

1-1-2006

I Always Feel Like Someone Is Watching Me: A Technological Solution for Online Privacy

David Goldman

Follow this and additional works at: https://repository.uchastings.edu/hastings_comm_ent_law_journal

 Part of the [Communications Law Commons](#), [Entertainment, Arts, and Sports Law Commons](#), and the [Intellectual Property Law Commons](#)

Recommended Citation

David Goldman, *I Always Feel Like Someone Is Watching Me: A Technological Solution for Online Privacy*, 28 HASTINGS COMM. & ENT. L.J. 353 (2006).

Available at: https://repository.uchastings.edu/hastings_comm_ent_law_journal/vol28/iss3/1

This Article is brought to you for free and open access by the Law Journals at UC Hastings Scholarship Repository. It has been accepted for inclusion in Hastings Communications and Entertainment Law Journal by an authorized editor of UC Hastings Scholarship Repository. For more information, please contact wangangela@uchastings.edu.

I Always Feel Like Someone is Watching Me: A Technological Solution for Online Privacy

by DAVID GOLDMAN*

I.	Introduction.....	353
II.	Development of Online Profiling and Attempts at Regulation	361
A.	Profiling and Advertising.....	364
B.	The Efficiency Lost from Profiling in the Current System.....	367
1.	Marketers Both Over- and Under-Produce Advertising	367
2.	The Unreasonable All-Or-Nothing Choice	368
3.	Loss of Trust Online.....	369
C.	Privacy Theories – Off and Online	371
1.	The Property Rights Approach.....	372
2.	The Tort Law Approach.....	374
3.	The EU Approach	375
D.	The Current Absence of Legislation	378
III.	Technology as a Market Creator.....	381
A.	Detailed Description of the Technology	383
B.	The Role of the Government	392
1.	Mandatory Adoption.....	392
2.	Create a Cause of Action.....	396
IV.	Benefits From The Automated System.....	398
A.	Benefits for Both Consumers and Websites	399
B.	Website Specific Benefits.....	401
C.	Advantages for the Government.....	403
D.	Commodifying Privacy	406
V.	Conclusion	407

I. Introduction

Robbie the Robot, R2-D2 and similar robot-heroes are some of the most popular characters in many science fiction stories. These

* Staff Law Clerk, Seventh Circuit, U.S. Court of Appeals; J.D., University of Pennsylvania 2003. For their helpful comments and encouragement, the author would like to thank Gideon Parchimovsky and R. Polk Wagner.

characters are always close at hand loading their memory banks with an enormous array of useful data about their owners, including their tendencies, likes and dislikes. This personal information is collected under the assumption that it will be used to better serve their compatriots; but what would happen if those "memories" fell into the wrong hands? All that stored information could be used for harmful purposes. The question thus presents itself: do we really want to own R2-D2?

Although modern machines do not yet have vibrant personalities, they are storing a great deal of personal information. The computer can attempt to use the stored data to ease the user's burden while they surf the web. When a person decides to purchase a book, for instance, a personal computer can communicate with a website to prepare to purchase the book, have suggestions for other products in which the user might be interested, and offer discounts for those goods.¹ The current day version of R2-D2 would not only offer Luke Skywalker his lightsaber, but also suggest alternate brands and maybe a discount on an accompanying blaster.

This sort of near telepathic technology was first being put to use in the middle to late 1990s.² Online stores were beginning to recognize and remember users from previous visits to their sites. The stores could offer special bargains for their return customers and simplify the purchasing procedure. Users could subscribe to online newspapers and the sites could distinguish their subscribers and allow them access to special content.

Marketers began to utilize this new technology to observe users' behavior. The marketers could start to use the information about people's online conduct to offer special deals on products in which a user's online activity indicated they might be interested.³ For the first time online, a bargain could be specifically tailored for a single user. Essentially, the World Wide Web was beginning to customize its presentation for each individual consumer. The Internet appeared as

1. For example, Amazon.com, an online bookstore, can currently give recommendations about products in which a user may be interested based on prior purchases, information volunteered by the user, and comparisons with other customers' activity. Amazon.com can then recommend products to a customer as soon as that person visits the site, without the user even having to identify themselves manually to the site.

2. John Schwartz, *Giving Web a Memory Cost Its Users Privacy*, N.Y. TIMES, Sept. 4, 2001 (explaining the invention of technology that allowed websites to recognize users on subsequent visits).

3. *Id.* (discussing some of the benefits from online tracking technology).

though it was on the verge of becoming a utopian market for information.

The companies that were developing this near perfect cyber-world overlooked several important issues, however. First, just like the movie robots, in order for the web to tailor the information it presented to a user it had to collect detailed data about that user – and the more detailed the information the better. An online store could not offer special discounts to specific customers if the site could not distinguish its customers and where their interests may lay. A tension arose, however, because many people felt as though their visit to the web should be a private activity and should therefore be an activity into which others should not intrude.⁴ Websites' desire to collect information about their customers was conflicting with many individuals' sense of personal space.

While the debate over privacy has been going on for over one hundred years, there were a few key differences that made the online problem unique. Primarily, the technology involved with the Internet allowed online surveillance to occur essentially invisibly to the user. It is virtually impossible for a user to keep track of all of the ways that they can be monitored while surfing the web. Also, under the current regulatory model (or absence thereof) for online information, there is almost no way for a user to prevent the collection of their personal information.

In the mid-1990s, the problem was compounded because the web marketers were harvesting information *en masse* without attempting to acquire the users' consent.⁵ The technology that first allowed websites to recognize users – the notorious cookie – was brought on to the scene with little fanfare. It was simply introduced to make online transactions more convenient by allowing websites to remember a user on subsequent visits.⁶ As the web became more

4. See, e.g., FEDERAL TRADE COMMISSION, PRIVACY ONLINE: A REPORT TO CONGRESS 1 (June 1998) [hereinafter 1998 FTC REPORT] ("While the online consumer market is growing exponentially, there are also indications that consumers are wary of participating in it because of concerns of how their personal information is used."), available at <http://www.ftc.gov/reports/privacy3/priv-23a.pdf>; Elec. Info. Privacy Ctr., *Surfer Beware: Personal Privacy and the Internet* (June 1997) (stating that online privacy was one of internet users' top concerns in 1997), available at <http://www.epic.org/reports/surfer-beware.html> (last visited May 25, 2005).

5. See, e.g., Elec. Info. Privacy Ctr., *Surfer Beware: Personal Privacy and the Internet* (June 1997) (few websites in 1997 had posted privacy policies), available at <http://www.epic.org/reports/surfer-beware.html> (last visited May 25, 2005).

6. Schwartz, *supra* note 2 (describing that online tracking technology was originally created to add convenience to online transactions).

popular, web designers were increasingly using cookies to collect more expansive information about an ever-growing online population.⁷ At the time, the data collectors did not pause to consider the harm this practice occasioned on consumers. After all, the owners of the websites felt as though they were just collecting information so they could better serve the customers. Unfortunately, many users did not share this same perspective.

As users were increasingly tracked online, they were beginning to openly express concerns about the collection of their personal information.⁸ Many legislators took their cue and started trying to develop methods to protect personal information. At the same time, the developers of online technology also sought to develop software that could answer consumer calls for more protection online. Internet and privacy scholars have also struggled to overcome the privacy impasse.⁹ Unfortunately, they have not yet been able to overcome the difficulties that both government and industry have encountered. Even the simple definition of what constitutes privacy has proven to be elusive. Worse yet, assuming a definition could be agreed upon, a clear method with which to place a value on privacy has yet to be developed. The twin obstacles of defining and gauging privacy have thwarted any serious efforts to respond to the consumer outcry. The best possible solution is, therefore, to approach the matter from a different perspective. Ironically, the same technology that makes the online privacy problem distinct from the offline issues may also help to solve the problem in a simpler manner than it could be approached offline. Rather than trying to define the nebulous notion of Internet privacy, a more goal-oriented approach may be an improved tactic. In this article, I argue that the existing approach to the privacy conundrum is misguided. Given the vague nature of privacy and the fact that individuals place such wide-ranging values on their personal

7. *Id.*

8. Louis Harris & Assocs. & Dr. Alan F. Westin, *Commerce, Communication, and Privacy Online, A National Survey of Computer Users* 20-21 (1997) ("Of those who use the World Wide Web and have been asked by a site to provide information, the majority have at some point declined to give that information. The majority of those who did not provide the information say they would have provided it if they were aware of, comfortable with, the information use policies of those sites or if they were more familiar with those sites."), available at <http://www.pandab.org/compsurv.html> (last visited May 25, 2005); *Business Week/ Harris Poll: Online Insecurity*, BUS. WEEK, Mar. 16, 1998 at 102 (finding that of those consumers who did not use the Internet as of February 1998, 61% would be more likely to start using the Internet if the privacy of their personal information and communications was protected), available at <http://www.businessweek.com/1998/11/b3569107.htm> (last visited May 25, 2005).

9. See discussion *infra* Part C.

information, all attempts at a one-size-fits-all answer have met with the same fate. I propose that a superior approach for the online issues is to use the strengths of both various technological and governmental privacy models to develop a hybrid solution that allows individuals and marketers to work together to determine their own value for personal information.

An automated system could be designed using existing technology that would allow users' browsers to silently negotiate with websites behind the scenes as users surf the web. A user could program their privacy preferences into their browser before they ever log on to the Internet. When the user subsequently visits a website, the browser would then inform the site of the user's preferences in the course of loading the website onto the user's machine.¹⁰ Based on these preferences, the website's computer can determine the amount of content to offer the user. If a user programs the browser in a way that shows she is uncomfortable offering any personal information to a site, she would receive minimal access to the webpage's content. Conversely, the user could actually volunteer information (an option that is not available in the current online protocols) in exchange for total access or other compensation such as discount coupons for products.

This model will also require minimal new legislation. All the government would need to do to foster this system would be to ensure that the technology is adopted and that agreements made between the users and websites are enforceable. For online privacy, the ultimate goal that policymakers should strive towards is to optimize Internet use. The web provides formidable cost savings for many industries, as well as consumers. Costs are lower to maintain a website than a traditional business, and online companies do not require the same inventory. To the extent that industries are able to take advantage of these benefits, the overall global economy can be improved.

The online community can also enjoy many benefits from the services marketers provide. Targeted advertisements are more efficient than "carpet bombing" every consumer with the same generic commercials. Sellers can focus their resources on those buyers most in purchasing what the seller has to offer. A byproduct of the

10. Before a web page can be displayed on a browser, the website's server must receive certain information from the user's computer. This information includes the computer's web address, processing capabilities, screen size and browser type. For a more detailed description of how these communications work please see the Internet Society website at www.isoc.org.

improved marketing is that advertisers are better able to subsidize websites. Many of the most popular websites are currently available at no cost for visitors because the sites are supported by advertising dollars. The growth of the Internet can be attributed, at least in part, to marketers' willingness to pay premiums to move their targeted advertising online. These premiums have enabled websites to stay in business – even after the notorious dotcom bust.

The growth in electronic commerce has fallen short of its full potential, however, because many users – and potential users – continue to be apprehensive about their privacy. Surveys consistently find that online privacy is one of the most significant issues for Internet consumers.¹¹ These concerns can lead many people to steer away from the Internet and the resulting observation that occurs online. If a more secure environment could be established, these consumers would be more willing to transact online and the Internet could grow to its full potential. For this to happen however, online transactions need to be better tailored to account for consumers' privacy preferences. If each user could receive their optimal level of online privacy, the Internet would truly live up to its potential as a mechanism of commerce. An automated transaction could help foster this increased security.

By setting optimal use as the goal, the government may be able to avoid the impossible task of finding an exact description of privacy. Additionally, the legislature will not have to force one version of privacy on a public with diverse beliefs about the subject. Instead, policymakers can turn their focus away from these difficult tasks and towards the mission of addressing both the financial concerns of marketers and the doubts about privacy held by many users.

11. See, e.g., Joseph Turow, Lauren Feldman & Kimberly Meltzer, *Open to Exploitation: American Shoppers Online and Offline* 4, (June 2005) (finding that 79% of respondents to their survey agree that they are nervous about websites having information about them), available at http://www.annenbergpublicpolicycenter.org/04_info_society/Turow_APPC_Report_WEB_FINAL.pdf (last visited June 1, 2005); Joseph Turow, *Americans and Online Privacy: The System is Broken* 16 (June 2003) (finding that 76% of internet users who designate themselves as beginners, 74% who designate themselves as intermediates and 70% of internet users who designate themselves as advanced users agree with the statement 'I am nervous about websites having information about me'), available at <http://www.appcpenn.org/reports/2003/turow-privacy-no-cover.pdf> (last visited May 26, 2005); see also *Opinion Surveys: What Consumers Have to Say About Information Privacy: Before the Subcommittee On Commerce, Trade, and Consumer Protection of the House Committee On Energy and Commerce*, 107th Cong. 14-19 (May 8, 2001) (statement of Dr. Alan Westin, Professor, Columbia University) (stating that nine out of ten Americans are concerned about potential misuse of their information).

Hence, the best solution results when both users and businesses can decide the value for privacy between themselves. Ideally, websites should utilize available technology to decide in conjunction with each user a value for that person's personal information. Websites and users could decide for themselves how much data collection and privacy is worth. The two parties could then negotiate to find an equilibrium value. According to the Coase theorem, the final arrangement should be the most efficient allocation of privacy between the parties.¹²

At its most basic the Coase theorem assumes, however, that a negotiation has no transaction costs.¹³ In contrast, if each business had to negotiate with each visitor to its site separately, communication costs would be enormous. Fortunately, because this problem arises in a technological environment, technology may also be used to help alleviate the problem. Because automation will significantly reduce the transaction costs for each exchange a mutually beneficial exchange will result, as Coase predicts.¹⁴

To simplify the process for users and further lower transaction costs, the browser could offer a menu of privacy options. The user could simply answer a series of questions when installing the browser. These settings will then be used as the starting point for the automated negotiation with the website. An important feature will be the system's flexibility. Users will be able to change their settings at any time they choose. A consumer could initially set their browser to provide complete protection for their personal information. As the consumer visits websites, however, she may become unhappy with the amount of content to which she is provided access. User would be able to reevaluate the worth they place on their privacy and readjust their browser's settings accordingly. Eventually, the user will reach a point at which her interest in privacy and desire for access to information are balanced. Users would no longer need to adjust the settings on their browser once they reach the point where additional content is not worth the sacrifice of more personal privacy.

The government would also need to help foster the negotiation. To help ensure users' security, the government should create a cause of action against websites that violate the terms of the agreement between the sites and the users. Currently, the Federal Trade

12. Ronald Coase, *The Problem of Social Cost*, 3 J.L. & ECON. 1 (1960).

13. Robert Cooter & Thomas Ulen, *LAW & ECONOMICS* 101 n.11 (4th ed., Addison Wesley 2003).

14. See Coase, *supra* note 12, at 7.

Commission will bring actions against websites that violate their posted privacy policies.¹⁵ Unfortunately, the threat of suit holds very little bite for websites under the current system because no restrictions govern the contents of their posted policies.¹⁶ Often the websites do not actually offer any protection for users, which is usually explicitly stated in the policies.¹⁷ However, it is generally too much effort for most users to review the policy for each site they visit. The privacy and security benefits of the automated system arise because in order to attract traffic, websites may need to agree to increase their privacy protection for many consumers. Once the sites come to an agreement with the user, the site will have to comply with the terms of the bargain or be the target of lawsuits. The result will be improved security for consumer information.

The system will also help eliminate consumer distrust of the online market. Trust has been shown to help economies operate more efficiently.¹⁸ The Internet can be viewed as its own economic system,¹⁹ and as such, improving trust will enhance the efficiency of the market. When consumers trust the privacy practices of the websites they visit, they will be more willing to conduct business on those sites. Further, the websites will not need to expend scarce resources on convincing consumers their information is secure.

Automated negotiations will help increase trust on the website side as well. Frequently, users use fictitious names and information to try and confuse marketers and protect their actual identities.²⁰ If

15. The FTC can bring privacy actions under Section 5 of the Federal Trade Commission Act against companies that fail to uphold promises made in their privacy policies. Federal Trade Commission Act, 15 U.S.C. §§ 41-58 (2004).

16. In fact, since 1999 the FTC has brought only 14 privacy actions under Section 5 of the FTC Act. See http://www.ftc.gov/privacy/privacyinitiatives/promises_enf.html for a list of cases brought by the FTC.

17. For example, the privacy policy at [cnn.com](http://www.cnn.com) states when ordering products, consumers may enter personally identifiable information such as their name, address and phone number. Use of certain services will be restricted for consumers who do not volunteer this information. In addition, the site allows consumers to enter information about other people. The [cnn.com](http://www.cnn.com) privacy policy also collects non-personally identifiable information that the user does not enter voluntarily. The statement provides that [cnn.com](http://www.cnn.com) can share the information it collects with other companies that do not comply with the [cnn.com](http://www.cnn.com) privacy policy. Cnn.com Privacy Statement available at <http://www.cnn.com/privacy.html> (last visited May 27, 2005).

18. Stephen Knack & Philip Keefer, *Does Social Capital Have an Economic Payoff? A Cross-Country Investigation*, 112 Q.J. ECON. 1251 (1997).

19. See, e.g., Internet Economics (Lee W. McKnight & Joseph P. Baily, eds., 1998).

20. See, e.g., Jessica Litman, *Cyberspace and Privacy: A New Legal Paradigm?* 52 STAN. L. REV. 1283, 1285-86 (2000) (listing methods that people may take to confuse data collectors such as using variations of their name and using work addresses).

consumers agree to provide certain kinds of data and the ways that data can be put to use, they are less likely to go through the effort of falsifying their information. The data collectors can then be more confident that the data they have collected is accurate. Overall, by eliminating distrust in both users and marketers, an automated transaction will improve the efficiency of the electronic market.

Part II of this paper will discuss the current system and the problems it presents. The section will describe academic and political solutions that have been proposed and then analyze why these resolutions have not been able to solve the problem. Part III will provide a detailed explanation of my content-for-privacy automated solution. Both the technological and legal aspects of the system will be analyzed. Finally, the discussion will address the benefits this system can provide over the current model (or lack thereof).

II. Development of Online Profiling and Attempts at Regulation

The widespread outcry about online privacy began in the late 1990's when one of the largest Internet advertiser –DoubleClick, Inc. - acquired an offline direct marketer named Abacus Direct, Inc.²¹ DoubleClick is an Internet advertiser that tracks users online and can then post targeted advertisements across their assembled network of different websites.²² Similarly, Abacus collects information about consumers' offline habits and uses this data to target direct postal marketing mailings.²³ Even prior to the merger, many privacy advocates had already taken issue with DoubleClick's data collection practices.²⁴ However, the issue had not gathered much widespread attention from consumers for several reasons. First, the information

21. Bob Tedeschi, *E-Commerce Report: DoubleClick is Seeking Ways to Use Online and Offline Data and Protect Users' Anonymity*, N.Y. TIMES, Jan. 29, 2001, at C9.

22. The DoubleClick website explains that one of DoubleClick's marketing products consists of "databases [that] contain transactional data with detailed information on consumer and business purchasing and spending behavior." The site goes on to explain that "[b]y combining pooled transactional data with proprietary modeling techniques, [DoubleClick] help[s] direct marketers profitably identify, acquire and retain customers in order to operate and grow their business." See http://www.doubleclick.com/us/products/direct_marketing/.

23. See Courtney Macavinta, *DoubleClick, Abacus Merge in \$1.7 Billion Deal*, CNET News.com, available at <http://news.com.com/2100-1023-233526.html?legacy=cnet&tag=st.ne.1005-200-1534533> (Nov. 24, 1999) (stating that prior to the merger with DoubleClick, Abacus owned two billion personally identifiable consumer catalog transactions) (last visited May 29, 2005).

24. 1998 FTC REPORT, *supra* note 4 (citing surveys that show that consumers may be avoiding the Internet rather than providing personal information to websites).

that online marketers collected was anonymous and only associated with a computer -- not with a particular user.²⁵ Second, many users were completely unaware of the practice.²⁶ With the merger, public attention focused on DoubleClick and online advertising.

Scrutiny increased because at approximately the same time as the merger, DoubleClick altered its privacy policy to allow association of the previously nameless information it collected with identifiable data.²⁷ Privacy advocates feared that not only would DoubleClick collect personally identifiable information on the Internet, but that this information would also be combined with data about consumers' offline habits as well.²⁸ After being contacted about privacy concerns by the FTC and several state Attorneys General, DoubleClick announced that it was no longer planning on combining its on and offline databases.²⁹

Later the same year, the bankruptcy of Toysmart.com contributed to the swelling consumer fears over privacy.³⁰ Prior to its

25. See Courtney Macavinta, *Privacy Fears Raised by DoubleClick Database Plans*, CNET NEWS.COM, Jan. 25, 2000, available at <http://news.com.com/2100-1023-236092.html?legacy=cnet&tag=st.ne.1002.bgif%3fst.ne.fd.gif.j>. ("Until recently, DoubleClick's policy was to not correlate personal information with its 100 million cookies, which are scattered worldwide.")

26. Turow, Feldman & Meltzer, *supra* note 11; Turow, *supra* note 11.

27. Prior to the change, DoubleClick's policy read, "All users who receive an ad targeted by DoubleClick's technology remain completely anonymous. We do not sell or rent any information to third parties." After the change the policy read, "DoubleClick does, however, collect certain non-personally-identifiable information about you . . . Upon completion of the merger, should DoubleClick ever match the non-personally-identifiable information collected by DoubleClick with Abacus' database information, DoubleClick will revise this Privacy Statement to accurately reflect its modified data collection and data use policies and ensure that you have adequate notice of any changes and a choice to participate." See Complaint and Request for Injunction, Request for Investigation and for Other Relief at 4-6, In the Matter of DoubleClick, Inc. (2000) (discussing the change in DoubleClick's privacy policy), available at http://www.epic.org/privacy/internet/ftc/DCLK_complaint.pdf; see also Electronic Privacy Information Center, <http://www.epic.org/privacy/doubletrouble/> (last visited May 29, 2005) for a list of articles chronicling the DoubleClick merger with Abacus.

28. Closing Letter from Joel Winston, Acting Associate Director, Division of Financial Practices, FTC, to Christine Varney, Attorney for DoubleClick, File No. 002 3122 (Jan. 22, 2001) (closing the FTC investigation of DoubleClick's merger with Abacus Direct) (on file with the FTC), available at <http://www.ftc.gov/os/closings/staff/doubleclick.pdf> (last visited May 29, 2005).

29. Matthew C. Keck, *Cookies, the Constitution, and the Common Law: A Framework for the Right of Privacy on The Internet*, 13 ALB. L.J. SCI. & TECH. 83, 91 (2002).

30. *FTC v. Toysmart.com, LLC*, Civil Action No. 00-11341-RGS, 2000 WL 34016434 (D. Mass. July 21, 2000) (enforcing a settlement order with the FTC in which Toysmart.com agrees to delete all customer information in their possession).

demise, the website had been assembling a database containing detailed information about its customers.³¹ Despite a privacy policy to the contrary, the company sold the information to help pay off its creditors.³² The FTC sued Toysmart.com to prevent the distribution of its information.³³ The case was eventually settled, but the damage to consumer confidence had already been done.³⁴

Spurred to action by these events and growing complaints from consumer advocates, the FTC and the U.S. Department of Commerce held several workshops with the largest online marketers to investigate these growing problems. The workshops resulted in two reports from the FTC to Congress.³⁵ The final conclusion proposed by these reports was that the industry should try to self-regulate before any legislative action took place.³⁶ In response, the advertisers formed a trade group called the Network Advertisers Initiative to monitor the industry's attempts at privacy reform.³⁷

Unfortunately, this attempt at self-regulation is now widely viewed as an abject failure.³⁸ Data gathering has not decreased and consumers do not feel any more secure. Congress has repeatedly tried to pass legislation addressing these growing problems, but to no avail.³⁹ Without any legislative action, the courts have been left to try

31. *Id.* at *1 (FTC complaint alleges that Toysmart.com collected customer information and the privacy policy stated that the company would not offer to sell the information to third parties).

32. *Id.* (FTC complaint alleges that Toysmart.com engaged in deceptive practices by offering to sell to third parties customer information, contrary to the company's privacy policy).

33. *Id.*

34. *Id.*

35. 1998 FTC REPORT, *supra* note 24; Federal Trade Commission, *Privacy Online: A Report to Congress Part 2 Recommendations* (July 2000) [hereinafter 2000 FTC REPORT], available at <http://www.ftc.gov/os/2000/07/onlineprofiling.pdf>.

36. 2000 FTC REPORT, *supra* note 35.

37. See Network Advertising Initiative, available at http://www.networkadvertising.org/aboutnai_nai.asp (last visited May 30, 2005).

38. Litman, *supra* note 20, at 1286-87 ("Industry self-regulation, of course, has got us where we are today. Studies of how well it is working confirm what one would expect: It works far better at enhancing commerce in personal data than it does in protecting personal data privacy."); see also Chris Jay Hoofnagle, Electronic Privacy Information Control, *Privacy Self Regulation: A Decade of Disappointment* (Mar. 4, 2005) (explaining why self-regulation has not worked and how the government needs to provide a better solution), available at <http://www.epic.org/reports/decadedisappoint.pdf> (last visited May 30, 2005). worked and how the government needs to provide a better solution), available at <http://www.epic.org/reports/decadedisappoint.pdf> (last visited May 30, 2005).

39. See Center for Democracy and Technology, available at <http://www.cdt.org/legislation/0/3/>.

to deal with the predicament on their own.⁴⁰ Unfortunately, the judicial branch of the government is ill-equipped to confront these proliferating difficulties. Courts operate on a case-by-case basis; however, a larger policy may result from – or at least be influenced by – the judicial decisions.⁴¹ Because of the lack of control and uncertainty regarding online privacy, there have been many calls on Congress to create some sort of policy on the subject.⁴²

A. Profiling and Advertising

Before any alternative solutions can be explored, it is first necessary to understand the precise nature of marketers' information-gathering behaviors. To appropriate the value of consumer information, online marketers have developed innovative technologies to harvest the data.⁴³ One of the primary concerns about these technological advances is not their ability to track a user on a single website, but to assemble profiles of each user across many

40. Keck, *supra* note 29, at 93.

41. *Id.*

42. See discussion *infra* Part C.

43. Before 1994, website servers were not able to identify a particular user. Schwartz, *supra* note 2. Until "that moment in Web history, every visit to a site was like the first, with no automatic way to record that a visitor had dropped by before. Any commercial transaction would have to be handled from start to finish in one visit, and visitors would have to work their way through the same clicks again and again; it was like visiting a store where the shopkeeper had amnesia." *Id.* That year, a programmer for a company soon to be known as Netscape invented a technology, called a cookie, which allowed websites to identify each individual computer that visited the site.

To understand the operation of a cookie, one must first recognize that to display a web page, a user's computer must communicate with the server that contains that information. During this communication, the website's server can place a small text file on the user's hard drive. This file, the cookie, contains a code unique to the user's computer and possibly other logon information, such as any password the user needs for that website. The next time the user's computer views the website, that site's server will recognize the cookie and thereby identify the viewing computer. Once the website server identifies the user's computer it can then begin to collect information about the user's habits while visiting the site.

A website's ability to record such information offers several benefits to the user. For instance, cookies allow users to discontinue an online operation in mid-stream and then complete the undertaking on a subsequent visit to the site without repeating already completed steps. Another convenience is the possibility of one-click purchasing; in this case the website's server retains the user's purchasing information, such as a credit card number and shipping address, from one transaction to the next. The user, therefore, only has to select the item s/he wishes to purchase to complete the transaction.

Cookies also allow the consumer to benefit from customized web pages. Web "portals" such as American Online, Yahoo! and Netscape can provide information preferred by a particular user such as local news, weather, sports scores, stock quotes, etc. By allowing the website to tag the user's computer with a cookie that is pre-programmed self-identification, the user needs only to link to that site to receive pre-selected information.

unrelated sites.⁴⁴ Advertisers contract with multiple websites, each of which permits the collection of information concerning visitors to the site.⁴⁵ The advertiser is then able to compile the information it collects from various sites into a single dossier or profile.⁴⁶ The resulting profiles can consist of hundreds of discrete data points about an individual. As an online advertiser collects more information about a particular web user, it becomes better able to narrowly target advertisements to that user's personal preferences and tastes.

User-specific targeted advertising is essentially a more focused version of traditional advertising methods. Offline, advertisers conduct marketing surveys to determine a consumer's likelihood to purchase its product. Advertisers, then, select a medium and location, such as a particular television show, with a demographic that most matches their ideal consumer.

Demographic-based marketing is constrained, however, by two factors. First, the marketer cannot target a precise consumer from the group that fits the relevant demographic. Second, it is difficult to determine which advertisements are most effective.⁴⁷ Online profiling has given the marketers the ability to overcome both obstacles. The detailed consumer profiles advertisers can collect online allow them to target their marketing to specific individuals who are most likely to be interested in their product. Additionally, because advertisers can track potential customers (i.e., match viewers of ads with purchasers of the product), they can determine the effectiveness of any particular advertisement. In these two ways, online profiling can make marketing much more effective.⁴⁸

44. See 2000 FTC REPORT, *supra* note 35 at 3 (noting that online advertisers act in a manner that is almost invisible to consumers to collect information from multiple sites in order to put together a profile from which they can predict future consumer behavior).

45. See, e.g., Abacus, available at http://www.abacus-us.com/about_abacus/abacus_overview/, which explains that one of DoubleClick's alliances consists "of over 1,550 catalog, online, and retail merchants offering shared data representing over 90 million households."

46. 2000 FTC REPORT, *supra* note 35, at 3.

47. Hence, the old advertising adage that an advertiser knows that half of its budget is wasted, it is just not sure which half.

48. Somewhat paradoxically, this ability to track the effectiveness of particular ads may have also led to the decline in online advertising since the late 1990's. Whereas offline, anytime sales go up, it can be inferred that certain advertisements had a role in that increase, online this inference can be measured directly. Since most online advertisements only had a small number of people click through them, it was assumed these were the only customers the advertisements were influencing. Once the marketers saw the low click-through numbers they decreased their online advertising budget.

It is extremely important to note, however, that despite this ability to create online user profiles, the information collected is generally not associated with any specific person.⁴⁹ The profile represents a pattern of usage, and is linked only to an identification code placed on a computer, not to the specific user.⁵⁰ The data found in this sort of anonymous profile are known as Non-Personally Identifiable Information (Non-PII).⁵¹ Several ways exist, however, to link the profile to a specific person, and thus, the profile becomes Personally Identifiable Information (PII).⁵² For example, if the user enters her name into a form on the website to make a purchase, the site can then connect the name with the user's previously anonymous profile.

Online advertisers can, therefore, create enormous databases of user information, both with and without PII. Some of the largest online advertisers have thousands of different websites as part of their network, including most of the sites with the majority of online traffic.⁵³ Although online profiling is usually associated with network advertising agencies, "[n]ot all profiles are constructed by network advertising companies (also known as online profilers). Some websites create profiles of their own customers based on their interactions. Other companies create profiles as part of a service – for example, offering discounts on particular products, or providing references to Web sites displaying the same topic as those already visited by the consumer."⁵⁴ Online profilers with even greater reach are Internet Service Providers (ISP's), such as America Online.⁵⁵ Because ISP's are able to track users the entire time they are logged on to their service, the ISP can compile extraordinarily thorough information about their consumers' interests and online habits. Specialists are then able to "analyze demographic, media, survey, purchasing and psychographic data to determine the exact groups

49. See, e.g., the DoubleClick privacy statement at http://www.doubleclick.com/us/about_doubleclick/privacy/ (stating that no personal information is used by DoubleClick to deliver advertisements).

50. See 1998 FTC REPORT, *supra* note 4.

51. *Id.*

52. *Id.*

53. *In re DoubleClick, Inc. Privacy Litig.*, 154 F. Supp. 2d 497, 502 (S.D.N.Y. 2001) ("DoubleClick is affiliated with over 11,000 Web sites for which and on which it provides targeted banner advertisements."); see also Abacus website, *supra* note 45.

54. 2000 FTC REPORT, *supra* note 35, at 1 n.4.

55. See, e.g., Litman *supra* note 20, at 1305 (describing a case in which the ISP America Online changed their privacy policy with little notice, and then contracted to sell subscribers' telephone numbers to third-party telemarketers.)

that are most likely to buy specific products and services. Psychographic profiling is also referred to in the industry as 'behavioral profiling.'⁵⁶

B. The Efficiency Lost from Profiling in the Current System

The harvesting of personal information can substantially benefit both marketers and consumers. Marketers ensure that their efforts are focused on the consumers who are most interested in their products, while users avoid generic promotions for which they have no interest. For users who continue to avoid the Internet, however, the privacy threat well-surpasses these benefits.⁵⁷ Many consumers use the Internet at a sub-optimal level due to several economic factors, such as an unproductive amount of advertising, an unreasonable all-or-nothing choice in terms of privacy, and a loss of trust.

1. Marketers Both Over- and Under-Produce Advertising

Profiling represents a substantial invasion of consumer privacy, yet consumers are not compensated for this loss. Data collection has two primary costs: the actual financial expense as well as the emotional toll consumers suffer when their privacy is invaded. The marketer pays the initial price for the data-collection and selection of targeted advertisements. Nonetheless, marketers do not pay for the accompanying loss of privacy, and the price can be substantial. Unlike situations offline where a person needs to leave home before he or she can be observed, surveillance online occurs in the most private spaces, such as kitchens, living rooms and bedrooms.⁵⁸ Currently, marketers underpay for their data because they do not pay for this diminished privacy. This discounted price allows collectors to gather more data than they could otherwise afford if they had paid in full.

Further, profiling generates both over- and under-production of targeted ads. Overproduction results when users receive targeted advertisements but would prefer a subscription service to sacrificing privacy. For these consumers, a more efficient online situation would allow a choice between paying for access to a site and receiving advertising that subsidizes the site's costs. Efficiency could be further enhanced by allowing a graded system in which consumers could decide on different ratios of advertising to subscription payments.

56. 2000 FTC REPORT, *supra* note 35, at 5 (internal citations omitted).

57. See sources cited *supra* note 8.

58. See sources cited *supra* notes 8 and 11.

Conversely, too few advertisements are sometimes generated. Underproduction of targeted ads results when consumers would prefer to offer private information in return for specific marketing but cannot. For example, a consumer who is currently in the market for a new car may be willing to supply her preferences in automobiles in return for promotions informing her about the car market. Many car dealers would probably also be willing to pay for the information about potential customers. As a result, the dealer would not waste resources locating an interested audience and the consumer would receive ads to which she is receptive. Presently, no method exists that enables consumers to easily alert companies of their preferences. For a consumer to alert advertisers of her preferences, she needs to visit a car dealer's website and hope that the advertisers will correctly interpret the resulting "clickstream" data.⁵⁹

2. *The Unreasonable All-Or-Nothing Choice*

A related source of underproduction stems from consumers with minimal privacy concerns that would willingly sell information. Advertisers value demographic information and some might pay for more detailed data than they can gather on their own. Unfortunately, a venue for this market is not readily available. Consequently, consumers and advertisers may be ready to transact but cannot find a ready marketplace.

Parties facing the problem of inefficient data collection are left with an unreasonable all-or-nothing choice. It is virtually impossible for consumers to block all the technology that data collectors use to harvest consumer information.⁶⁰ Therefore, consumers must decide to

59. "Clickstream" is a commonly used term used to describe the "digital footprints" left behind when a person moves through the Internet.

60. Cookies are relatively easy to block through most browsers, although many websites do not operate effectively if they cannot place and read cookies on the user's system. There are other technologies, such as web bugs and spyware that are not nearly as easy to stop. The web bug, a small graphic embedded into the background of a web page, is increasingly popular. See Stephanie Olsen, *Web Bug Swarm Grows 500 Percent*, CNET NEWS.COM, Aug. 14, 2001, at <http://news.com.com/2100-1023-271605.html>. Web bugs use the same technology that displays images on web pages. In normal operation, a website's internal code contains information that directs the user's computer to retrieve the image to be displayed from a specified location on the website server or any computer linked to the Internet. The retrieval instructions also direct the user's computer to send information about that computer that permits the web server to send an image of the correct size and configuration.

The web bug is an extension of this standard process of image display. Attached to the retrieve command for even a single pixel are instructions to send additional information to the server. Because such a small display creates no noticeable image on the screen, web bugs are sometimes called "clear" GIFS (Graphics Interchange Format). See Sean

allow marketers' surveillance or maintain their privacy by remaining offline. Regrettably, choosing privacy inevitably results in either a reduction in Internet use or, in many cases, avoidance of the web altogether. Many users, however, when properly informed about the benefits connected with some data collection, may elect an intermediate option. The consumer surplus available from users who remain offline but would favor an intermediary alternative is lost in this all-or-nothing paradigm.

3. *Loss of Trust Online*

Perhaps the gravest consequence from profiling is that it fosters distrust online. Because users are not generally aware of marketers' methods of collection and distribution, many feel insecure about surfing the web. This anxiety increases every time the media reports stories extolling the dangers of personal information that has been bought, sold or stolen.⁶¹ Overall, data collection, coupled with the lack of privacy protection, decreases consumer trust online.

Recently, economists have demonstrated that higher levels of trust in a community are generally associated with more efficiency in the related economy. For example, trust can be associated with higher productivity because "[i]ndividuals in higher-trust societies spend less to protect themselves from being exploited in economic transactions."⁶² Government policy regarding online privacy directly

Donahue, *GIF Tiff*, Business 2.0, December 1999, at <http://ecompany.com/articles/mag/0,1640,13282,FF.html?ref=cnet>. Specifically, "[t]he Web bug sends back to its home server (which can belong to the host site, a network advertiser or some other third party): the IP (Internet Protocol) address of the computer that downloaded the page on which the bug appears; the URL (Uniform Resource Locator) of the page on which the Web bug appears; the URL of the Web bug image; the time the page containing the Web bug was viewed; the type of browser that fetched the Web bug; and the identification number of any cookie on the consumer's computer previously placed by that server." 2000 FTC REPORT, *supra* note 35, at 3 n.12. Additionally, the web bug can place a cookie on the user's computer that configures itself to the user's email address, thereby making all the information collected from the cookie identifiable. *Id.* Because web bugs are invisible to the naked eye, the only way a user can detect a web bug is to search the website's source code for a single pixel image embedded in the programming, or to download special detection software. See Stephanie Olsen, *Privacy Group Shines Light on Web Bugs*, CNET NEWS.COM, June 7, 2001, <http://news.com.com/2100-1023-268055.html>.

61. See, e.g., *FTC v. Toysmart.com, LLC*, Civil Action No. 00-11341-RGS, 2000 WL 34016434 (D. Mass. July 21, 2000); Tom Zeller Jr., *The Scramble to Protect Personal Information*, NY TIMES.COM, June 9, 2005, <http://www.nytimes.com/2005/06/09/business/09data.html?oref=login> (reporting on the ways in which personal information collected by businesses have been stolen).

62. Knack & Keefer, *supra* note 18, at 2. When individual trust is higher, fewer transactional terms need to be expressed in written contracts and litigation is less frequent.

bears on the level of trust associated with Internet transactions. "Whereas firms have incentives to abuse their access to privileged information, their desire for future deals requires the trust of consumers who don't fear their information will be stolen or abused."⁶³ Hence, if users feel that their personal information is secure, they will be more inclined to use the Internet.

Because users do not have enough faith in the websites they visit, people are confronted with added costs as they attempt to protect their privacy. For instance, many people use pseudonyms,⁶⁴ or resort to other deceptive tactics such as supplying different home addresses, using incorrect email addresses and providing incorrect consumer interests.⁶⁵ Not only is this effort inefficient but also ineffective. The pretexts are not efficient because resources are expended that could be spent more productively if privacy were valued correctly. The ploys are ineffective because there are many ways to collect data and marketers will usually uncover the correct facts eventually. The final result would be that the consumer will still receive advertising, but the ads will not be of any interest.

Increased trust can prove beneficial for web businesses as well. Once users feel more secure, they will visit more sites and conduct more transactions online; overall Internet traffic will grow. Companies would not spend as much to assure their customers if a standard level of protection were the social norm. Businesses could use these savings to reduce prices or to develop new products. If users could control the ways in which their information was used then they would not be as wary. Hence, provision of protection for information is a wealth enhancing good for both users and businesses. However, online privacy will never be optimally equilibrated under the existing all-or-nothing paradigm, and the attendant cost is underutilization of the web.

Id. at 3. Importantly, societies with high levels of trust also require fewer institutions to enforce the terms of transactions. *Id.* To the extent that the society spends less on protection, it can increase expenditures on innovation and other more productive activities. *Id.*

63. Avner Ben-Ner & Louis Putterman, *Trusting and Trustworthiness*, 81 B.U.L. Rev. 523, 539 (2001).

64. See Litman, *supra* note 20, at 1290 (citing Avrahami v. U.S. News & World Report, Inc., No. 96-203, 1996 WL 1065557, at *2 (Va. Cir. Ct. June 13, 1996) (finding that defendant used at least 19 different names in making purchases)).

65. *Id.* at 1285-86.

C. Privacy Theories – Off and Online

The conundrum presented by the issue of online privacy and marketers profiling behavior has attracted considerable scholarly attention. Ever since Warren and Brandeis published their path-breaking article that first recognized "a right to be left alone,"⁶⁶ legal scholars have attempted to define the boundaries of this right.⁶⁷ These attempts have created an almost incomprehensible array of definitions and values for privacy. At one end of the spectrum is the claim that privacy is inalienable and should be granted to all citizens regardless of that citizen's personal perceived value for their privacy.⁶⁸ At the other end of the continuum is the belief that people only want it when they have something to hide.⁶⁹ Within this spectrum, most of the literature tends to be biased in favor of granting a rather extensive privacy right. As Thomas Murphy noted, since scholars tend to favor privacy "a large portion of the literature – both popular and scholarly – consists of articles extolling the virtues of privacy and bemoaning the absence of judicial and statutory protection."⁷⁰

The disparate interpretations of even the simple definition of privacy may lead to the conclusion that legislating privacy is impossible. Legislation requires community values, yet the community does not seem able to agree on the importance of privacy. Nevertheless, because so many people view online privacy as a major

66. Samuel Warren & Louis Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 193-96 (1890) (explaining the evolution of the right to privacy).

67. See, e.g., discussion *infra* Parts 1, 2, 3.

68. See, e.g., Cal. Const. Art. I, § 1 (listing privacy among specific inalienable rights enjoyed by all people).

69. By conducting an economic analysis of privacy, Judge Richard Posner came to the conclusion that there should not be an allocation of property rights over an individual's personal information because the primary reason to keep information private is to misrepresent oneself. Richard A. Posner, *The Right to Privacy*, 12 GA. L. REV. 393, 407 (1978). According to this view, the only reason people want control over the spread of true facts is to commit fraud – either social or financial. Privacy protection encourages fraud. "The more (accurate) information is available, and the cheaper that information is to obtain, the more beneficial transactions will occur. In the market context, if disclosure of information is inhibited, the decision to transact will be made either with second-rate information or with information obtained at a higher cost. The same holds true in the social 'market,' except with different terminology." Richard S. Murphy, *Property Rights in Personal Information: An Economic Defense of Privacy*, 84 GEO. L.J. 2381, 2386 (1996).

Seemingly paradoxically, economic analysis leads to the conclusion that while individuals should not receive privacy protection, businesses should. While individuals try to hide information in an attempt to deceive, businesses hide information as part of development, as in trade secret law. By removing protection from businesses, the government would be taking away an incentive to create. Posner, *supra*.

70. Murphy, *supra* note 69, at 2381.

concern,⁷¹ there have been many attempts to place legal control over the collection and dissemination of personal information.⁷² These attempts have failed, however, due partly to a general lack of enthusiasm among legislators to pass laws that govern the Internet.⁷³ Additionally, the proposals have not been able to overcome the difficult task in defining what protections to give.⁷⁴ To try to address this legislative impasse, a surge of articles attempting to deal with the specific problem of privacy online have emerged. Three of the most popular theories are the property rights approach, the tort law approach and the European Union approach.

1. *The Property Rights Approach*

Recently, one of the most popular proposals is to grant a property right over personal information.⁷⁵ Once the property right is created, people should be able to control their information. Although the privacy as property argument is not new, the resistance towards regulating both the Internet and privacy has helped generate renewed interest in the concept.⁷⁶ Recent Congressional attempts at legislating privacy in other contexts have drawn wide criticism.⁷⁷ The property rights solution has gained momentum because it can help solve the

71. See sources cited *supra* notes 8 and 11.

72. Schwartz, *supra* note 2 ("In Washington, at least 50 privacy-related bills are awaiting consideration, though the current leadership in the House has focused its attention on privacy invasions by government, not by private business."); see also <http://www.cdt.org/legislation/0/3/> for a list of privacy-related proposals.

73. This reluctance stems from several different sources. The most obvious reasons are that laws governing the Internet are difficult to enforce, would demand extensive resources and would give a false sense of security. *Internet Privacy and Electronic Communications: Hearing Before the Subcommittee on Courts and Intellectual Property of the House Committee on the Judiciary*, 105th Cong. 25-26 (1998) (statement of David L. Aaron, Under Secretary, International Trade Administration, Department of Commerce), available at <http://judiciary.house.gov/legacy/41176.htm>. There are also philosophical reasons why the government should not pass laws for the Internet specifically. See, e.g., Frank H. Easterbrook, *Cyberspace and the Law of the Horse*, 1996 U. CHI. LEGAL F. 207 (1996) (arguing that it is more efficient to allow traditional law to govern issues arising online than to create a new set of laws that pertain only to cyberspace). Finally, there are very practical reasons, such as intense industry lobbying, why the government has been slow to enact any regulation over the Internet. Lawrence Lessig, *The Architecture of Privacy*, 1 VAND. J. ENT. L. & PRAC. 56 (1999) ("The reasons for this lack of law in America protecting privacy are complex . . . one set relates to the extraordinary lobbying power of interests that would use the data affected by informational privacy regulation. . . .").

74. See Lessig, *supra* note 73.

75. Littman, *supra* note 20, at 1287-88.

76. *Id.*

77. See *infra* note 193.

problem without undue government intrusion into the realm of privacy or the web. Once the right is declared, standard property and contract law can take over.

Professor Lawrence Lessig has taken the property rights approach one-step further.⁷⁸ According to Professor Lessig, assignment of a property right is only the first piece of the solution; technological controls over personal information must also be put in place.⁷⁹ Professor Lessig envisions a system where privacy preferences can be entered into an automated "privacy butler" which can then negotiate with websites and marketers automatically.⁸⁰ To ensure the system works, entitlement to the property rights for personal information must initially be allocated to the user.⁸¹ Users should then have control over their own information.

The idea of a property right has not won over all scholars; indeed, it has several drawbacks. For example, creating a property right in personal information means that people can control that information. However, anytime someone can control information there is a potential conflict with First Amendment principles.⁸² Once information can be restricted, freedom of expression can also be restricted.⁸³

The primary concern with the property rights proposal, however, is that property is alienable and consumers will end up selling the rights to their information. Most users do not ever read click-through agreements online.⁸⁴ If property rights are given for personal information, it is very likely that data collectors will include assignments of personal information in their click-through agreements. Therefore, before a consumer realizes that they have

78. Lawrence Lessig, *Code and Other Laws of Cyberspace* (1999).

79. *Id.*

80. Paul M. Schwartz, *Beyond Lessig's Code for Internet Privacy: Cyberspace Filters, Privacy-Control, and Fair Information Practices*, 2000 WIS. L. REV. 743, 750 (2000) (discussing Professor Lessig's proposed privacy solution in which property rights to information are assigned to the user and then technology can be used to negotiate away these property rights).

81. *Id.*

82. Litman, *supra* note 20, at 1294 n.56

83. *Id.* at 1294-95.

84. A click-through or clickwrap agreement is a type of online contract where users can simply click a digital button to manifest assent. *See* *Specht v. Netscape Communications Corp.*, 306 F.3d 17, 22 n.4 (2d Cir. 2002) (defining clickwrap agreements and noting that most plaintiffs in that case never read the agreement before downloading the corresponding software); Turow, *supra* note 11, at 18 (concluding that most adults who are not aware of what cookies do either do not read or do not understand the posted privacy policies on the sites they visit).

given up their property rights, it has been fully assigned. The consumer will then no longer have control over the downstream trading. The problem is compounded because property rights will probably make this information more valuable.⁸⁵ As profilers are able to exclude their competitors from the information they collect, the information's market value will increase.⁸⁶ The increased value could encourage even more harvesting.⁸⁷

2. *The Tort Law Approach*

An alternative approach proposed by Professor Jessica Litman relies on tort, rather than property, law.⁸⁸ Just as the property rights approach is attractive due to its grounding in traditional common law, so is the tort law approach. As mentioned above, the trade of personal information can violate consumer trust.⁸⁹ Many consumers have developed an expectation that their information will not be collected, bought or sold. Recently, some legislation has created causes of action in the case of medical or financial information when that trust is violated.⁹⁰ Advocates of the tort law approach believe these types of causes of action should apply to every class of data collection.⁹¹

As Professor Litman points out, this solution has some appeal for several reasons. First, tort law is already well established and would not need significant modification to add a cause for invasion of privacy to its arsenal of possible claims.⁹² Just as the property law approach has an air of possibility that makes the solution more attractive, a tort solution has some allure because of its sense of feasibility. Second, tort law already has built-in methods through which parties can show consent by expressing "willingness in fact that an act or an invasion of an interest shall take place."⁹³ Because one of the primary issues involved in online privacy has been the difficulty of

85. Litman, *supra* note 20, at 1294-95.

86. *Id.* at 1295.

87. *Id.*

88. *Id.*

89. *See supra* pp.117-19.

90. 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.) (provides privacy protection for certain types of financial information); Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (1996) (provides privacy protection for certain types of medical information).

91. Litman, *supra* note 20, at 1291-92.

92. *Id.* at 1312-13.

93. Restatement (Second) of Torts § 10A (1965).

user consent, tort law can help by contributing a mechanism to deal with the problem. A final advantage of tort law is that as a common law solution, the rules can be altered to reflect changing technology and societal attitudes about privacy.⁹⁴

Unfortunately, like property law, even Professor Litman admits tort law is not a panacea for the problem of Internet privacy.⁹⁵ A tort solution ultimately relies on judicial intervention between private parties. Courts, therefore, will be the final arbiters of privacy rights. This solution can work, but only if consensus as to the definition and value of privacy can be achieved. While courts may be good at determining a community's norms, the courts place such divergent value on their personal information that it would be virtually impossible for a court to decide how much protection any particular party should receive. What may be seen as a heinous invasion of privacy to some members of a community could be a welcome attempt to customize services to others. The courts would be left either setting general guidelines that everyone must follow or make decisions on a case-by-case basis, leaving future litigants uncertain of their rights.

The court system may also have a difficult time deciding what constitutes a breach of consumer trust.⁹⁶ Obviously, once a case gets to court the consumer will claim their trust was violated. It is very difficult from an *ex ante* position, however, to determine what sort of implicit agreement was made between the litigants at the time of the breach.

3. *The EU Approach*

A third type of privacy regime based on the privacy laws established in the European Union has become increasingly popular.⁹⁷

94. Keck, *supra* note 29, at 84 ("Solving the privacy debate is a task that the common law is particularly well-suited for because it can adapt to changing views and perspectives without requiring new legislation or regulations.").

95. Litman, *supra* note 20, at 1312-13 ("The features that make [the tort law] approach plausible, however, also make it weak.").

96. *Id.* at 1313.

97. See, e.g., *Issues in U.S.—European Union Trade: European Privacy Legislation and Biotechnology/Food Safety Policy, Hearing Before the House Committee on International Relations*, 105th Cong. (1998) (statement of Marc Rotenberg, Executive Director, Electronic Privacy Information Center), available at http://commdocs.house.gov/committees/intlrel/hfa50549.000/hfa50549_of.htm; Rachel K. Zimmerman, *The Way the "Cookies" Crumble: Internet Privacy and Data Protection in the Twenty-First Century*, 4 N.Y.U.J. LEGIS. & PUB. POL'Y 439, 449 (2001); Marsha Cope Huie, et al., *The Right to Privacy in Personal Data: The EU Prods the U.S. and Controversy Continues*, 9 TULSA J. COMP. & INT'L L. 391 (2002).

The European Union has been much more aggressive about protecting privacy online and many advocates have applauded the approach. The European Union has passed a Directive on the Privacy of Personal Data (the "EU Directive" or the "Directive").⁹⁸ The Directive declares that privacy is a fundamental human right and ensures that all member states have equivalent privacy protection.⁹⁹ All member states are required to pass laws creating a high level of protection for personal information.¹⁰⁰

The European Union stresses each citizen's right to have "information self-determination."¹⁰¹ The Directive attempts to balance business interests with individual privacy concerns by putting strict restrictions on the ways in which data collectors can collect personal information.¹⁰² Limits include controls over the collection of sensitive data, such as medical information, and limitations on collection of personal information that is not related to the purpose for which it was initially gathered.¹⁰³ Organizations collecting information in an EU Member State must report their activities to a national security board.¹⁰⁴ Clear notice must be given to individuals when their information is being harvested.¹⁰⁵ Citizens also have the right to access profiles containing their personal information and correct any errors.¹⁰⁶ The Directive requires explicit user consent any time their personal information is used in a way not contemplated during the first collection.¹⁰⁷ Additionally, the EU Directive requires appropriate security for the processing of personal information.¹⁰⁸

98. Council Directive 95/46, 1995 O.J. (L281) 31(EC) [hereinafter EU Directive], discussing the protection of individuals with regard to the processing of personal data and on the free movement of such data.

99. *Id.* at 10 (noting that privacy is a fundamental human right as recognized "both in Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms and in the general principles of Community law"); see also Julia M. Fromholz, *The European Union Data Privacy Directive*, 15 BERKELEY TECH. L.J. 461 (2000) (analyzing the EU Directive).

100. The EU Directive, *supra* note 98, at Art. 1 ("Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data").

101. Joel R. Reidenberg, *E-Commerce and Trans-Atlantic Privacy*, 38 HOUS. L. REV. 717, 731 (2001).

102. *Id.*

103. *Id.* at 732.

104. *Id.* at 733.

105. *Id.* at 732.

106. Reidenberg, *supra* note 101, at 731.

107. *Id.* at 732.

108. *Id.* at 732-33.

Because geographical and political borders do not bind the Internet, the EU added provisions concerning transfer of data between countries.¹⁰⁹ The Directive prohibits the transfer of data across national borders to countries without adequate privacy controls.¹¹⁰ Also, to ensure the local rules apply regardless of where the information collector is based, choice of law provisions in the Directive indicate that the laws of the state in which the data harvesting takes place will apply in any legal action.¹¹¹

Constitutional hurdles make it highly unlikely that the EU directive will be adopted in the United States.¹¹² While the Directive declared that privacy is a fundamental human right, the U.S. Constitution places a much higher value on freedom of information. Critics of the EU approach claim that if the laws were imported into the United States it would run afoul of constitutional protections, namely First Amendment protection and protection against government takings.¹¹³ A privacy law would violate the First Amendment if it were a government action that restricted freedom of expression. "[W]hen privacy rights conflict with free expression rights before the Court, the latter prevail, virtually without exception."¹¹⁴ Any law that attempts to protect privacy by restricting information faces significant First Amendment obstacles.¹¹⁵

The EU Directive would face similar problems overcoming the takings clause of the Fifth Amendment. The takings clause prohibits the government's ability to take private property without legal due process and just compensation.¹¹⁶ The prohibition has even been extended beyond tangible property to certain kinds of stored data.¹¹⁷ It is debatable whether the Fifth Amendment would stop the federal government from adopting the EU Directive, because collected personal information has been found to be the private property of the

109. *Id.* at 733.

110. *Id.*

111. Reidenberg, *supra* note 101, at 733.

112. Fred H. Cate, *The Changing Face of Privacy Protection in the European Union and the United States*, 33 *IND. L. REV.* 173, 203-9 (1999-2000) (discussing the First and Fifth Amendment limitations to application of the EU Directive in the United States).

113. *Id.*

114. *Id.* at 204.

115. *Id.* at 205.

116. U.S. CONST. amend. V ("No person shall . . . be deprived of life, liberty, or property, without due process of law; nor shall private property be taken for public use, without just compensation").

117. *Ruckelshaus v. Monsanto Co.*, 467 U.S. 986, 87 (1984) (finding that the takings clause applies to health, safety and environmental data cognizable as trade-secrets).

collector.¹¹⁸ Nonetheless, it is possible the government would be required to compensate profilers for regulations restricting their use of their data.¹¹⁹

D. The Current Absence of Legislation

Despite the drawbacks of the standard solutions to the challenge of online privacy, both the federal and state governments have still proposed many legislative solutions – albeit unsuccessfully. Although there have been several hundred different privacy related legislative proposals brought up at the federal level and almost four times that amount at the state level, so far, nothing related to marketers' profiling activity has passed.¹²⁰ These legislative attempts have failed for many reasons.¹²¹ Chief among those is the government's general reluctance to regulate the Internet on any issue.¹²² Because the Internet has been growing so rapidly – even during the economic downturn – politicians do not want to be seen as putting obstacles in the way of that development.¹²³ The result has been very little regulation of the Internet.

Aside from that general reluctance, however, several other reasons account for the lack of legislative action to specifically regulate privacy online.¹²⁴ Many businesses that operate online argue that limiting personal data collection will hurt the economy, and without proving tangible damage the harm is unnecessary.¹²⁵

118. See Alan E. Littmann, Comment, *The Technology Split in Customer List Interpretation*, 69 U. CHI. L. REV. 901, 901 (2002) (noting that courts have treated customer lists containing personal information as alienable).

119. Cate, *supra* note 112, at 207-08.

120. Keck, *supra* note 29, at 93; see also Jennifer O'Neill, *Congress Navigates a Flood of Net Privacy*, PCworld.com, at <http://www.pcworld.com/news/article/0,aid,42002,00.asp> (Feb. 20, 2001).

121. Schwartz, *supra* note 2, see also Major Consumer Internet Privacy Bills in the 106th Congress, Center for Democracy and Technology [hereinafter INTERNET PRIVACY BILLS], at <http://www.cdt.org/legislation/106th/privacy/majorbills.shtml> (last visited Aug. 28, 2005).

122. See, e.g., Elizabeth Hurt, *What does Bush Mean for E-commerce?*, at <http://www.business2.com/articles/web/0,1653,16423,00.html?ref=cnet>. (there is "bipartisan respect for an unregulated Internet as key to a healthy economy").

123. *Id.*

124. See Declan McCullagh & Ryan Sager, *Privacy Laws: Not Gonna Happen*, WiredNews, Mar. 2, 2001, ("[A] combination of factors—including widespread disagreement on Capitol Hill about what form legislation should take, increasingly vocal opposition from business groups, and concern that intervention might harm the economy—could derail the best efforts of privacy advocates.") <http://www.wired.com/news/privacy/0,1848,42123,00.html>.

125. *Id.*

Advocates of this position believe that any legislation that does pass should be narrowly tailored to fix a specific problem, and that lack of consumer confidence is not sufficient.¹²⁶ Because there have not been widespread actual harms associated with data collection, therefore, these companies argue that there should not be any regulation of the practice.¹²⁷

Others contend that the market will correct itself without any government intervention.¹²⁸ If consumers truly value their privacy, then they will become more educated on the topic.¹²⁹ Eventually privacy-conscious consumers will become more attracted to websites with better protection. Conversely, if the public does not "vote with their feet" (or eyeballs, in this case) for sites with stricter privacy policies, then privacy may not have been as large a concern as first suspected.

The largest current obstacle, however, is the debate over whether legislation should fall under an opt-in or opt-out rule.¹³⁰ If opt-out regulation were adopted, then the default rule would be set to allow data collection unless consumers specifically request out of the system. Under an opt-in default rule, by contrast, businesses would need to convince consumers to permit collection. Obviously, profilers prefer the former while privacy advocates prefer the latter model. The proposals that have gained the most attention and are viewed as the most realistic would require commercial sites to post a privacy policy and consumers must then decide whether or not to participate.¹³¹

These issues are all symptoms of a more overarching dilemma, however. Legislation is designed to represent community ideals and values. Yet, while the community struggles to come to a consensus, even scholars have offered little guidance because their views mirror the divisions apparent in the rest of the public.¹³² Not only is there an absence of an overwhelming majority on the topic, a plurality is not

126. *Id.* ("To pass privacy legislation just because it will boost consumer confidence but undermines the economy isn't a good idea.")

127. *Id.*

128. *See, e.g.,* Need for Internet Privacy Legislation: Hearing Before the Senate Commerce, Science and Transportation Committee, 106th Cong. (2001)(statements of Sen. John McCain)(stating a disbelief that laws are the proper way to control the Internet).

129. *Id.* (stating the consumers should be informed about their personal information to make appropriate decisions regarding their privacy).

130. McCullagh & Sager, *supra* note 124.

131. *Id.*

132. *See* discussion *supra* Part II.C.

even present. Congress typically struggles in situations where it is difficult or impossible to garner a clear majority – or even a plurality – accord. So far, most legislative proposals have attempted to draw distinctions despite this theoretical morass by establishing a specific range of proper behavior that is deemed suitable for every member of the public.¹³³ Without a clear definition for privacy, however, the determinants of inappropriate behavior become rather arbitrary as the value people place on their privacy may be relatively evenly distributed across the population.

Further, these proposals will not change the inefficiency that results from the all-or-nothing choice with which both consumers and profilers are confronted.¹³⁴ Ultimately, whether the default favors profiling or privacy, those who desire a middle ground are not given that option. By trying to define and quantify privacy, legislatures are ignoring people's diverse preferences.

Legislators are lodged between profilers who exhibit proven economic benefits from their behavior, and consumers with an ill-defined but powerful affinity for their privacy. While the government does not want to ignore the emotional pleas for privacy protection, it cannot deny the financial gains. This impasse has not yet been overcome because the ultimate goals that the proposed legislation has tried to attain so far have been misplaced. Policy makers should not aim to triumph over the hurdle of defining or valuing privacy (which may ultimately prove impossible), but should attempt the more modest objective of allowing a level of consumer confidence and trust whereby the Internet can be used at its most efficient level. The remainder of this paper will detail a solution employing some of the same technologies that are currently being employed to collect data; this technology can instead be used as a mechanism for individual consumers and profilers to work together to create an exchange for personal information. Specifically, the technology can be used to

133. *E.g.*, Internet Spyware (I-SPY) Prevention Act of 2005, H.R. 744, 109th Cong. (2005) (attempting to make accessing protected computers using spyware a criminal offense); Software Principles Yielding Better Levels of Consumer Knowledge Act, S. 687, 109th Cong. (2005) (making it unlawful to install spyware on a computer used in interstate commerce without the users knowledge); Information Protection and Security Act, H.R. 1080, 109th Cong. (2005) (directing the FTC to promulgate regulations over data collectors and authorizing states to bring civil claims to enforce FTC regulations); Information Protection and Security Act, S. 500, 109th Cong. (2005) (same); Privacy Act of 2005, S. 116, 109th Cong. (2005) (Prohibiting sale or disclosure of PII unless notice has been given and users are given an opportunity to object).

134. *See* discussion *supra* Part II.B.2.

foster negotiations between the parties that should help the market achieve a more efficient allocation of privacy protection.

III. Technology as a Market Creator

In the case of online advertising, the most reasonable approach is to overcome existing inefficiencies by allowing both users and marketers to place a value on personal information for themselves. Legislation can attempt to foster a negotiation where all involved can come to a mutually beneficial decision. Therefore, the goal of any legislation should not be to place a definition and value on privacy, but to enable trust by allowing users and websites to set the optimal terms for Internet use.

With this goal in mind, the best way to enhance trust is to allow consumers to decide their own privacy's worth and then allow websites to decide how much content to give up in exchange for each user's choice of privacy protection. The government can help to encourage an exchange of information between consumers and websites. Through private interactions, the parties can determine the importance each side places on the information. Although at first glance it seems that the transaction costs from such an arrangement would be tremendous, online software could be used to automate the negotiation and decrease costs to a manageable level.

An automated system could facilitate a privacy-for-content transaction between the user and the website. Users could offer private information to websites. In exchange, the websites would allow access to their content. As users allow more collection of personal information, websites could increase the users' level of access to the sites' subject matter. In this system, when a user is not willing to allow the websites to gather much information, the website can respond by only authorizing a cursory right to view content. Conversely, when users are willing to volunteer more information than sites would normally be able to collect under the current model, the websites could grant full access or even special privileges to those users. The sites could offer coupons or other incentives to encourage users to furnish additional information. In effect, the transaction taking place will be an information-for-information exchange; the user offers personal information and in return the website would allow access to the site's substance.

To simplify the process, the transaction can piggyback on the communication that is already taking place between user computers and the website servers. Presently, when a user visits a website, the user's computer relays a request to the site for the content that

webpage provides. In return, the site sends its content, and often, takes information from the user in return.¹³⁵ Currently, this communication and information divulgence occurs without the user's consent or even knowledge. An automated negotiation would simply correct the information asymmetry in the current model and condition the website's release of content on the release of the user's personal information.

For instance, a web user could program her browser to prevent the release of all personally identifiable information. When the user visits a website, say – a news site – that wishes to ascertain personally identifiable information, the user's browser would stop the collection. In response, the web server would inform the browser that if it cannot proceed with its data collection the site will only provide access to headlines and a few select full stories. This way the website and the user can exchange data up until the point where the marginal cost for one of the parties giving up more information equals the marginal benefit of receiving any new information from the other.

The business running the website can decide how much content it is willing to release in exchange for different levels of personal information. If a website decides that it will not provide very much content unless it is allowed to collect a high level of personal information, it is likely many consumers will decide not to visit that site. In the news-provider example, if the website restricts access to headlines unless it is allowed to collect personally identifiable information, users will simply turn to other, more "generous" sites. As a result, traffic would decrease for the restrictive website as consumers search for competitors that provide more favorable terms of exchange.

Of course, over time websites will adjust their menus of options in response to consumer demands. If the menu of privacy options is well defined, websites could make calculated judgments as to their expected loss in consumer traffic versus the gain in profiling information. If the menu system allows users to decide among many distinct privacy levels, the website can calculate the type of personal

135. Once a web address (in the form of either an Internet Protocol Address or domain name) is typed into a browser, the browser contacts the computer at the address. The browser alerts the server that the user is requesting the server's web page. The browser also tells the server its own address. The server may then request more details about the user's computer such as the browser type, the operating system and the screen size. This information is used to ensure that the page is displayed in its optimal format. The server then sends the web page to the browser to display to the user. For a detailed description of how computers and web servers communicate on the web see Jeff Tyson, *How Stuff Works*, at <http://computer.howstuffworks.com/internet-infrastructure.htm>.

information it values most and what information is subordinate to their purposes. The news site, therefore, must decide if the loss in traffic is worth the benefit from the types of personal information they are trying to collect. A loss in consumer traffic can be devastating for a commercial website. Because many sites are subsidized by advertising revenue, decreases in traffic means a decline in sponsorship.

In a Coasean world without transaction costs, marketers and users will bargain to the most efficient allocation of privacy.¹³⁶ The automated system I propose helps reduce transaction costs and allows consumers to have better information. Thus, it brings us closer to a Coasean equilibrium result.¹³⁷

A. Detailed Description of the Technology

With this framework in mind, an automated system can now be explained with more specificity. The automated system can be embedded into web browsers and can communicate with web servers that are pre-programmed to complete the negotiation. When a consumer first installs her web browser, the installation program could prompt the user to input her privacy preferences. This could be done in many ways; one way is through a series of multiple-choice questions. Each question could be primed by a brief description of the type of information with which the question is dealing and the ways that information can be used once given up. The description could also inform the user about the benefits she may be giving up by not allowing the collection of data.¹³⁸

136. ROBERT COOTER & THOMAS ULEN, *LAW AND ECONOMICS* (4th ed. 2003) discussing Ronald Coase, *The Problem of Social Cost*, 3 J.L. & ECON. 1 (1960). For example, if a cattle rancher and a corn farmer own adjacent land, the two parties can bargain to arrive at the most efficient distribution of the land depending on the value each party receives from that property. The cattle rancher would be willing to give up a certain portion of his land as long as he received a payment that is greater than the incremental benefit he would receive from allowing his cattle to graze on that property. Likewise, the corn farmer would be willing to pay for a portion of the cattle rancher's estate, providing the payment was less than the incremental benefit the farmer could receive from growing corn on that land. If the amount the corn farmer were willing to pay exceeded the amount the cattle rancher would require, the cattle rancher would sell that part of his land. At the same time, the corn farmer will continue to purchase more land from the cattle rancher until the marginal benefit of purchasing the next piece of land is less than the price necessary for the cattle rancher. Therefore, each portion of the property will be distributed to the party who values that portion the most – a Pareto efficient equilibrium will be achieved. *Id.*

137. Coase, *supra* note 136.

138. See 2000 FTC REPORT, *supra* note 35, at 8-10 (consumer benefits from online data collection include allowing websites to remember usernames and passwords, creation

Table 1: A proposal for menu setting for the automated system.

PRIVACY LEVEL / INFORMATION AVAILABLE FOR COLLECTION	TYPES OF INFORMATION AVAILABLE FOR COLLECTION AND TO WHOM
Highest privacy / no information available	The user does not allow anyone to collect any information. User consent is required before any monitoring can be conducted for any reason.
High Privacy Intermediate Levels	Single-session cookies can be set by the website. The cookies can help a user complete a transaction, but the site cannot save any data that is not related to the specific exchange. Data cannot be used for advertising.
	The website can collect information, but third party advertisers cannot. The site could use the information for its own advertising, but cannot sell the data.
	Websites can collect information, but still cannot sell it. Specific user consent is required any time a third party wishes to collect data.
Medium privacy / medium information available	Allows cookies to be set on the computer and surfing habits to be monitored by the website and third parties. Profiles cannot be combined with personally identifiable information. The non-identifiable profiles can be sold.
Low Privacy Intermediate Levels	All advertisers can collect information, but cannot combine profiles with information about the user's offline activities.

of online shopping carts, personalization of home pages, making recommendations about future purchases, targeted advertisements sent to interested consumers, and reduction of repeated exposure to the same ads).

	Both the sites and third party advertisers can collect information. Websites can combine profiles with personally identifiable information, but third parties cannot.
	Any advertisers can set cookies, collect information, and combine profiles with personally identifiable information.
	The user will make personal information such as their name, address, phone number, email address and product interests available. The user would not be available for future contact.
	Offers name, address, phone number, email address and product interests. This setting will also make consumers available to marketers who wish to contact them for further information.
Lowest privacy/most information available	The user would make personal information available to marketers and would make himself available for future contact. Further, the user agrees to provide even more detailed information, if requested.

The system would provide consumers a menu from which to choose how much information they are willing to give up and for what price (*see* Table 1). At one end of the gamut, users could elect to prohibit any information from being tracked without express approval. This prohibition would extend to information required for the website to provide services; however, the exclusion would not stop consumers from providing certain information manually. For instance, if a website normally places a cookie on a user's computer for the sole purpose of tailoring the appearance of their pages for the user,¹³⁹ that service would not be permitted. Therefore, the user would not be able to customize a website, but would be able to protect any disclosure of her personal information.

At the other end of the privacy-preference spectrum, users could elect to actively sell all of their information. The setting would go beyond just allowing websites to collect information; users who

139. For example, many web portals such as MyYahoo! allow users to choose the information that will appear on the user's web page. The user can request that the site provide local and business news, but not sports. The user can also choose the look of the page, specifically the color scheme and layout. Since this level of customization requires the web server to remember information about the user, such as their hometown, under the maximum privacy protection these services would not be provided.

choose this extreme will effectively be putting out an active solicitation to profilers who may want to purchase their information. In effect, this setting will create a venue through which users who wish to sell their information can find buyers. Under the current regime, consumers cannot operate in this manner. This setting is ideal for people who place a very low value on their personal information, but do prefer to receive very tailored advertisements.

Consumers who volunteer to sell their information do not mind giving up personal information about themselves when they are adequately compensated. People who choose to set their browsers to this extreme would not merely allow marketers to track their movement online, but would in fact be offering even more information than the data collectors could mine on their own. These consumers could enter the information that they wish to sell into their browser to help further reverse transaction costs. This way, the consumer will not have to manually supply his personal information to each site that wants to collect the data; instead, the browser will automatically supply the data when the web server makes the request.

Most likely, many marketers would be willing to pay for this information in some form. Even in the current model, marketers pay for personal information about users from websites, either by purchasing entire user profiles or by paying for the ability to work through a website to gather the information. Conceivably, as long as the price is on par with the current model, these data collectors would be willing to pay the users directly for the same information. It is even possible that the marketers would be willing to pay even more than they currently do. By paying the users directly, the marketers will receive more information about the users than through mere observation. Also, there will not be harsh consequences to the company's reputation because the collection will be straightforward, unlike under the current scheme. Furthermore, the information is more likely to be accurate because the users can provide the data directly and willingly. Marketers who would like to purchase accurate and detailed information about consumers can either contact the consumer with an offer or collect the information from the browser for a predetermined price.

A sample transaction under this setting would work as follows. A user could select a price ahead of time and enter that price into his browser. Whenever a data collector is willing to pay that price, they will get access to the information.¹⁴⁰ The tender could be a cash

140. One serious issue that may arise from this system is the threat to the user's

payment, discount coupons or any other sort of compensation. Consumers will have an incentive to set a reasonable price for their information if they wish to be compensated. Although many data collectors may be prepared to pay for the information, they may not be willing to pay exorbitantly high prices. Therefore, users who truly wish to sell their information would try to set an affordable price.

This setting would also be beneficial for consumers who desire specific targeted advertising. For example, if someone is currently in the market for a car or other major consumer good they could enter their buying preferences into the browser. The consumer could then set a low price for marketers to purchase the information – possibly offer it for free. As marketers collect the information from the consumer, the marketers will learn about the purchase the consumer wishes to make. The marketer could then target advertisements to the user. These advertisements could help inform the user about different products and prices in the relevant market. Because the ads will be targeted to specific consumers, the seller could also offer special discounted prices for specific products. This way, the advertiser benefits by only having to advertise to interested consumers and the user benefits from becoming more informed about desired products, which, in turn, lowers search costs. This is a significant improvement over the present system where marketers must extrapolate users'

personal security. It is possible nefarious characters will try to access this information either by purchasing it or through hacking. Once the data is accessed, the information can be used to carry out identity theft or other crimes. While this system may raise the risk of this sort of criminal behavior, these risks already exist and are addressed in the criminal law. *See, e.g.*, The Identity Theft and Assumption Deterrence Act, 18 U.S.C. § 1028 (2003) (making it a federal crime to "knowingly transfers or uses, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, any unlawful activity that constitutes a violation of federal law, or that constitutes a felony under any applicable state or local law."); ALASKA STAT. § 11.46.565 (2005) ("A person commits the crime of criminal impersonation in the first degree if the person . . . without authorization of the other person, uses the access device or identification document of another person to obtain a false identification document, open an account at a financial institution, obtain an access device, or obtain property or service"); CAL. PENAL CODE §§ 530.5-8 (2002) ("Every person who willfully obtains personal identifying information . . . of another person, and uses that information for any unlawful purpose" is guilty of identity theft); FLA. STAT. ANN. § 817.568 (2003) ("Any person who willfully and without authorization fraudulently uses, or possesses with intent to fraudulently use, personal identification information concerning an individual without first obtaining that individual's consent, commits the offense of fraudulent use of personal identification information, which is a felony of the third degree"); N.J. STAT. ANN. §§ 2C:21-17 (2003) (illegal identity theft is when someone "impersonates another or assumes a false identity and does an act in such assumed character or false identity for purpose of obtaining a benefit for himself or another or to injure or defraud another").

interests and users have no way to indicate their preferences to the market.

One question that may arise is: how will the specific marketers find out about consumers who are willing to sell their information? If a consumer who is in the market for a house is visiting an online news-provider, how will the housing advertiser know to purchase the information, and the news-provider know that it should not? First, the problem with the news-provider can be solved by the pricing scheme the consumer uses. If the consumer truly wants advertisements about houses, that user can set their browser to release that information for free. That way the news-provider's server can look at the user's preferences quickly and decide whether it wants to send specific ads.

Conversely, to solve the problem of alerting the appropriate housing marketers, the system could take advantage of the network that advertisers, such as DoubleClick, have already put in place. These network advertisers already contract with thousands of websites to collect information. When a user visits a site in the network, the advertiser could collect the consumer's information and alert their clients in the housing market.

Between the two extremes of the privacy preference spectrum described above fall many intermediary points. These different levels of privacy could provide different benefits and protections for consumers. The user could choose to allow collection of personal information, but not personally identifiable information. For example, if a user decides she does not mind being watched or receiving targeted advertising, but does not feel comfortable having their profile tied to them personally, that level of protection can be afforded.

Another point on the spectrum could allow the collection of certain types of information, but not others. For instance, the user could allow the assembly of a profile containing information about the type of sites the user visits, but not information about in which city the person lives. This option could satisfy users who do not mind data being gathered about their online habits, but would prefer to keep information about their lives offline secure.

The browser could also be set to prevent users from even manually turning over information to the website. Parents may choose this option as a security measure to prevent their children from unwittingly giving up information. Some parents may also like the idea of preventing their children from making purchases on the Internet, which require some information to be given over to the website. Manual data entry is one way marketers combine their

profiles with personally identifiable information under the current regime.¹⁴¹ This setting could help parents protect children's information and also assist anyone who wants to make sure they do not mistakenly turn over information themselves.

This setting could also address certain consumer fears by allowing consumers to request that websites only use the information they collect for the specific purpose for which the information is entered. For example, the user's address may be turned over to a site that sells and delivers books to help facilitate a delivery. The user's pre-programmed browser would then instruct the web server that the information could only be used for that single purpose – the delivery of the book.

Although this discussion has focused on the user's side of the bargain thus far, the websites would also have to make certain adjustments to comply with this system. Websites would need to tailor their systems based on how much content they are willing to offer in exchange for the personal information the user will provide. The site could also decide to charge a subscription fee if it is not given access to enough information. Because many sites are subsidized by advertising revenue, if they are not able to collect sufficient information, they will not be able to operate their site effectively. Therefore, charging a subscription as an alternative to giving up the collections of personal information may be an attractive solution for some sites.

While many privacy advocates demand better security for information, most do not offer alternative revenue sources for the websites.¹⁴² Under the proposed automated system, the sites could choose how much content to provide and whether they need to charge a supplement to their advertising income. As discussed above, this decision can be computed by calculating the point at which the marginal utility of collecting personal information falls below the marginal cost of providing more content or charging a subscription.¹⁴³

One issue that may arise is how smaller websites or personal sites will implement the system. While it may be relatively easy for larger

141. See Federal Trade Commission, *Online Profiling: A Report to Congress* (Jun. 2000). A marketer could tag a user's computer with a cookie and observe the user's behavior online. Then, when the user makes a purchase and has to enter his name and address, the information can be added to the profile. From then on, whenever the marketers track the computer with that cookie, it will also have the personally identifiable information handy.

142. See discussion *supra* Part II. C.

143. *Id.*

websites to customize, smaller sites may not have the wherewithal to install such a system. For these sites, they may choose to put in a one-size-fits-all setting for their system. Personal websites can simply set their page to allow complete access to anyone, regardless of the users' privacy preferences. Smaller commercial websites could set a firm floor: users who have restrictive privacy preferences below the floor will not receive any access and users above the floor get total access. This way, smaller sites do not have to go through the expense of developing a complex access scheme that depends on user preferences.

Of course, this regime may cause some sites to fail. Most likely, there will be a few sites that cannot afford to give up the total access to personal information that they currently enjoy. With regards to privacy, however, these sites represent a loss to overall economic efficiency. As mentioned above, the current state of privacy protection is not optimal.¹⁴⁴ If websites fail because they cannot afford to restrict their access to personal information, the sites are not operating efficiently within the market. When the automated system is put in place, the resulting privacy allocation will be much closer to the most efficient level. If a website cannot exist at this equilibrium point, then the site was most likely collecting more information than an efficient market would have allowed, anyway. The loss of these sites will help correct the current market failures. The result is a traditional *Laissez Faire* solution; either the site will adjust to the market or it will fail.

The cost of implementing the system will not be exorbitant to most users or sites, however. An advantage of this system from an operational perspective is that it can be easily developed from existing technology. Most web browsers already allow users a certain level of input about the level of privacy they desire online.¹⁴⁵ This pre-existing system can be modified to give the user more options and to communicate these choices with the websites servers.

144. *Id.*

145. For instance, in Microsoft's web browser – Explorer – users can choose among several levels of protection from cookies. At one end, cookies will be blocked entirely; conversely, users can also choose to allow complete surveillance. Other browsers use different variations of this system. The system does not block technology such as web bugs, however. Also, the system is completely a defensive measure. Users can try to block websites' encroachments on privacy, but the system does not deal with the marketers to assure they will not try to circumvent the privacy protections. This type of system may encourage an arms race between users and websites, with each trying to develop better technology to combat the other. This arms race is an economic waste.

On the website side, servers are designed to collect information from users. Currently, the server can choose to format the page in specific ways to account for the user's computer capabilities and software. Many websites also can determine whether certain content should be made available to specific users. For example, some sites require a subscription, and the site must determine whether the user attempting to access the site has paid for that right.¹⁴⁶ Also, many businesses, such as banks, keep a separate account for each client.¹⁴⁷ These sites require a username and password to access individualized accounts. Because websites are already capable of customizing and tailoring content for each user who visits the site, it is conceivable that the sites could also customize their content to each visitor based on the user's privacy preferences.

Another possibility would be to allow the system to be loosely based on the technology from a current privacy program called the Platform for Privacy Preferences Project ("P3P"). This platform is already in place on many current browsers and websites.¹⁴⁸ P3P is a developing industry standard for privacy practice designed to create a benchmark for privacy that can be easily interpreted by users' computers.¹⁴⁹ The program attempts to simplify and automate website privacy policies.¹⁵⁰ Essentially, P3P is designed to allow users to enter their privacy preferences into their browser (similar to this proposed solution) and at the same time websites can convert their privacy policies into a machine-readable language. When the browser visits a website, it can read the site's policy. If the terms of the policy do not match the user's preferences, the browser will alert the user. The users can then decide whether or not they want to remain at the website or move on to a more privacy-friendly site.

An automated system could conceivably be built on top of the existing P3P platform. Because the technology already exists and has been extensively employed in some form, implementation would not be overwhelmingly expensive. Although P3P represents an important first step, it is important to realize that it is only a beginning. P3P

146. See, e.g., www.lexisnexis.com.

147. See, e.g., www.ameritrade.com.

148. Approximately 25% of the top 100 websites had adopted the program by the beginning of November 2002. <http://www.w3.org/2002/12/18-p3p-workshop-report.html>. Both Netscape and Internet Explorer have some form of the P3P system already in place. <http://www.w3.org/P3P/implementations>.

149. See Platform for Privacy Preferences, <http://www.w3.org/P3P/#what> (last visited September 3, 2005).

150. *Id.*

simply alerts users when some parts of their privacy preferences do not match a website's privacy policy. To be fully effective, however, the system must have many more levels of control for both the users and websites. Additionally, the system must foster an exchange between the parties. P3P is grounded on a model of "notice and choice."¹⁵¹ The automated system proposed here goes well beyond this simple model. The automated transaction is not based on the concept of simply alerting a user, but allowing the user to interact with a website. The system will allow the two parties to come to mutual – and enforceable – decisions about the value of private information and the related value of the website's content.

B. The Role of the Government

The market's experience with P3P can also provide guidance with regard to the second part of this proposed solution. Although the P3P technology is relatively widespread, it has not taken hold with consumers or smaller websites.¹⁵² By making the system mandatory and creating a cause of action for violating the agreement, the government can ensure more pervasive adoption of an automated program and therefore even more trust in the system.

1. Mandatory Adoption

In the case of P3P, although the system was originally adopted relatively quickly among top websites, that growth slowed with the economic downturn following the burst of the dotcom bubble.¹⁵³ Several difficulties have plagued the program since its inception, which has contributed to the lack of interest from both consumers and websites. One fundamental problem has been a pervasive misunderstanding of the concept behind the program. Although the idea of P3P has been promoted as a cure-all for Internet privacy,¹⁵⁴ it is actually only an attempt to create an industry standard for privacy policies.¹⁵⁵ "P3P needs a regulatory or policy context to help protect

151. *Id.*

152. Paul Festa, *Promise of P3P Stalls as Backers Regroup*, CNet, Oct. 29, 2002, <http://news.com.com/2100-1023-963632.html>.

153. *Id.*

154. See, e.g., Lawrence Lessig, *The Architecture of Privacy*, 1 VAND. J. ENT. L. & PRAC. 56, 63-65 (1999) (suggesting that P3P could create a change in the architecture of the Internet and allow machines to be the agents to protect privacy).

155. Platform for Privacy Preferences website, <http://www.w3.org/P3P/#what> (P3P "is emerging as an industry standard providing a simple, automated way for users to gain more control over the use of personal information on Web sites they visit") (last visited September 3, 2005).

privacy, it cannot do this by itself."¹⁵⁶ This misunderstanding has led many privacy advocates to condemn the system for not providing enough protection, even though protection has never been the stated purpose of the program. The condemnation has led to deflated user interest.

Another obstacle has been economic. The protocol was conceived during an economic boom in the technology sector. Unfortunately, the market lost steam before the standard could be widely accepted. Because P3P is only a proposed industry standard, it is not mandatory. Supporters of the system believed websites would adopt the program as a result of user demand. The belief was that because users place such high value on their privacy they will generally be attracted to sites that use the protocol; as user preference for the system becomes apparent, websites will adopt the system to attract more traffic. Regrettably, this adoption pattern never developed, creating a cycle of disinterest. As smaller websites' economic resources diminished, their interest in providing privacy waned due to the cost of setting up the system and the loss of profiling-related revenue.¹⁵⁷ Once website adoption floundered, many web users (those who are aware of the system) gave up the hope that even setting up the system in their browsers was worth the effort. According to some online privacy progress reports, "[i]f few sites support P3P, consumers will have little incentive to use the technology, thus creating a sort of chicken and egg problem."¹⁵⁸

The cycle of disinterest intensified because the system is entirely voluntary, and the sites with the most to lose chose not to comply. These sites generally collect the most information and have privacy policies consumers would most like to avoid. For these sites, adoption of the standard would hinder their ability to collect information and hurt their profitability. Some critics believe the protocol can never reach the critical mass necessary to become a true standard because adoption is not in the best interest of many websites.¹⁵⁹

156. Center for Democracy and Technology, *P3P AND PRIVACY: AN UPDATE FOR THE PRIVACY COMMUNITY* (2000), <http://www.cdt.org/privacy/pet/p3pprivacy.shtml>.

157. *Id.*

158. Electronic Privacy Information Center, *PRETTY POOR PRIVACY: AN ASSESSMENT OF P3P AND INTERNET PRIVACY* (2000) (discussing the problems the creators of P3P had getting their system adopted as an industry standard), <http://www.epic.org/reports/pretypoorprivacy.html>.

159. Jason Catlett, *Open Letter 9/13 to P3P Developers* (Sept. 13, 1999) (arguing that P3P will hinder, rather than increase, privacy protections online), at <http://www.junkbusters.com/standards.html> (last visited Sept. 4, 2005).

Even if these sites do accept the standard, it does not come with any enforcement mechanism.¹⁶⁰ The protocol, therefore, does not breed the trust required to make the Internet perform optimally, further decreasing the probability of consumer adoption. In the current environment of unclear privacy laws, especially in the case of financial and medical websites, no one is sure how enforcement would even operate practically.¹⁶¹

A quick look at the causes of P3P's failure to take hold can lead to some clear solutions. The first issue to be addressed is the critical mass problem: websites will not adopt the standard without consumer demand, but consumers have not demanded the protocol without widespread website adoption. The question, then, is how acceptance of the system can achieve the critical mass where both consumers and websites view it as in their best interest to comply with the system.

There may be a simple fix to this problem – make the system mandatory. Without making compliance compulsory, websites will face a classic Prisoner's Dilemma game:¹⁶² although the adoption of the privacy system can benefit all websites,¹⁶³ each site will be better off individually by not adopting the system.¹⁶⁴ The most efficient result for the web community as a whole comes when all websites adopt a certain level of privacy protection. Protection benefits consumers by increasing the feeling of security; likewise, privacy can help online businesses because increased privacy can lead to improved electronic commerce.¹⁶⁵ If a site acts alone, however, it will lose the ability to

160. Electronic Privacy Information Center, *supra* note 158 ("Even where there is agreement about the privacy terms for a particular transaction, P3P provides no means to ensure enforcement of the stated privacy policies and the P3P developers do not seem particularly concerned about this problem").

161. *Id.*

162. COOTER & ULEN, *supra* note 136, at 93 n.3.

163. *See* 1998 FTC REPORT, *supra* note 4, at 3-4 (discussing how privacy can be beneficial for all websites).

164. Steven A. Hetcher, *The Emergence Of Website Privacy Norms*, 7 MICH. TELECOMM. TECH. L. REV. 97, 116-17 (2000/2001) (describing that although it may be to the industry's overall benefit to have increased privacy protection for consumers, each individual site has an incentive to lower its own particular privacy standards).

165. *See, e.g.*, Turow, *supra* note 11, at 22. Fifty-seven percent of respondents to a survey said it would bother them if stores that they shopped at collected detailed information. Further, the survey also found that only 49% of respondents said that if they trusted an online store that they would not mind giving the store information about products purchased during the last month. *See also* 2000 FTC REPORT, *supra* note 35, at 10-17 which describes many consumer concerns about profiling and notes that ultimately consumer concerns become business concerns. Another FTC Report notes that 87% of respondents to a survey were concerned about giving information to business online, and that it was not surprising that only a quarter of users who look for information online

collect detailed information about its consumers while its competitors maintain their advantage. The loss of this information will, in turn, decrease advertising revenue for the one site that complies. Sites that respect privacy will, therefore, have a difficult time competing financially with competitors that do collect information and maintain their marketing income. Hence, without across the board adoption, no individual site will have an incentive to decrease their data collecting behavior. The websites will, in fact, have motivation to avoid privacy protection, even if the rest of the community develops a strong privacy norm. If the site were to collect personal information while its competitors do not, the assembled profiles will be a scarcer commodity, and thus worth more to the advertising market.¹⁶⁶

The failure of self-regulation comes from the government's common assumption that the web community acts as a cohesive whole.¹⁶⁷

This is the fallacy of thinking that because a group, considered as a whole, would benefit from some particular political outcome, that therefore it is in the interest of each of the particular members of that group to do its part to help bring about this political outcome. It is simply false to assume that a typical website would have such an interest.¹⁶⁸

It is, therefore, necessary to compel action from the parties or else the individual self-interest of the websites will lead to a sub-optimal result.¹⁶⁹ While the industry has thus far shown an aversion to government regulation, opposition to the automated system should not be as firm because it does not force websites to adopt a strong privacy norm. The system will lead to increased consumer trust, but websites will not have to give up all of their profitable data collection behavior.

actually make online purchases. FEDERAL TRADE COMMISSION, THE FTC'S FIRST FIVE YEARS: PROTECTING CONSUMERS ONLINE (1999), available at <http://www.ftc.gov/os/1999/12/fiveyearreport.pdf>.

166. Hetcher, *supra* note 164, at 119 ("Each website would like all the other sites to be respectful so that it alone can take advantage of the more trusting consumers").

167. *Id.* at 117 (noting that the FTC has failed to create a successful privacy program because the programs are based on the assumption that websites act together rather than in their own individual self interests).

168. *Id.* at 117-8.

169. *Id.* at 119-123 (explaining why self-regulation cannot work, and that the government must take a more active role to protect consumer privacy).

2. *Create a Cause of Action*

The most important legislative aspect of an information-for-privacy solution is to allow users to bring suits against websites that fail to comply with the conditions to which their automated programs agree. By creating a private cause of action, consumer trust will be enhanced and websites will have an incentive to make sure consumers are aware of the agreement. While websites can currently suffer many harsh consequences including user-initiated lawsuits if the site does not comply with its posted privacy policy, the policies themselves do not have to be very respectful of users' privacy.¹⁷⁰ Nor is it required that the site make it easy for a consumer to understand the policy. The transaction costs are usually high enough for consumers that they never read the policies, and therefore websites do not have an incentive to post secure guidelines. Consumer transaction costs arise for several reasons. The policies may be hard to locate on the site. Once found, the policy can be extremely long and in complex, legalistic language. The transaction costs are usually high enough that most users would rather risk their privacy than spend the time to find out about each site's policy.

Because most users do not read the policies, websites are not very worried when they have to disclose unfair terms. If the users were to read the policies on many of the sites that they visit, they may be surprised to learn that their favorite sites generally collect and sell consumers' personal information unabated.¹⁷¹ The policies would also inform the users that third parties can collect information through the website, and these third parties are not even bound by the stated

170. For example, the Federal Trade Commission Act, 15 U.S.C. §§ 41-58 (2004) allows the FTC to bring suits against companies that do not comply with their own privacy policies, but it does not control the substance of the policies. *See, e.g.*, *Petco Animal Supplies, Inc.*, No. C-4133, 2005 FTC LEXIS 39, at 2-4 (Mar. 4, 2005)(bringing a claim against Petco for failing to adequately protect personal information collected from the website, even though their privacy policy states "At PETCO.com, protecting your information is our number one priority, and your personal data is strictly shielded from unauthorized access.").

171. *See, e.g.*, Turow, *supra* note 11 ("75% [of survey respondents] do not know the correct response—false—to the statement, 'When a website has a privacy policy, it means the site will not share my information with other websites and companies.'"). *See also* the "privacy guidelines" from *cnn.com* that states that both personally identifiable and non-personally identifiable information may be collected. *Available at* <http://www.cnn.com/privacy.html>. The guidelines go on to state that "Certain Time Warner sites may disclose personally identifiable information to companies whose practices are not covered by this privacy notice . . . that want to market products or services to you." *Id.*

policy.¹⁷² Additionally, many users may be disturbed to find out that the websites reserve the right to change the policy at any time without notice.¹⁷³ This means that to stay informed about a sites privacy practices, not only does the user have to read the posted privacy policy, the policy must be reviewed prior to each visit to the site to make sure it has not changed since the last review. Given that most current privacy policies offer so little restriction on the sites' behavior, the threat of suit for a violation does not really have any teeth. It would be extremely difficult for a website to actually violate their policy. Under the automated system, however, the conditions to which sites agree could provide significantly more protections than are currently offered. Under this system, the consequences from a lawsuit would be much more dire for a website and provide more security for users.

One issue that would exist for users under the automated system, however, would be the cost to monitor and enforce the agreement.¹⁷⁴ Discovering a violation could be difficult for users. It may also be prohibitively expensive to litigate the matter; most litigation will cost significantly more than any damage from a violation. As a result, websites may not feel obligated to respect the terms of their arrangement because they will not have a real fear of any penalty.

The solution for both the monitoring and enforcement costs could be class action suits and consumer activist groups. While litigation expenses may be too high for most individual users, collectively it will be cost effective for consumers to bring an action against non-compliant sites. Presumably, if a website were to break its agreement with a single user, it would also break the terms of the contract with other users. It would be costly and pointless for a website to seek out a single user to cause a violation. The value of profiling comes from the information in the aggregate; it is not cost-effective to single out users for observation. A violation of the terms of the automated agreement will probably result from a website adjusting its server to ignore the terms of all of the agreements. Therefore, violations will be much more widespread across visitors to

172. See, e.g., <http://www.cnn.com/privacy.html>.

173. *Id.* ("From time to time, we may update this privacy notice. We will notify you about material changes in the way we treat personally identifiable information by placing a notice on our site. We encourage you to periodically check back and review this policy so that you always will know what information we collect, how we use it, and to whom we disclose it.")

174. COOTER & ULEN, *supra* note 136, at 101. Two primary sources of transaction costs are monitoring and enforcement. A third cost is communication. Ideally, the automated system will reduce communication costs to zero.

that site. All the users against whom the website breaches could bring a class action suit against the site to help defray the costs of litigation. Additionally, if monetary awards were possible, lawyers may seek out litigation themselves and find victims to represent. This will help decrease monitoring costs for the users.

The only adjustment the government would need to make to normal contract law would be to allow a single suit for the violation of many different contracts. Defendant websites may argue that each time a user's browser negotiates a deal with a website server a new contract is created. A website that is targeted by litigation could claim that a violation is a breach of each contract separately and therefore requires separate litigation. Any legislation should allow collective actions in such cases and the damages could be split according to the harm done to each consumer.

Aside from class actions, another solution could be consumer privacy advocate groups that bring suits against websites on behalf of all consumers. Already some consumer groups bring significant resources to their battles for more online privacy.¹⁷⁵ Advocate groups have brought complaints to the FTC, to congressional legislative meetings and some privacy related lawsuits.¹⁷⁶ It is very likely these groups would continue their vigilance to promote enforcement of the automated agreements.

IV. Benefits From The Automated System

By mandating a technological solution to the problem of online privacy the government can bring several benefits to both consumers and websites. Part A of this section will focus on benefits to both consumers and websites. Specifically, part A will address the ways an automated negotiation can help both sides internalize the other's positions and reduce the economic externality websites are currently imposing on users. The discussion will also focus on how an automated system can help increase consumer trust. Once established, the increased trust can serve benefits on both websites and consumers. Part B will discuss benefits that can be enjoyed by

175. For example, Electronic Privacy Information Center ("EPIC") is a public interest research center that focuses on privacy issues. According to their 2003-2004 Annual Report, EPIC raised between one million and one and a half million dollars each year from 2001 to 2003. EPIC ANNUAL REPORT (2003-2004), http://www.epic.org/epic/annual_reports/2003.pdf.

176. *Id.* at 11 (listing several cases that EPIC brought or to which they contributed including complaints against the Department of Defense, Department of Justice and others).

websites specifically. Websites can benefit from more certainty about future legislation and litigation. Part C will turn to how the system can allow the government to avoid the impossible task of defining and valuing privacy. Finally, the last part of this section will address some issues that may linger in any system that allows privacy to be commodified.

A. Benefits for Both Consumers and Websites

The automated system can help each party internalize the motivations of the other by eliminating the all-or-nothing option that currently exists. Profilers create a negative externality when they collect information; while they pay the cost for the actual collection of the data they do not pay the costs their intrusion tolls on Internet users' lives.¹⁷⁷ In the current system, many consumers are also ignoring the benefits marketers can provide. Consumers who choose to avoid the Internet or decrease their use of the web are disregarding the possible benefits from targeted advertising. Both parties to this transaction are discounting the implications of their actions on the other.

An information-for-privacy exchange could allow both sides of the transaction to take the other's interests into account. Profilers would be more sensitive to user interests when the parties negotiate. Part of the internalization, of course, will be obligatory. When the websites are forced to negotiate and agree to some user demands for increased security, they will have no choice but to respect privacy concerns. Not all of the internalization will be required, however. Marketers currently spend significant resources to develop advertisements that can attract progressively more disinterested users' attention. If users agree to allow targeted advertising, they are much more likely to devote some attention to the advertisements. The advertisements that consumers do receive will be much more tailored to them personally and consumers will be more likely to solicit the businesses that market to the consumer's particular needs.

Presently, barrages of advertisements assail users each time they log on to the network. Advertisers now use various blinking lights, moving pictures and the notorious pop-up ads to attract users to their business. Most users have learned to simply tune out all the advertisements and focus completely on the content of the page.¹⁷⁸

177. See discussion *supra* Part II.B.

178. However, a recent survey found that over 93% of consumers find pop-up advertisements "extremely annoying", Hostway, CONSUMERS' PET PEEVES ABOUT

Worse for the content providers, consumers may avoid some pages completely if the attempts at their attention become too much of an annoyance. Online advertising has become such an aggravation that many software programs are now available that block advertisements and help thwart attempts to gather information.¹⁷⁹ In response, marketers are constantly developing ways to work around these obstructions.¹⁸⁰ If the consumer could negotiate with a website to allow the collection of specific personal information, the advertisements are likely to be more tailored to the users disclosed preferences. As a result, marketers will not have to use so many resources in attempts to attract users' attention.

Likewise, consumers can also support the marketers' values by increasing the accuracy and volume of information marketers can collect. When consumers explicitly allow collection of their personal information they are more likely to be forthright about their preferences. Under the current model, web users who are concerned about the many ways in which information can be surreptitiously collected elect to take countermeasures to avoid this profiling.¹⁸¹ For instance, users may give fictitious names or email addresses when registering for various websites.¹⁸² The misinformation can lower the effectiveness of marketer's advertising by introducing inaccuracies into their user profiles. Even if users did not actively try to confuse their observers, simple observations still have their limit. If a consumer buys a book online, the profiler would not know immediately if that book represents an interest of that person, a one-time gift or even a mistaken purchase. A profiler could finally make that determination by collecting even more information and plugging the data into algorithms that look for patterns in the user's habits.

A profiler's advertising decisions would be much more effective if it received users' cooperation. Once a user has agreed to certain types of data collection, she could help supply some of that data. Consumers would be much more willing to assist in the process if they are aware of the type of information being collected and the

COMMERCIAL WEB SITES, <http://www.hostway.com/media/survey/petpeeves.html>.

179. By 2004, all major web browsers included programs that allowed users to block pop-up advertisements. Wikipedia, POP-UP AD, http://en.wikipedia.org/wiki/Pop-up_ad.

180. *Id.* Many different spyware programs and advertising supported software will cause advertisements to pop-up outside of the web browser. Also, some forms of instant messaging will allow pop-up advertisements to come up on a user's computer. http://en.wikipedia.org/wiki/Pop-up_ad.

181. See Litman *supra* note 20, at 1285-6 (listing measures users take to avoid profilers).

182. *Id.*

restrictions on the use of that data. Further, as users become more aware of the benefits of targeted advertising, they may even encourage the practice in certain situations. Overall, profiles would be much more accurate when users are given a chance to interact with a profiler without fear.

Another benefit of an automated negotiation is the elimination of user distrust found in the current market. As noted above, economists have observed that economies with higher levels of trust operate more efficiently.¹⁸³ The automated system will help enhance trust in the electronic market: consumers will know exactly what information is being collected and how it will be used and be able to put limits on that use. Also, because users will be able to enforce their agreements through the courts, the public does not need to fear widespread violations of the agreements. A majority of Internet users claim they restrict the amount of business they conduct online due to concerns for their privacy.¹⁸⁴ Hence, an increase in trust should help increase electronic commerce overall. This increase in online business will benefit all websites as they receive more traffic and more consumers are willing to do business. The increased use of the web will also help take advantage of the efficiencies the web provides for the economy as a whole.

B. Website Specific Benefits

Organizations will be able to increase the amount they invest in their online business because legislation instituting the automated system will reduce legal uncertainty. For the past several years, each Congressional session has been greeted with several hundred Internet privacy related bill proposals.¹⁸⁵ Although none of these bills have passed yet, uncertainty about future legislation has certainly hampered online marketing. It is a risky venture to invest too heavily in Internet advertising when the legal landscape is so unclear.

Additionally, since the advent of the web there has been continual litigation concerning privacy online.¹⁸⁶ These suits have been

183. See discussion *supra* Part II.B.3.

184. See, e.g., Turow, *supra* note 11.

185. See, e.g., Internet Privacy Bills, *supra* note 121.

186. See, e.g., *In re Pharmatrak Privacy Litig.*, 329 F.3d 9 (1st Cir. 2003) (finding that users did not consent to having personal information collected by a company that tracked internet traffic); *In re Doubleclick Privacy Litig.*, 154 F. Supp. 2d 497 (S.D.N.Y. 2001) (granting defendant's motion to dismiss for failure to state a claim when web users claimed their personal information had been stolen); *In re Toys R Us, Inc., Privacy Litig.*, MDL No. M-00-1381 MMC, 2001 U.S. Dist. LEXIS 16947 (N.D. Cal 2001) (denying defendants' motion to dismiss claims regarding their surreptitious data mining).

brought against websites, ISPs and marketers.¹⁸⁷ Although most cases have been found in favor of the websites, the risk of future lawsuits still exist. The risk is amplified because there have not been coherent common law rules in effect to help guide future behavior.

Any type of privacy legislation has the potential to help cure this uncertainty, however. Once a standard set of rules is put in place, businesses will be able to predict their future legal positions more accurately. This clarity will help encourage future investment in online businesses.

The automated transaction has a benefit over many other proposed solutions because it is more politically feasible. Most online privacy proposals that attempt to limit information gathering have met with opposition from industry groups. Many of the proposals also face heavy criticism from privacy advocates asking for even more protection.¹⁸⁸ The advocates feel that once legislation is put in place, the government will essentially be implicitly condoning all behaviors that are not expressly restricted by the law. The rapid development of the technology on the Internet further increases privacy advocates concerns because most proposed legislation will only address the current methods of data collection. As a consequence of the heavy lobbying from both sides of the debate, the government has been at a virtual standstill on the issue and the FTC has only been able to recommend self-regulation among marketers.¹⁸⁹

The automated system is not likely to meet the same level of opposition, however. The proposal does not attempt to impose blanket restrictions on harvesting or profiling behavior. Although marketers will be restricted in some of their activities, they are not as likely to oppose an automated system as adamantly because it will allow many of the same types of profiling to exist. In fact, many marketers may welcome the proposal because it gives users an

187. See cited cases, *supra* note 186.

188. See, e.g., *FCC's Privacy Petition*, Red Herring, Aug. 30, 2005, <http://www.redherring.com/Article.aspx?a=13382&hed=FCC%2%80%99s+Privacy+Petition>. ("The Electronic Privacy Information Center (EPIC), . . . filed a petition with the FCC demanding more stringent requirements for telecommunications companies releasing personal information about their customers."); Letter from EPIC to Florida Committee on Privacy and Court Records (Nov. 1, 2004) (recommending Florida increase security for personal information by regulating commercial data brokers) *available at* <http://www.epic.org/privacy/publicrecords/flcomments.pdf>; Letter from Ari Schwartz, Associate Director, Center for Democracy and Technology, to Data Privacy and Integrity Committee, Department of Homeland Security (July 18, 2005) *available at* <http://www.cdt.org/testimony/20050718schwartz.pdf>.

189. 2000 FTC REPORT, *supra* note 35.

opportunity to supply more information. Additionally, even marketers have acknowledged that improved security will help augment web traffic.¹⁹⁰ Because the system will encourage more people to business online, many marketers should support the system.

The information-for-privacy exchange may also address many of the concerns from privacy supporters. The system will not expressly allow or forbid any type of behavior. Therefore, the government will not be implicitly supporting any particular conduct. Additionally, because the system is flexible it can also be adaptive. If new data collecting technology emerges or new techniques become popular, the parties can simply readjust their browsers' settings. For the most part, the automated system is much more politically feasible than any hard rule governing privacy.

C. Advantages for the Government

Finally, an automated system will allow legislators to overcome the difficult task of protecting personal information without ever being forced to find a clear definition of privacy. Paradoxically, uncertainty has escalated recently in the very areas in which the government has already attempted privacy legislation – financial and medical information. Many critics believe The Gramm-Leach-Bliley Act ("GLB"),¹⁹¹ which addresses financial privacy, and the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"),¹⁹² which addresses medical privacy, have created more uncertainty than they have eliminated.¹⁹³ Both laws attempt to create a federal "privacy floor" for the use of sensitive information.¹⁹⁴ However, it is difficult to

190. 1998 FTC REPORT, *supra* note 4.

191. Gramm-Leach-Bliley Act, Pub. L. No. 106-102, 501, 113 Stat. 1338, 1436-37 (1999) (requiring financial institutions to secure personal information).

192. Health Insurance Portability and Accountability Act, Pub. L. 104-191, 264, 110 Stat. 1936 (1996) (codified as amended at 42 U.S.C. §1320d-2) (requiring medical institutions to secure certain personal medical information).

193. See, e.g., Jeffery B. Ritter, Benjamin S. Hayes & Henry L. Juoy, *Emerging Trends in International Privacy Law*, 15 EMORY INT'L L. REV. 87, 97-104 (2001) (discussing how American privacy legislation conflicts with other countries' laws); Edward E. Furash, *The GLB Conundrum*, 83 RMA J. 88 (2001) (noting that under GLB banks face "inappropriate expectations, confusion over who does what, and unclear costs"); Press Release, LifePoint Hospitals, Inc., LifePoint Hospitals Reports First Quarter Results and Announces Share Repurchase Program (Apr. 28, 2003) (listing uncertainty with HIPAA compliance as a risk factor for the companies financial statements.) available at <http://www.lifepointhospitals2.com/>.

194. Christopher C. Gallagher, *Health Information Privacy: The Federal Floor's State Elevator*, 2 Privacy & Info. L. Report 1 (2000), available at <http://www.gcglaw.com/resources/healthcare/healthprivacy.pdf>.

determine where the floor sits and what behaviors operate above the basic protections.¹⁹⁵

The GLB purports to increase privacy protection by requiring that financial institutions: (i) notify customers about their information practices, (ii) give the consumers an opportunity to opt-out of the practices and (iii) create methods for protecting the collected information.¹⁹⁶ Despite the enactment of the GLB, however, the possibility of additional federal legislation and proposed state financial laws has continued to make the legal terrain uncertain for financial institutions.¹⁹⁷ Both the federal and state governments continue to consider stricter guidelines for the use of financial information because it has not been clear what actions industry will need to take to comply with the new laws.¹⁹⁸ The federal government has also been investigating ways to ensure that the GLB will be compatible with the EU Directive.¹⁹⁹ To further complicate matters, the Act does not preempt state action, so industries must be wary of possible state laws on the topic.²⁰⁰

Methods of compliance with HIPAA have also created uncertainty for businesses operating within the medical industry.²⁰¹ Like the GLB, HIPAA is meant to help set a federal "privacy floor," over which financial and medical organizations must act. Unfortunately, the attempt to quantify privacy with that floor has led to difficult and often contradictory regulations.²⁰² Some of the difficulty originates from the establishment of the floor itself.²⁰³

195. *Id.* ("the promised stability of the proliferating 'federal floor' doctrine is becoming a policy nightmare more likely to result in consumer confusion than consumer protection.").

196. Richard Lauter, *Privacy Concerns and Safeguards in the Governmental Dissemination of Bankruptcy Data on the Internet*, 19-4 ABIJ 10 (2000) ("The new regulations would (1) limit the non-consensual use and release of private health information; (2) inform consumers about their right to access their records and to know who else has accessed them; (3) restrict the disclosure of protected health information to the minimum necessary; (4) establish new disclosure requirements for researchers and others seeking access to health records; and (5) establish new criminal and civil sanctions for the improper use of disclosure of such information.").

197. Ritter, *supra* note 193, at 106 ("despite the enactment of GLB, delayed implementation of its regulations, proposed additional federal legislation, and a proliferation of state legislation have created great uncertainty for financial institutions in choosing a path forward.")

198. *Id.*

199. *Id.* at 106-7.

200. *Id.* at 107-8.

201. *See* Hurt, *supra* note 122.

202. Gallagher, *supra* note 194.

203. *Id.*

Unlike the GLB, HIPAA does preempt state laws unless the state laws offer more strict privacy protections.²⁰⁴ Determining which laws are on point and which offer more security, however, becomes a very subjective undertaking.²⁰⁵ Medical organizations are left unsure whether they must comply with state or federal privacy laws.²⁰⁶ Additionally, most state privacy laws try to strike a balance between the need for information and personal security.²⁰⁷ HIPAA's limited preemption only leaves the strictest federal and state laws resulting in an imbalance between privacy and data compilation that overly restricts information flows.²⁰⁸

The reason for the uncertainty under both the GLB and HIPAA can be traced back to the premise underlying both attempts to quantify privacy. Because privacy is so ill defined, the parties involved cannot be sure what they must do to comply with the laws. Both laws endeavor to create a definite minimum level of security without ever deciding upon the exact contours of privacy in their respective contexts.

The benefit of an automated transactional system, then, is that it does not require the government to decide what constitutes private information. The system will lower transaction costs and bring the online privacy environment closer to Coase's ideal world. As such, the negotiations between consumers and electronic businesses will eventually arrive at an optimal allocation of privacy.²⁰⁹ The government can allow markets to operate unobstructed to determine the value of privacy for each consumer, rather than force a clunky, one-size-fits-all definition on all members of the online community.

Additionally, by creating a private cause of action, the government can ensure ample security for users. After users decide individually how much restriction they would like to place on the use of their information, they can feel comfortable that their wishes will be respected. Despite the lack of a federal floor, users will still be protected.

204. *Id.*

205. *Id.*

206. *Id.*

207. Gallagher, *supra* note 194.

208. *Id.*

209. COOTER & ULEN, *supra* note 136, at 100.

D. Commodifying Privacy

Many privacy scholars may still object to the automated system, nevertheless, because privacy is the type of good where consumers do not know the benefits until they are lost. Professor Anita Allen argues that the development of markets for privacy has led to an erosion of privacy-related tastes and expectations.²¹⁰ There has been evidence in recent decades that people's expectations of privacy are dwindling.²¹¹ Professor Allen attributes this attrition, at least in part, to the many opportunities to both sell and consume private information.²¹² People are able to sell their privacy for money and celebrity through such venues as television reality shows and tabloids.²¹³ Conversely, consumers can buy other people's private information in newspapers and magazines and through the Internet.²¹⁴ The wearing down of a taste for privacy can be damaging both because of the moral implications and the loss of other benefits privacy provides.²¹⁵

If these presumptions are true, then an automated exchange of information online will speed up the diminution of the taste for privacy. As people become accustomed to trading away their private information for data, their expectation for privacy will decrease. The eventual result will inevitably be a loss of any expectation of privacy online.

Professor Ian Ayers and Matthew Funk point out, however, that whether commodification diminishes people's taste to secure their private information depends on the status quo that the market replaces.²¹⁶ When an item is given extremely high significance, encouraging commodification could lead to a loss of value. In the current system, however, marketers are allowed to invade consumers' privacy at no cost.²¹⁷ Marketers do not need consent before they monitor users' activities online. In fact, users often do not even know

210. Anita L. Allen, *Coercing Privacy*, 40 WM. & MARY L. REV. 723, 729-735 (1999).

211. *Id.*

212. *Id.*

213. *Id.*

214. *Id.*

215. Allen, *supra* note 210, at 737-41

216. Ian Ayres & Matthew Funk, *Marketing Privacy*, 20 YALE J. ON REG. 77 at 130-32 (2003).

217. *Id.* at 79, 83-87 ("Telemarketers don't bear the full costs of their marketing because they do not compensate recipients for the hassle of, say, being interrupted during dinner. Telemarketers bear the cost of their speaking, but not of residents' listening").

the observation is taking place.²¹⁸ The creation of a market would increase the importance the community places on private information. The regime would change from one where privacy is worth nothing to one where people could receive added safety measures for their data.²¹⁹ Additionally, the level of monitoring will decrease, as some people who currently receive no protection will receive some or even complete security.

Creating an automated exchange will also allow users to experiment with the importance they place on their privacy. A user could originally set their browser to allow complete disclosure. If this setting turns out to reveal too much information and the user suffers undesirable consequences, she could simply adjust the setting to allow more protection. The automated system will thus give an opportunity to test Professor Allen's conclusions.

V. Conclusion

This article has developed the concept for a technological solution to the problem of online privacy. Technology can be used to encourage an information exchange between users and websites. Because the technology can serve to reduce transaction costs, the two parties will come to the optimal allocation of privacy online.

This solution assumes a different perspective on the traditional debate. While most proposals endeavor to come to a consensus upon either a common definition or a common value system for privacy, an automated transaction simply makes optimal use of the online market the ultimate goal. Because the Internet is efficiency enhancing, encouraging optimal utilization will help increase the effectiveness for the overall market. Rather than define privacy, the government should instead encourage trust, which will result in the maximum benefits for the economy as a whole. Maybe R2-D2 is not so bad after all.

218. 1998 FTC REPORT, *supra* note 4.

219. See Ayres & Funk, *supra* note 216, at 130-32.

* * *