at <http://www.cnn.com/2001/TECH/internet/11/09/infrastructure.protection.idg/?related>.

4. For a discussion of proposals for federal regulation of online privacy made prior to 2002, see Robert W. Hahn and Anne Layne-Farrar, *The Benefits and Costs of Online Privacy Regulation*, 54 ADMINISTRATIVE LAW REVIEW 85 (2002).

5. For an overview of existing laws and regulations, see FRED H. CATE, *PRIVACY IN THE INFORMATION AGE* (1997). For a summary of federal privacy legislation introduced since 1997, see Center for Democracy and Technology, *105th Congress Privacy*, at <http://www.cdt.org/legislation/105th/privacy/> (last visited April 2, 2002); Center for Democracy and Technology, *Privacy 106th Congress*, at <http://www.cdt.org/legislation/106th/privacy/> (last visited April 2, 2002). Also see FRED H. CATE, *PRIVACY IN PERSPECTIVE* (2001).

evidence, it is hard to build a case for new legislation to spur online purchases. In fact, federal regulation could do more harm than good by hobbling an industry that must be able to change rapidly to respond to consumer needs.

II. EVIDENCE THAT PRIVACY CONCERNS SLOW E-COMMERCE IS WEAK

A. Support For “Lost Sales” Due To Privacy Concerns Is Not Compelling

The statistics used to support federal intervention are typically based on problematic forecasts and surveys.⁶ Relying on surveys and forecasts to justify any policy position—either in support of or against additional legislation—is problematic. As is well-known, forward looking estimates depend heavily on the underlying assumptions and the opinions held by the forecaster. Modifying the assumptions changes the resulting forecast. Moreover, different analysts viewing the same data can easily arrive at different forecasts.⁷ Surveys are even less reliable. How a question is worded, the potential answers offered, or even the order in which potential answers are presented can all influence the results.⁸ Researchers looking for a particular response can manipulate a questionnaire in favor of a desired result.

The data that privacy advocates cite in defense of more regulation suffer from these criticisms. For example, one study cited by the Federal Trade Commission in their 2000 report predicted that by 2002, a total of \$18 billion in online sales would be lost because of consumer privacy worries.⁹ The number was derived by comparing forecasts of e-commerce growth under two different scenarios, one that accounted for privacy concerns and one that did not. In particular, online spending in 2000 was predicted to reach \$12 billion if nothing were done to address consumer privacy concerns, and reach \$17 billion if those concerns were addressed.¹⁰ In fact, actual online spending in 2000 was \$27 billion—far exceeding both forecasts.¹¹

Moreover, another recent survey found no significant difference in Americans’ concerns about shopping online and offline. Among those who

6. FTC Commissioner Orson Swindle noted in dissenting from the 2000 FTC Online Privacy report, “The FTC, however, never compiled or generated any solid empirical evidence concerning to what extent consumers are not purchasing online because of privacy concerns, much less that they would purchase if the government imposed privacy requirements.” Orson Swindle, *E-Commerce: The Future of Banking and Financial Services*, Address at the Suffolk University Law School (June 16, 2000), at <http://www.ftc.gov/speeches/swindle/fedbsn000621.htm> (last visited April 2, 2002).

7. See generally “Pitfalls in Data Analysis,” ERIC/AE Digest, available at http://www.ed.gov/databases/ERIC_Digests/ed410231.html (last visited May 31, 2002)

8. See generally Harper and Singleton (2001).

9. Jupiter Communications, *Proactive Online Privacy: Scripting An Informed Dialogue to Allay Consumers’ Fears*, (June 1999) cited in FTC (2000), at 2.

10. Jupiter forecasts cited in Harper and Singleton 8 (2001), supra note 1, at 8.

11. U.S. Census Bureau, supra note 1.

had used credit cards to buy something over the phone, 56 percent said they worried that their card numbers would be stolen. The equivalent figure for online purchasers was 54 percent.¹² Certainly these figures indicate significant numbers of consumers are concerned about credit card fraud, but these concerns are general and do not justify singling out online shopping.¹³

12. Susannah Fox, The Pew Internet & American Life Project, *Trust and Privacy Online: Why Americans Want to Rewrite the Rules* (August 20, 2000), at 13, at http://www.pewinternet.org/reports/pdfs/PIP_Trust_Privacy_Report.pdf.

13. A recent study conducted by the Department of Commerce and relying on Census Bureau data finds a slightly different answer for overall privacy concerns (as opposed to credit card fraud worries). It finds that 51 percent of respondents were more concerned about confidentiality over the Internet than over the telephone. Another 41 percent were equally concerned about confidentiality in both mediums, and around 8 percent were less concerned about the Internet than the phone. The question asked was comparative only, so we cannot directly compare percentages worried about confidentiality over the Internet with those worried about it over the phone. See US Department of Commerce: National Telecommunications and Information Administration, *A Nation Online: How Americans Are Expanding Their Use of the Internet*, at 77 (February, 2002), at <http://www.ntia.doc.gov/ntiahome/dn/anationonline2.pdf> [hereinafter NTIA (2002)].

B. Factors Other Than Privacy Concerns Affect Online Shopping

Privacy advocates have not made a compelling case that concern for privacy is the most important factor inhibiting online purchases. An Ernst and Young study found that "...high shipping costs discourage people from buying online more than any other single reason."¹⁴ In their survey, 53 percent of non-online purchasers gave this reason for not shopping over the Internet. Only 20 percent mentioned a lack of confidence in the online merchant as the reason for not shopping. A concern that merchandise cannot be easily returned apparently also deters some potential Internet shoppers.¹⁵

Consider who seems to be most hesitant about shopping online. A recent Pew study found that "[c]oncerns about privacy are notably higher among some groups, especially Internet novices (those who first got online within the past six months), parents, older Americans, and women."¹⁶ Lack of confidence about the Internet in general, which novices and older Americans are likely to experience, will undoubtedly slow the use of online shopping by these groups regardless of federal regulations.¹⁷

Misplaced fears may also be driving some consumer worries about online privacy and security. A recent American Express study points out that "gaps in consumer knowledge about the Internet [suggest] that much of the apprehension about the online world could be eliminated through better

14. Ernst & Young, *Global Online Retailing, An Ernst & Young Special Report*, STORES, (January 2000), at 19, at <http://www.stores.org/archives/archives00.html>. Corroborating the numbers reported above found by the Pew study: see Fox, *supra* note 12. Ernst & Young report that 50 percent of those surveyed who have not shopped online mentioned the fear of entering credit card numbers over the Internet as one reason. A study by Jupiter Media Metrix supports the finding that shipping costs discourage Internet shopping. That study finds that "shipping and handling (S&H) charges have dissuaded 63 percent of consumers from completing online purchases." Jupiter Communications, *Shipping and Handling Charges Deter 63 Percent of Consumers From Buying Online* (June 11, 2001) (Press Release). Jupiter press releases are available online at <http://www.jmm.com/xp/jmm/press/pressreleaselist.xml> (last visited April 2, 2002).

15. "...41 percent of online consumers expressed reluctance to buy online due to concerns over returns, according to a separate consumer survey fielded in October 2001." Jupiter Communications, *Jupiter Online Shopping Index Reaches Record High During Third Week of The Holiday Season* (December 13, 2002) (Press Release).

16. Fox (2000), at 16. The Department of Commerce study corroborates the finding that concern about confidentiality online is considerably higher among older Americans (55 percent of respondents 55 years and older as compared to 36 percent for respondents under 25 years of age). NTIA (2002), at 77.

17. A survey conducted by AARP found that among computer users age 45 and older "nearly four in ten (39 percent) are not confident about executing business transactions [online], including 24 percent who are 'not at all confident'." AARP, *AARP Survey: Many Americans Face E-Commerce Skills Gap* (News release), at <http://www.aarp.org/press/2000/nr033000.html> (last visited April 2, 2002).

education and awareness of its opportunities and benefits.”¹⁸ Indeed, the Pew study found that “[t]he actual incidence of unpleasant events [online] is modest and the incidence of criminal events online is miniscule...”¹⁹ Some 19 percent of Internet users have been the victims of credit-card fraud or identity theft. But in four out of five of those cases the theft apparently occurred offline. Just eight percent of the victims reported that the information had been stolen online.²⁰

The point of the statistics presented above is not that consumers are not worried about privacy online or that security is not an issue for Internet shopping. The surveys showing high percentages of people concerned about shipping costs or about hassles over returned merchandise suffer from the same problems as the surveys and forecasts privacy advocates use. Talk is cheap and finding a study to support your particular argument is relatively easy. But the burden of proof should lie with those calling for more regulation—it is not at all clear that the desired regulation will result in benefits that significantly exceed costs.²¹ Thus far, as we discuss further in the following section, the data do not support arguments of a market failure in need of government regulation.

III. THE CASE FOR FEDERAL REGULATION IS WEAK

The statistics on “lost” sales, consumer concerns, and incidents of fraud do not support the argument that e-commerce needs special protection as compared to more traditional commerce. Nonetheless, if privacy advocates could tie the need for regulation to evidence of an online market failure, their case would be made.²² Is there a good reason to believe that firms do not have adequate incentives to protect consumers’ information privacy and security when they make online purchases?

18. American Express, *Online Attitudes Move in Line Across the Globe*, *The American Express Global Internet Survey* (October 2000), at 9.

19. Fox (2000), at 3.

20. Fox (2000), at 13.

21. When the benefits of a proposed policy exceed the costs, it is sometimes said to be more economically efficient than the status quo. For a general discussion and defense of the use of economic efficiency, see LOUIS KAPLOW AND STEVEN SHAVELL. *FAIRNESS VERSUS WELFARE* (2002).

22. A market failure can arise, for example, if there are differences in the amount of information easily available to buyers and sellers or if the private and social costs of production differ. See, for example, Francis M. Bator, *Anatomy of a Market Failure*, 72 Q.J. Econ. 351 (1958); George A. Akerlof, *The Market for 'Lemons': Quality Uncertainty and the Market Mechanism*, 84 Q.J. Econ. 488 (1970).

A. Company and Industry Efforts Indicate Increasing Consumer Privacy

Clearly, firms understand that online sales depend on their ability to allay consumer concerns about security and privacy. That does not mean, however, that the incentive structure is perfect. Consumers, for example, may find it costly or impossible to ferret out how some personal information they provide to complete a transaction is being used by Web merchants. New technologies like the Platform for Privacy Preferences Project (P3P) should help in this regard, though. P3P is an industry led effort that enables Web sites to post their privacy practices in a standardized, machine-readable format that can be automatically retrieved and interpreted by a consumer's computer. If the site's policy is not in line with the consumer's wishes (as defined in a P3P file residing on the consumer's computer), the consumer is warned and can decide not to visit that site.²³ Even though P3P was not available until late summer in 2001, Microsoft's most recent Web browser, Internet Explorer 6.0, supports P3P, as do 25 percent of the most frequently visited U.S. based Web sites.²⁴

Another industry-led initiative may help consumers identify sites with meaningful privacy policies. Programs like TRUSTe, BBBOnLine Privacy Seal and SAFEcertified.com evaluate privacy policies and provide sites that post clear privacy protection policies with their seals of approval.²⁵ According to a recently conducted survey of U.S. based Web sites, over 40 percent of the most frequently visited sites have earned a privacy seal.²⁶

23. See W3C Platform for Privacy Preferences Initiative, P3P and Privacy on the Web: FAQ, at <http://www.w3.org/P3P/> (last visited March 26, 2002). W3C members include AOL, AT&T, Citigroup, Hewlett Packard, IBM, Microsoft, NCR, NEC, and Netscape, to just name a few. Some advocates of P3P technology argue that it could evolve into a personal privacy advocate, enabling machine to machine negotiation at each Web site. See Lawrence Lessig, *The Architecture of Privacy*, Second Draft (April 3, 1998), at http://cyber.law.harvard.edu/works/lessig/architecture_priv.pdf (pointing out that with P3P “. . . machines can bear the costs of this negotiation. Machines, that is, could be our agents for protecting our privacy.”). Opponents of P3P argue that even machine-to-machine negotiations may be too complicated and require too many privacy sacrifices on the part of consumers. See, e.g., Electronic Privacy Information Center, *Pretty Poor Privacy: An Assessment of P3P and Internet Privacy* (June 2000), at <http://www.epic.org/Reports/pretypoorprivacy.html> (last visited March 26, 2002).

24. William F. Adkinson et al., Progress and Freedom Foundation, *Privacy Online: A Report on the Internet Practices and Policies of Commercial Web Sites*, at 26 (March 27, 2002), at <http://www.pff.org/publications/privacyonlinefinalael.pdf>. The data are “directly comparable” to those contained in the May 2000 FTC report; FTC (2000), supra note 3, at 3.

25. See TRUSTe, *Privacy Statement*, at http://www.truste.org/truste_privacy.html (last visited September 4, 2001); Better Business Bureau OnLine, *Online Privacy Policy*, at <http://www.bbbonline.org/about/privacy.asp> (last visited September 4, 2001); SAFEcertified.com, *Privacy Policy*, at <http://www.safecertified.com/betasf/privacypolicy.asp> (last visited June 12, 2002).

26. Adkinson et al. (2002), supra note 24, at 24-25.

Consumers visiting these sites can simply check for a seal and then, if they wish, read a merchant's privacy policy before shopping at the site.

Seal programs have the potential to solve the problem of asymmetric information.²⁷ The Better Business Bureau takes on the task of verifying the information a Web site collects and how that site uses its information and then grants the site its *BBBOnline* seal when the privacy policy is understandable and offers a basic level of protection. Thus far, however, the seal programs have not required Web sites to stand by their privacy policies. Neither *BBBOnline* nor *TRUSTe* charge fines or otherwise penalize a site for changing or violating its policy. This lack of enforcement could explain the stunted growth of seal programs. While *BBBOnline* and *TRUSTe* both report increasing memberships, the percentage of frequently visited Web sites posting a seal is little changed from the May 2000 findings reported by the FTC. Nonetheless, the potential for seal programs to play an important role in providing information remains.

Given industry-led developments like seal programs and P3P, before regulating online privacy one must ask whether additional government intervention is likely to do more good than harm.²⁸

Individual online vendors are deeply involved in addressing privacy concerns as well. The 2000 FTC study mentioned earlier found that 100 percent of the "most popular" U.S. Web sites (measured by the number of unique visitors) and over 80 percent of all U.S. based Web sites already post privacy policies.²⁹ A study conducted in December 2001 that replicated the FTC's methodology confirmed these statistics. It also found that policy notice content had improved since May 2000.³⁰ More importantly, the 2001 study found that fewer sites were even collecting personally identifiable information: among the 85 most frequently visited Web sites, the percentage collecting personal information (excluding email addresses) fell to 84 percent from the 96 percent reported by the FTC 2000 report.³¹

²⁷ Asymmetric information refers to situations in which a buyer and seller may possess or have access to different information about a product. In the classic example, a potential purchaser of a used car cannot determine whether the car is a "lemon"—something the original owner and seller knows from experience. See Akerlof – Market for Lemons – qje paper. +m: pls get cite out of me reference list.

²⁸ This concern is treated more generally in CATE (1997) and Hahn and Layne-Farrar (2002). Both studies argue that additional online privacy regulation is not warranted at this time based on existing data on the costs and benefits. For an opposing view, see Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 STAN.L. REV. 1193 (1998).

²⁹ FTC (2000), *supra* note 3, at ii-iii.

³⁰ Adkinson et al. (2002), *supra* note 24, at 18.

³¹ Among the random sample of 309 domains, information collection fell from 87% in May 2000 to 74% in December 2001. Adkinson et al. (2002), at vii.

Web sites are also offering consumers more of a say in whether their information is shared. The 2001 survey of Web sites found that 93 percent of the most popular sites offer consumers a choice in whether their personal information is shared with third parties; that is up from 77 percent in the FTC 2000 report.³² Opt-in, the practice of requiring consumers to actively consent before information is shared rather than allowing sharing unless consumers object, is on the rise as well.³³ Thirty-two percent of the most popular sites require opt-in before information is shared with third parties, more than twice as many as the 15 percent reported by the FTC in May 2000.³⁴

Of course, the above statistics include many Web sites that do not offer online shopping or commerce of any kind. A recent report focusing strictly on e-mail marketers found that 94 percent allow customers to select out of future e-mail solicitations.³⁵ The survey also found that around three quarters of online marketers do not send unsolicited commercial e-mails and the majority do not rent third-party customer lists.

Advertisers exert additional pressure on online retailers to respect consumer privacy. Some prominent companies, including American Express, Compaq, Disney, IBM, Microsoft and Proctor & Gamble, refuse to advertise on Web sites that do not have a posted privacy policy.³⁶

Sites offering sub-standard privacy protection presumably suffer if consumers refuse to shop there. For example, AOL cancelled its plans to sell subscribers' telephone numbers to telemarketers after AOL members complained.³⁷ Thus if privacy is genuinely a driver of e-commerce, online

32. Adkinson et al. (2002), at 21.

33. Opt out is the practice of sharing personal information unless (or until) a consumer objects. Opt in and opt out mechanisms provide for significant differences in the information available for use by Web sites and by others, such as credit agencies and the FBI. See Hahn and Layne-Farrar (2002), supra note 4, for detailed discussions of the meanings of choice and its implications.

34. Opt in is up from 11 percent to 18 percent in the random sample. Adkinson et al. (2002), at 21-22.

35. The survey contacted 700 U.S. companies; the report was issued by the Direct Marketing Association (DMA). See Sandra Swanson, *Most E-Mail Marketers Let Customers Opt Out, Report Says*, INFORMATIONWEEK, March 22, 2002, at <http://www.informationweek.com/story/IWK20020322S0011>. For information on the DMA, see <http://www.the-dma.org/> (last visited March 26, 2002).

36. Paul H. Rubin and Thomas M. Lenard, Progress and Freedom Foundation, *Privacy and the Commercial Use of Information*, at 51 (July 2001), at <http://www.pff.org/RubinLenard.pdf>.

37. See Jessica Litman, *Information Privacy/Information Property*, 52 STAN. L. REV. 1283, 1305 (2000), (citing Rajiv Chandrasekaran, *AOL Cancels Plan for Telemarketing: Disclosure of Members' Numbers Protested*, WASH. POST, July 25, 1997, at G1) (stating dismayed consumers flooded AOL with complaints until the company abandoned its plans). For additional examples of companies altering their information sharing plans after angry consumer reactions, see Hahn and Layne-Farrar (2002), at 108-109.

merchants have every incentive to convince consumers that they do protect personal information. After all, consumers unhappy with an online merchant can turn to traditional brick-and-mortar stores or to catalog phone shopping. Indeed, catalogs are a close substitute for Internet shopping in terms of convenience, but catalog shopping has been around since the late 1800s and is far more familiar to consumers.³⁸

B. Web Merchants Have Strong Incentives to Provide Information Security

Under current practices, online merchants have a stronger incentive to resolve consumer fraud issues than typical offline firms. While credit card fraud committed in a traditional brick-and-mortar setting is the financial responsibility of the banks that issue the cards, Web merchants are generally responsible for online credit card fraud.³⁹ The costs are substantial: according to one trade news source, “Fraud costs eMerchants an average of five percent of their gross sales, severely eroding profit margins and potentially causing business failures.”⁴⁰ Costs like these have led e-commerce sites to be more proactive in preventing fraud. An analyst with Gartner Inc. notes that online merchants terminate one in every 20 online sales because it “looks suspicious.”⁴¹ Hence it seems unlikely that Internet merchants need prodding by Washington to provide tight security.

Not surprisingly, then, online sellers appear to be addressing consumers’ security worries. The 2001 follow-on survey to the FTC’s 2000 report found that among frequently visited Web sites 72 percent currently disclose that they take security precautions after data are collected, as compared to 48 percent in 2000.⁴² In addition to protecting consumer information after it is collected, methods are now available to protect information before it is transmitted. For example, a recent survey commissioned by the National Consumers League found that two consumers in three would prefer to use some substitute for traditional plastic in paying

38. For a discussion of the history of catalog sales, see ROBERT J. GORDON, *THE MEASUREMENT OF DURABLE GOODS PRICES* 417-424 (1990). Online shopping does have one advantage over catalog shopping: products, prices, and availability are likely to be updated more frequently.

39. *Fraud-Check Launches Online Ecommerce Fraud Detection Solution Developed with Integrated Information Systems*, BUSINESS WIRE, October 9, 2001, available in LEXIS. In addition to being responsible for fraudulent charges, Internet merchants must pay higher credit card fees since they deal in “card not present” transactions (i.e., no signature is obtained). Donna Howell, *Credit Card Fraud Continues to Dog Internet Sales, Says New Gartner Report*, INVESTOR’S BUS. DAILY, March 6, 2002, available in LEXIS.

40. *Fraud-Check Launches Online Ecommerce Fraud* (2001), supra note.

41. Avivah Litan, cited by Donna Howell (March 6, 2002), supra note 39.

42. Adkinson et al.(2002), at 23.

for online transactions.⁴³ Such products are now in advanced stages of development by several companies. In particular, American Express offers single-use credit card numbers linked to a permanent account.⁴⁴ And Visa is developing an authentication process that allows online merchants to verify a customer's identity and credit card account without requiring that a customer's card number travel across the Internet.⁴⁵

In addition to the industry efforts underway, tools exist to aid consumers in protecting their own information privacy and security. For example, anonymous Web surfing software used in combination with single-use credit cards can keep an e-commerce Web site from obtaining personal information from shoppers.⁴⁶ In fact, Internet users may prefer a self-protection approach. According to the Pew-sponsored survey, half of the Americans who surf the Web would prefer to control their own protection, while just one in four would put the federal government in charge.⁴⁷

Consumer and Web merchant incentives thus appear to be well aligned for e-commerce. Shoppers may vote with their feet, refusing to spend money at Web sites that do not provide the privacy and security demanded. In fact, this kind of pressure may be behind the increased privacy and security measures reported above. If e-commerce sites are still not providing the level of privacy protection that federal regulation advocates envision, it may be that privacy is simply not a top priority for Internet shoppers.⁴⁸

43. *The National Consumers League Online Shopping Survey Highlights Substitute and Single-Use Credit Card Numbers as a Safe Way to Shop This Holiday Season*, BUSINESS WIRE, October 9, 2001, available in LEXIS. A recent survey by Visa reports similar findings: 70% of consumers said they would feel safer making purchases on the Web if they had a password verifying their identity. *First USA Boosts Online Shoppers' Confidence; Verified by Visa Service Offers Online Security to Cardholders*, BUSINESS WIRE, January 16, 2002, available in LEXIS.

44. Rather than use an actual credit card number online, a user of a single-use credit card number receives and uses a unique number each time a transaction is made. The unique numbers are linked to the consumer's actual account. See American Express, Private Payments, at http://www26.americanexpress.com/privatepayments/info_page.jsp (last visited April 2, 2002).

45. *First USA Boosts Online Shoppers' Confidence; Verified by Visa Service Offers Online Security to Cardholders*, BUSINESS WIRE, January 16, 2002, available in LEXIS. See Visa's Web site also, at http://www.usa.visa.com/personal/secure_with_visa/secure_commerce_program.html (last visited April 2, 2002).

46. For information on anonymous Web browsing, see, e.g., Freedom – Internet Privacy & Internet Security, Internet Privacy Suite, available at <http://www.freedom.net/products/standard/index.html?product=standard> (last visited Oct. 29, 2001). Single-use credit cards, used much like a pre-paid phone calling cards, can provide anonymity for Internet shopping. See American Express, Private Payments, supra note 44.

47. Fox (2000), at 6. As noted earlier, the Pew survey suffers from the standard problems associated with survey data. Nonetheless, it is interesting to note the lack of enthusiasm for government intervention.

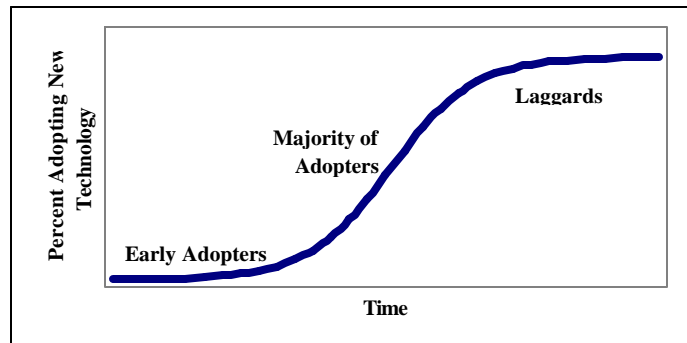
48. A survey conducted in March 2001 by Jupiter Media Metrix suggests this may, in fact, be the case. It finds that 70 percent of online shoppers register to receive email notices of new products and special offers; 50 percent register to store personal information on a Web site; and 41 percent

IV. E-COMMERCE GROWTH IS NOT NECESSARILY SLOW

A. Adopting New Technology Takes Time

Researchers have generally found that the adoption of new technologies is sluggish at first. In fact, a substantial literature on technology adoption rates shows that acceptance usually follows an “S curve” pattern, as shown in Figure 1.⁴⁹ Phase 1, the bottom of the curve, is defined by a small group of “early adopters.” These early adopters are less sensitive to perceived risk or see greater benefits to adoption than others. In phase 2, the sharply rising part of the curve, the majority of potential users adopt the technology. This group of users needs to be persuaded, not merely informed, about the new technology.⁵⁰ Thus, they benefit from observing the experiences of early adopters. Finally, in phase 3, the flat portion at the top of the curve, the “laggards” adopt.⁵¹ This last group sees less benefit in adopting the technology, is especially resistant to change, or is more isolated and thus observes the benefits of adoption later than others.

Figure 1. The Diffusion S-Curve



register to receive physical mail. Moreover, 85 percent of online shoppers stated that they were very or somewhat more likely to return to a site after receiving an email message from a retailer. See Jupiter Press Release: *Reports Of The Death of Online Retail Are Greatly Exaggerated* (May 22, 2001).

49. For an early and influential analysis, see EVERETT M. ROGERS, *DIFFUSION OF INNOVATIONS* (1962). Also see a Department of Commerce report, which argues that adoption of new technologies involving network effects (such as the Internet) begin slowly. U.S. Department of Commerce, *Falling Through The Net: Toward Digital Inclusion 2-4* (October 2000), at <http://www.ntia.doc.gov/ntiahome/fttn00/contents00.html>.

50. Paul Geroski, *Models of Technology Diffusion*, Centre for Economic Policy Research, Discussion Paper No. 2146 (May 1999).

51. Sunil Sharma, *Behind the Diffusion Curve: An Analysis of ATM Adoption*, UCLA Economics Working Papers 686, at 11 (1992).

A “slow” start is thus typical for the adoption of new technologies. This is especially true when the technology requires a significant commitment on the part of the adopter, as is the case for e-commerce. Consumers new to e-commerce need to familiarize themselves with ways of buying and selling on the Internet, and determine where it is best for them to do business. Internet service providers such as America Online are able to lessen the commitment cost of going online by providing free trial periods, during which consumers can test access to the Internet without spending money on it. However, unlike Internet activities such as browsing or research, online shopping can be tried only by committing money, not just time. This raises the price of trying online shopping, and as a result slows the rate of adoption.

Commitment cost factors probably played a role in the cautious adoption of several electronic financial services in the recent past. For example, the use of ATM cards for withdrawing and depositing cash and for making consumer purchases is taken for granted today.⁵² But in the late 1980s, consumers were still leery of the then new technology.⁵³ While banks had distributed 80 million ATM cards to U.S. consumers by 1989, only one in five used their cards at least once a month and one third of the cardholders never used ATMs at all.⁵⁴

Debit cards were similarly slow to take off. In 1988, 87 percent of all retail purchases were paid in cash and only a handful of merchants (mostly gas stations and supermarkets) even accepted debit cards.⁵⁵ By 2000, however, annual purchase volume had reached around \$300 billion, with 250 million cards in circulation.⁵⁶ And by late 2001, debit cards accounted for 8.3

52. In the U.S. alone, over \$11 billion was withdrawn from ATMs in 1999. In a 2001 speech, Federal Reserve Board Governor Laurence H. Meyer noted that “The use of debit cards with personal identification numbers (PINs) for making consumer purchases is growing, and the use of signature-based cards sponsored by the major credit card companies has grown even more rapidly during the past decade. In 2000, there were approximately 3 billion PIN-based debit transactions with a total value of \$138.2 billion and 5.3 billion signature-based debit transactions with a total value of approximately \$210 billion.” Laurence H. Meyer, Address delivered at the Distinguished Lecture Program, Swarthmore College, (December 5, 2001), at <http://www.federalreserve.gov/boarddocs/speeches/2001/20011205/default.htm>.

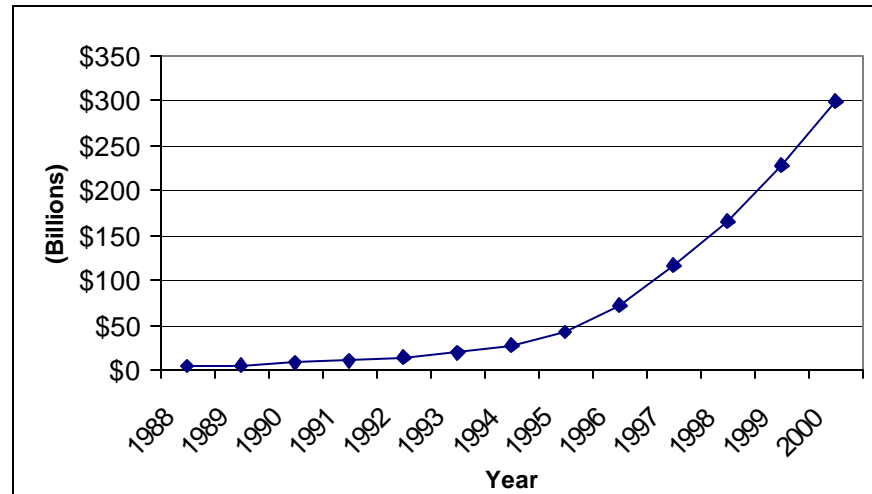
53. One contemporaneous trade press article reported that “many customers still fear deposits made at an ATM will not properly post to their accounts.” D. Mark Jackson, *Are ATM Strategies Changing?*, THE MAGAZINE OF BANK MGMT., April 1987, at 16. Thus, even though depositing funds through an ATM did not “cost” money in the true meaning of the word, it did require consumers to put their money into a “black box” and trust that the box worked as described.

54. John Hillkirk, *Withdrawing from ATMs: Vision of Cashless Future Fades*, USA TODAY, July 31, 1989, at 1B.

55. Hillkirk (1989).

billion transactions worth \$348 billion.⁵⁷ Figure 2 charts the dramatic rise in debit card spending over the period from 1998 through 2000.

Figure 2. Debit Card Spending in the U.S., 1988-2000



Source: The Nilson Reports.

B. E-Commerce Growth Appears Strong

Adoption rates for e-commerce are likely following the same slow start of the standard S-curve adoption pattern as did the electronic financial products discussed above. Ecommerce would necessarily be in the early phases of adoption because the World Wide Web is still fairly new. While it was first released in 1991, the Web did not achieve widespread popularity until around 1997.⁵⁸ Unfortunately, we do not have statistics on adoption rates over time for e-commerce, but available statistics suggest that growth has been healthy.

Online transactions have grown substantially over the past few years, with 4.9 million credit card transactions in 1997, 9.3 million in 1998 and

56. Federal Reserve Bank: Check and Electronics Payment Research Project (November 2001), as cited in *New Payment Methods Give Old-fashioned Checks and Credit Cards a Run for Their Money*, MANAGING TECHNOLOGY, at <http://knowledge.wharton.upenn.edu> (last visited April 2, 2002). A forecast developed by the financial consulting firm Sphere and Associates predicts that by 2005 consumers will rely on debit cards more often than credit cards. *By 2005 Consumers Will Be Using Debit Cards*, CNNFN, March 12, 2002.

57. *New Payment Methods*, supra note.

58. CERN – European Organization for Nuclear Research, History and Growth, at <http://public.web.cern.ch/Public/ACHIEVEMENTS/WEB/history.html> (last visited February 6, 2002).

19.2 million through the third quarter of 1999.⁵⁹ That is, the number of online credit card transactions roughly doubled each year. The average number of transactions per online shopper increased as well, rising from four in 1997, to six in 1998 to 13 in 1999.⁶⁰ The Pew survey, conducted in 2000, found that 48 percent of Internet users have bought something online with a credit card.⁶¹ Moreover, a government study found that the number of Americans using the Internet grew to 54% of the U.S. population in 2001, up 26% from 2000.⁶² Looking at the entire U.S. population over the age of 3, a report issued by the U.S. Department of Commerce found that 21 percent made online purchases as of September 2001, compared to 13 percent in August 2000.⁶³ Thus, we are observing more people using the Internet and larger numbers engaging in transactions online.

Statistics for online consumer retail spending show sharp increases as well.⁶⁴ Online holiday retail purchases grew from just over \$1 billion in 1997 to just under \$14 billion in 2001, as shown in Figure 3.⁶⁵

59. Harper and Singleton (2001), *supra* note 1, citing Cyber Dialogue, *Best Practices in Online Customer Privacy Protection*, April 2001.

60. Ernst & Young (2000), *supra* note 14, at 5.

61. Fox (2000), at 3.

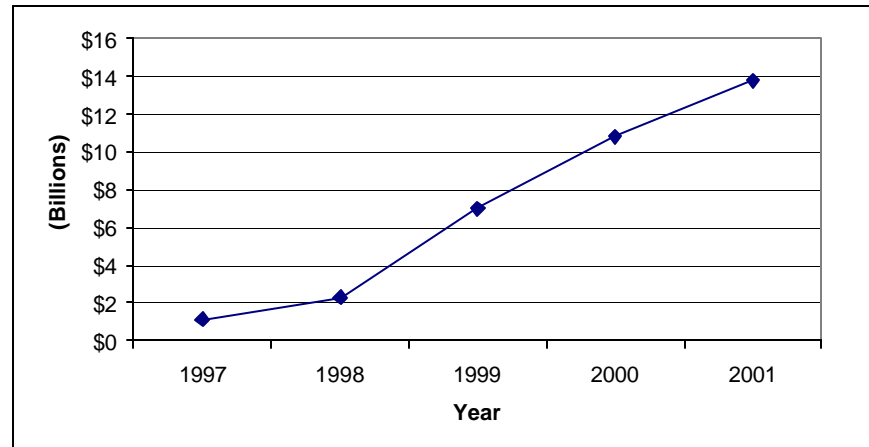
62. Yochi J. Dreazen, *American Web Usage Reached 54%, In Autumn, Government Study Says*, THE WALL STREET JOURNAL ONLINE, February 4, 2002, at <http://online.wsj.com>.

63. NTIA (2002), at 30. Note that the 2000 figure, 13 percent, also includes people using online banking. The 2001 figure, 21 percent, is solely for online shopping. An additional 8 percent conducted online banking in 2001, making the comparison 13 percent to 29 percent. The study reports a somewhat smaller percentage of Internet users shopping online than the Pew study. The Department of Commerce finds 39 percent of Internet users purchase products and services online. *Id.*, at 31. Among 25 to 34 year olds, however, the Department of Commerce finds that 53 percent of Internet users shop online. *Id.*, at 32. The difference as compared to the Pew study may, therefore, reflect the age composition of the Pew sample.

64. Researchers following e-commerce have drawn the same conclusion. Ernst & Young note, "As you look at the countries in our report —Australia, Canada, France, Italy, the UK, and the U.S.—it is clear that there is a market life-cycle for e-tailing. The U.S. is the only market of the six that has moved out of the startup phase of the cycle into a fast-growth, 'penetration' phase." Ernst & Young (2000), *supra* note 14, at 7. In our terminology, Ernst & Young argue that e-commerce has entered phase 2.

65. Various press releases by Jupiter Media Metrix: *Holiday Online Sales Hit \$2.3 Billion, But Gift Opportunity Still Untapped* (November 2, 1998); *Online Holiday Sales Hit \$7 Billion, Consumer Satisfaction Rising* (January 13, 2000); *Jupiter Online Shopping Index Reaches Record High During Third Week of The Holiday Season* (December 13, 2001). For 2001 statistics, see Goldman Sachs, Harris Interactive, and Nielsen/Net Ratings study (December 2001), as cited in Helen D'Antoni, *E-Business Proves A Worthy Investment*, INFORMATIONWEEK, January 14, 2002, at <http://www.informationweek.com/story/IWK20020110S0006>. The "Holiday" period is defined as November 1 through December 31 and typically contributes at least one-third of annual retail purchases, regardless of the sales channel.

Figure 3. Annual Online “Holiday” Season Spending in the U.S., 1997-2001.



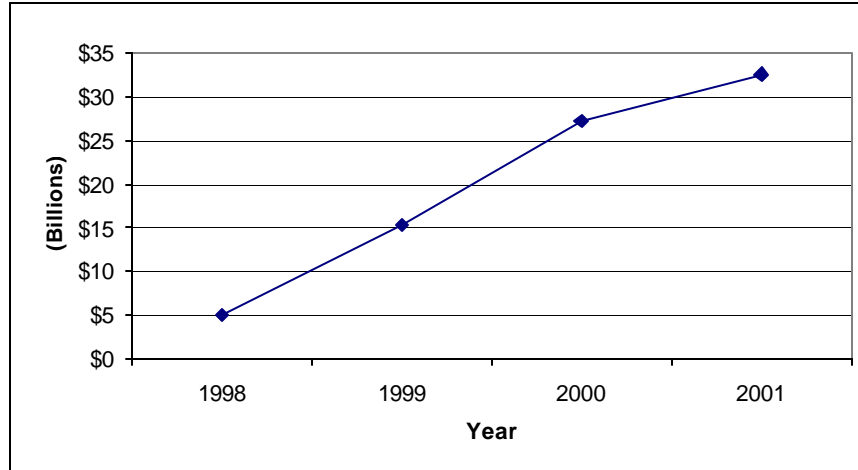
Sources: Jupiter Media Metrix; Goldman Sachs, Harris Interactive, and Nielsen/Net Ratings study.

Full-year online retail statistics present a similar picture.⁶⁶ Annual online consumer purchases are presented in Figure 4 for 1998 through 2001. Annual consumer purchases were slightly over \$5 billion in 1998, but were up to \$32 billion by 2001.⁶⁷ In fact, online sales grew much faster than total retail sales: 2001 e-commerce sales increased 19.3 percent over 2000 while total retail sales only increased 3.3 percent.⁶⁸

66. The annual data follow a similar pattern to the Holiday statistics. The data do not begin until 1998. See U.S. Census Bureau, *4th quarter 2001 release*, supra note 1.

67. Forrester Research reports considerably higher annual statistics than the U.S. Census Bureau. According to their analysis, total online retail sales were \$42.4 billion in 2000 and \$47.6 billion in 2001. See Forrester Research Press Release, *December Shopping Up From Last Year In Spite of Rough Economy, According To The Forrester Research Online Retail Index* (January 24, 2002) at <http://www.forrester.com/ER/Press/Release/0,1769,678,00.html>

68. “Retail E-Commerce Sales in Fourth Quarter 2001 were \$10.0 Billion, up 13.1 Percent from Fourth Quarter 2000.” U.S. Census Bureau, *4th quarter 2001 release*, supra note 1. Online retail sales contributes around 1 percent to total retail sales.

Figure 4. Annual Online Retail Sales in the U.S., 1998-2001

Source: U.S. Census, 1998, 1999 and 2001 Annual Retail Trade Surveys.

In addition to the steady growth of online spending, profiles of online shoppers are consistent with what one would expect in an S-curve adoption scenario. Early online shoppers were commonly male, affluent, under 40, and well educated—typical of early adopters in general.⁶⁹ Online shopping may be moving out of the early adoption phase, though. A study by Jupiter Media Metrix predicts that the number of online shoppers age 50 and older will triple and that shoppers' average income will fall between 2002 and 2006.⁷⁰ The Department of Commerce study is consistent with this finding: Internet use among the lowest income bracket, those earning less than \$15,000 a year, increased at an annual rate of 25 percent in 2001.⁷¹

As the demographics of online shoppers change, so too will the types of products available for online purchase. Reflecting an increase in female

69. Ernst & Young (2000), at 12. See also, Federal Reserve Bank: Check and Electronics Payment Research Project (November 2001), as cited in *New Payment Methods Give Old-fashioned Checks and Credit Cards a Run for Their Money*, supra note 56. Early ATM users were also younger, well-educated people. See Jeffrey Kutler, *Poll Shows Need for Marketing to Stimulate Frequent ATM Use*, THE AMERICAN BANKER, September 30, 1988, available in LEXIS.

70. Bob Tedeschi, *Though There Are Fewer New Internet Users, Experienced Ones, Particularly The Middle Aged, Are Increasingly Shopping Online*, N.Y.TIMES, March 4, 2002, at C7. See also, Jupiter Media Metrix Press Release, *Tomorrow's Online Shopper Will Be Older and Less Affluent, Reports Jupiter Media Metrix* (March 4, 2002).

71. NTIA (2002), at 1.

shoppers online,⁷² Ernst and Young report that “Just a year or two ago, categories like apparel were not considered appropriate for online retailing. Today, online apparel sales are accelerating rapidly.”⁷³ And Jupiter anticipates that prescription drugs and home products will experience increases as well, due largely to increasing numbers of women and older Internet buyers.⁷⁴

72. The US Department of Commerce study reports that, as of September 2001, males and females were using the Internet in equal proportions, with both usage rates around 54 percent. NTIA (2002), at 15.

73. Ernst & Young (2000), at 6.

74. Jupiter Press Release (March 4, 2002), *supra* note 70.

V. CONCLUSIONS

The e-commerce marketplace is evolving rapidly. E-commerce sales, though still a small fraction of total retail sales, are growing at a much faster rate.⁷⁵ Recent analysis emphasizes that private companies and industry groups are continuing to address privacy and security issues. Consumers are seeing more privacy notices on Web sites; they are being offered more opportunities to tell Web sites not to share their information; and they are able to choose from a widening array of security enhancing services, like credit card authentication procedures. This process naturally takes time as new services and technologies are developed to meet consumer needs.⁷⁶ An examination of the growth of e-commerce suggests that its rate of diffusion is broadly consistent with other similar innovations.

It is critically important to develop evidence on the benefits and costs of regulation before moving forward with further regulation of e-commerce. As FTC Commissioner Swindle aptly noted, "Before an agency recommends that Congress pass legislation to impose regulatory requirements, it should make a concerted effort to compile and analyze data on the costs of such requirements. This analysis is particularly important with regard to e-commerce because regulatory compliance costs may be high enough to serve as a barrier to entry and many prospective online entrants are small businesses."⁷⁷ It is, of course, also important to consider the benefits of further regulatory requirements. But in this case, we have argued that the benefits are likely to be largely illusory. There is a very real danger that federal regulation of a market that is changing rapidly, such as e-commerce, could impose net costs on consumers.

Privacy advocates would like to use the alleged slow growth of e-commerce as a justification for further regulation of the Internet. The evidence, however, does not suggest a problem worth fixing. While some consumers, particularly older Americans and those new to the Internet, are clearly concerned about online privacy and security, these issues do not appear any more urgent for online shopping than offline shopping. Nor do these issues emerge as significant deterrents to e-commerce. Indeed, it is not even clear that any e-commerce has been deterred. Absent evidence of a significant market failure, the case for further government intervention is weak at best.

75. E-commerce composed 1% of total retail sales in 2001, according to U.S. Census data. U.S. Census Bureau, *supra* note 1.

76. Geroski observes that, "Diffusion is as much a process by which new technologies are developed as it is a process by which usage spreads ..." Geroski (1999), *supra* note 50, at 41.

77. Swindle (2000), *supra* note 6.