NOTE

LEGISLATION FOR EFFECTIVE SELF-REGULATION: A NEW APPROACH TO PROTECTING PERSONAL PRIVACY ON THE INTERNET

Richard M. Marsh, Jr.[*]

Cite as: Richard M. Marsh, Jr., *Legislation for Effective Self-Regulation: A New Approach to Protecting Personal Privacy on the Internet*, 15 MICH. TELECOMM. TECH. L. REV. 543 (2009), *available at* http://www.mttlr.org/volfifteen/marsh.pdf

INTRODUCTION

How can we best reap the benefits of online profiling while avoiding the privacy pitfalls plaguing the e-commerce community? Experts advocate legislation,[1] civil litigation,[2] or self-regulation[3] to provide the ideal

* J.D., May 2009, The University of Michigan Law School.

1. *See, e.g.*, Andrew Hotaling, *Protecting Personally Identifiable Information on the Internet: Notice and Consent in the Age of Behavioral Targeting*, 16 COMMLAW CONSPECTUS 529 (2008); Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 STAN. L. REV. 1193 (1998). The European Union has enacted its own legislative regime to deal with this issue. *See* Council Directive 95/46, 1995 O.J. (L 281) 31 (EC).

2. *See, e.g.*, Jessica Litman, *Information Privacy/Information Property*, 52 STAN. L. REV. 1283 (2000); Patricia Mell, *Seeking Shade in a Land of Perpetual Sunlight: Privacy as Property in the Electronic Wilderness*, 11 BERKELEY TECH. L.J. 1 (1996); Richard S. Murphy, *Property Rights in Personal Information: An Economic Defense of Privacy*, 84 GEO. L.J. 2381 (1996).

3. *See, e.g.*, LYDIA PARNES, FEDERAL TRADE COMMISSION, PREPARED STATEMENT OF THE FEDERAL TRADE COMMISSION ON BEHAVIORAL ADVERTISING BEFORE THE SENATE COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION (2008), *available at* http://www.ftc.gov/os/2008/07/P085400behavioralad.pdf [hereinafter FTC STATEMENT ON BEHAVIORAL ADVERTISING].

solution. Analyzing these proposals reveals a conflict between two basic principles: the need to preserve personal privacy and the desire to foster a thriving Internet-based industry. This Note argues that each approach tends to favor one principle at the expense of the other. This Note also proposes a new solution which creates incentives for effective self-regulation backed with legal enforcement. This scheme strikes an appropriate balance between privacy and e-commerce principles and brings a flexible standard to address future innovation.

Tracking a user's Internet activity seems intrusive because companies can exploit intimate information. For example, Sir Tim Berners-Lee, inventor of the World Wide Web, worries that searching for books on cancer could result in increased health insurance premiums because companies can track consumers' online activity and then sell this information to the insurance industry.[4] This apprehension will only increase as technology enables greater data collection and more accurate profiling. For instance, breakthroughs in deep packet inspection have opened the door to surveillance by Internet Service Providers (ISPs), which can now track everything a user does online. Advanced processing power then swiftly sorts this data into individually tailored profiles to be used or sold at the ISP's will.

At the same time, online profiling brings users considerable prosperity. Credit reporting is cited as one of the best benefits of information sharing,[5] saving consumers "as much as $80 billion a year on mortgage loans because of the liquidity that credit bureau information makes possible."[6] Online profiling also creates more advertising opportunities which then fund much of the content users currently access for free.[7]

The dilemma posed by online profiling is further discussed in Part I of this Note, which concludes that the optimal solution to the profiling problem must prevent privacy harms without smothering e-commerce. Part II then evaluates solutions which create a private cause of action and determines that using civil litigation to balance these interests is less than ideal. Part III examines existing self-regulatory efforts and legislative options. While self-regulation and legislation offer important advantages, each solution, by itself, suffers from considerable defects that render a

4. Rory Cellan-Jones, *Web Creator Rejects Net Tracking*, BBC NEWS, Mar. 17, 2008, http://news.bbc.co.uk/1/hi/technology/7299875.stm.

5. Robert W. Hahn & Anne Layne-Farrar, *The Benefits and Costs of Online Privacy Legislation*, 54 ADMIN. L. REV. 85, 106 (2002).

6. Fred H. Cate & Michael E. Staten, *Putting People First: Consumer Benefits of Information-Sharing* (2000), http://www.privacyalliance.org/resources/consumerbenies.pdf (emphasis omitted) (last visited June 28, 2009) (on file with author).

7. *See* FEDERAL TRADE COMMISSION, ONLINE BEHAVIORAL ADVERTISING MOVING THE DISCUSSION FORWARD TO POSSIBLE SELF-REGULATORY PRINCIPLES (2007), http://www.ftc.gov/os/2007/12/P859900stmt.pdf.

single policy tool unlikely to satisfactorily resolve the profiling dilemma. Meanwhile, a frenzy of political action over ISP surveillance suggests that privacy problems are pressing enough to create broad support for legislation. Part IV proposes a solution to the profiling problem—a modified legislative approach which incorporates aspects of self-regulation. It then argues that this solution is ideal because it capitalizes on existing political momentum to create flexible and functioning standards that will increase personal privacy and nurture e-commerce.

I. CURRENT PRACTICES AND POLICIES

The Internet currently reaches 72.5 percent of the U.S. population.[8] One poll indicates that, "[a]mong those who use the Internet daily, more than 80 percent use it several times a day and nearly half use it constantly."[9] For many, the Internet opens new channels of communication and allows people to become more deeply connected with those around them.

A. *Profiling Perils*

While the Internet allows for new means of communication, this flow of information does not travel in isolation. Invisible to most users, companies use an array of sophisticated software to siphon bits of information from a user's data stream. Search engines, for example, account for an enormous proportion of web site visits, and most search engines keep track of users' search queries.[10] Other companies monitor when users visit certain web sites and what content they access. The data are then used to deliver specific ads to targeted individuals. This practice, known as "behavioral advertising,"[11] has become so profitable that Google, Yahoo, Microsoft, and AOL all recently acquired behavioral advertising firms to increase their profit margins.[12] Notwithstanding the rosy picture painted by these financial successes, online profiling raises

8. Internet World Stats, *Usage and Population Statistics*, http://www.internetworldstats.com/ am/us.htm (last visited Mar. 23, 2009).

9. Andrew D. Smith, *Most U.S. Workers Use Net on Job*, MIAMI HERALD, Oct. 20, 2008, http://www.miamiherald.com/business/story/731057.html.

10. *See* Markham C. Erickson & Kevin Bankston, *Should Web Search Data Be Stored?*, WALL ST. J. ONLINE, Aug. 15, 2006, http://online.wsj.com/public/article/SB115530662685133335-OJwdGqVy4BFV8l10 JmjhOxqaoHc_ 20060913.html.

11. *See* FEDERAL TRADE COMMISSION, *supra* note 7.

12. Hotaling, *supra* note 1, at 539–40 (citing Saul Hansell, *Which Advertiser Is on Your Friend List?*, N. Y. TIMES, Nov. 2, 2007, http://bits.blogs.nytimes.com/2007/11/02/which-advertiser-is-on-your-friend-list).

concerns because serious harms can happen as these practices become more invasive and the data collected becomes more personal in nature.

Cookies,[13] for example, are commonplace today because they can "remember" log-in information, personal preferences, and can be used for security purposes.[14] But cookies are capable of much more: they can store, and later transmit, personally identifiable[15] or sensitive information.[16] This data could include an individual's name, credit card number, health condition, social security number, or lifestyle preference.[17]

Even if non-personally identifiable information is collected, a company could match this data (for example, web page visits to research sexually transmitted diseases) with personally identifiable information obtained elsewhere (a name, address, or phone number) and sell everything as a package to third parties.[18] When all the data are assembled and analyzed by powerful computers, each profile can match a user's interests and personality in frighteningly accurate terms. Meanwhile, the average user is unaware of what data is collected or how that data will be used. Cookies are, by design choice and not by coding constraints, largely invisible to consumers and encrypted to be unintelligible to any user wanting to know what the cookies are saying about him or her.

Other monitoring methods, such as "web bugs,"[19] spyware,[20] and email content extraction[21] are capable of gathering more information and

---

13. Cookies are small text files placed on a user's hard drive by websites. *See* HowStuffWorks, *What Is an Internet Cookie?*, http://www.howstuffworks.com/question82.htm (last visited Mar. 19, 2009).

14. *See* Reid Goldsborough, *The Benefits and Fears of Cookie Technology*, NFIB, Jan. 10, 2005, http://www.nfib.com/object/IO_19680.html.

15. Personally identifiable information refers to data capable of identifying an individual, such as a name, address, or social security number. Non-personally identifiable information does not refer to any specific individual.

16. *See* Goldsborough, *supra* note 14.

17. Frederic Debusseré, *The EU E-Privacy Directive: A Monstrous Attempt to Starve the Cookie Monster?*, 13 INT'L J.L. & INFO. TECH. 70, 77 (2005).

18. Svetlana Milina, *Let the Market Do Its Job: Advocating an Integrated Laissez-Faire Approach to Online Profiling Regulation*, 21 CARDOZO ARTS & ENT. L.J. 257, 264 (2003).

19. Web bugs are small pictures, usually one pixel in height by one pixel in length—the smallest image physically possible. They are designed to be the same color as the background on which they are placed which renders them essentially invisible. JODIE BERNSTEIN, FEDERAL TRADE COMMISSION, ONLINE PROFILING: BENEFITS AND CONCERNS n.27 (2000), http://www.ftc.gov/os/2000/06/onlineprofile.htm.

20. What Is Spyware or Adware, and How Can I Remove It?, University Information Technology Services, Indiana University (Oct. 21, 2008), http://kb.iu.edu/data/anfs.html ("Spyware is Internet jargon for any data collection program that secretly gathers information about you and relays it to advertisers and other interested parties.").

21. *See* Electronic Privacy Information Center, Gmail Privacy FAQ, http://epic.org/privacy/gmail/faq.html (last visited Nov. 18, 2008) (detailing Google's content extraction policy).

are harder to detect than cookies.[22] In addition, several ISPs have contemplated tracking user activity using deep packet inspection,[23] which allows ISPs to sift through email contents, web page visits, VOIP conversations, or anything else users do online.[24] These encroachments seem even more dangerous because ISPs already have users' billing information in their database and could easily combine the data.[25]

Information gathering techniques have even moved to cell phones. The Smartphone, for example, can note every email, text message, or song a user enjoys.[26] Soon, companies may track and record a user's physical location[27] and share all this information over a network of affiliated profiling firms.[28] With the current pace of technology, sophisticated and powerful data gathering tools will likely become even more stealthy and profitable.

Besides being creepy, these practices bring harmful consequences. When creating personal profiles, companies often use advanced algorithms to mine user information. These algorithms create inferences about a user's personality, which are largely based on existing stereotypes.[29] Behavioral advertising then reinforces those stereotypes by altering consumer behavior through marketing efforts.[30] Besides the ethical problems raised by reinforcing stereotypes, these practices may violate personal privacy and compromise personal autonomy because the consumer has no idea how she has been categorized and may be "induced to act in ways she would not have chosen if she knew about her profile."[31]

---

22. *See* Jordan M. Blanke, *"Robust Notice" and "Informed Consent:" The Keys to Successful Spyware Legislation*, 7 COLUM. SCI. & TECH. L. REV. 2 (2006).

23. *See* Saul Hansell, *The Mother of All Privacy Battles*, N.Y. TIMES, Mar. 20, 2008, http://bits.blogs.nytimes.com/2008/03/20/the-mother-of-all-privacy-battles/.

24. *See* Electronic Privacy Information Center, Deep Packet Inspection and Privacy, http://epic.org/privacy/dpi/ (last visited Nov. 18, 2008).

25. FTC STATEMENT ON BEHAVIORAL ADVERTISING, *supra* note 3, at 13 n.27.

26. John Markoff, *You're Leaving a Digital Trail. What About Privacy?*, N. Y. TIMES, Nov. 29, 2008, at BU1, *available at* http://www.nytimes.com/2008/11/30/business/30privacy.html (reporting a Smartphone marketing scheme where students exchange personal information collected via the Smartphone for free phone services).

27. *See id.*

28. *See* FTC STATEMENT ON BEHAVIORAL ADVERTISING, *supra* note 3, at 2.

29. Nancy J. King, *When Mobile Phones Are RFID-Equipped—Finding E.U.-U.S. Solutions to Protect Consumer Privacy and Facilitate Mobile Commerce*, 15 MICH. TELECOMM. TECH. L. REV. 107, 145 (2008) (citing Mireille Hildebrandt, *Profiling into the Future: An Assessment of Profiling Technologies in the Context of Ambient Intelligence*, 1 FIDIS J. OF IDENTITY IN THE INFO. SOC'Y 7 (2007)).

30. *Id.* at 135.

31. *Id.* at 146 (citing Mireille Hildebrandt, *Profiling into the Future: An Assessment of Profiling Technologies in the Context of Ambient Intelligence*, 1 FIDIS J. OF IDENTITY IN THE INFO. SOC'Y 7, 9 (2007)).

In addition, if there is a security breach or a user's profile is mishandled, her data may become publicly available—a problem which is even graver if her profile contains sensitive information. Trusting corporate security may not be the wisest idea. Companies currently battle against increasingly complex security threats as identity thieves develop sophisticated tactics for obtaining private data.[32] Acxiom, one of the largest database companies, provides a particularly alarming example. In 2004, Scott Levine stole 8.2 gigabytes of information from Acxiom.[33] The stolen data included names, home addresses, bank accounts, and credit card information.[34]

Some companies argue that they protect customers' privacy by collecting only non-personally identifiable information and by making all data anonymous. However, experience shows that this may not be as safe as advertised. In 2006, AOL released thousands of anonymous profiles. From this data, the New York Times was able to identify a specific person, Thelma Arnold, a 62-year-old woman living in Georgia.[35]

Perhaps the real harm is loss of consumer control. One scholar noted that "[t]he more cognizable and immediate problem with a loss of information privacy . . . is our inability to avoid circumstances in which others control information that can affect us in material ways."[36] Advancing technology makes it "virtually impossible for a user to keep track of all of the ways that they can be monitored while surfing the web."[37] At the same time, data collection practices are so pervasive that "there is almost no way for a user to prevent the collection of their personal information."[38] Indeed, Scott McNealy's cold counsel to consumers, "You have zero privacy anyway. Get over it,"[39] has never been truer.

---

32. Karim Z. Oussayef, Note, *Selective Privacy: Facilitating Market-Based Solutions to Data Breaches by Standardizing Internet Privacy Policies*, 14 B.U. J. SCI. & TECH. L. 104, 116 (2008).

33. Declan McCullagh, *Data Thief Gets Eight Years*, ZDNET, Feb. 23, 2006, http://news.zdnet.com/2100-1009_22-146938.html.

34. *Verdict Awaited in Hacking Trial*, AGE, Aug. 11, 2005, http://www.theage.com.au/news/breaking/verdict-awaited-in-hacking-trial/2005/08/11/1123353411040.html.

35. Kelly Martin, *AOL Search Data Identified Individuals*, SECURITY FOCUS, Aug. 9, 2008, http://www.securityfocus.com/brief/277.

36. James P. Nehf, *Recognizing the Societal Value in Information Privacy*, 78 WASH. L. REV. 1, 26 (2003).

37. David Goldman, *I Always Feel Like Someone Is Watching Me: A Technological Solution for Online Privacy*, 28 HASTINGS COMM. & ENT. L.J. 353, 355 (2006).

38. *Id.*

39. Polly Sprenger, *Sun on Privacy: Get over It*, WIRED NEWS, Jan. 26, 1999, http://www.wired.com/news/politics/0,1283,17538,00.html.

B. . . . *and Profits*

Even though online profiling threatens personal privacy, it also enables many of the opportunities the Internet now offers. Advertising is one of the principle vehicles for e-commerce,[40] with revenues of over $21 billion in 2007.[41] Behavioral advertising is simply more effective than contextual advertising,[42] and funds many of the websites used today. The FTC observed that:

> [B]ehavioral advertising may help subsidize and support a diverse range of free online content and services that otherwise might not be available or that consumers would otherwise have to pay for—content and services such as blogging, search engines, social networking, and instant access to newspapers and information from around the world.[43]

Targeted ads can also be more enjoyable to the average user, which may "facilitate shopping for the specific products that consumers want."[44] Amazon.com, for example, presents a user with a selection of recommended items based on that user's prior purchases and searches.[45] Using behavioral advertising has helped make Amazon.com a big success[46] and Amazon.com recently received a patent on its profiling system.[47] Other perks of online profiling include customized content, such as personal web pages, local news and weather, or favorite stock quotes.[48]

Online profiling can also lower costs by "reducing the risks of accepting checks and other non-cash payments"[49] and offers "the unprecedented ability to examine consumer behavior in order to minimize marketing and distribution costs."[50] Simply put, companies can use

---

40. FTC STATEMENT ON BEHAVIORAL ADVERTISING, *supra* note 3, at 4.

41. PRICEWATERHOUSECOOPERS, IAB INTERNET ADVERTISING REVENUE REPORT (2008), http://www.iab.net/media/file/IAB_PwC_2007_full_year.pdf.

42. Helen Leggatt, *Behavioral Advertising Attracts More Consumer Attention*, BIZREPORT, Sept. 13, 2007, http://www.bizreport.com/2007/09/behavioral_advertising_attracts_more_consumer_attention.html.

43. FTC STATEMENT ON BEHAVIORAL ADVERTISING, *supra* note 3, at 4.

44. *Id.* at 3.

45. *See* Amazon.com, *Amazon.com Privacy Notice*, http://www.amazon.com/gp/help/customer/display.html/188-0513236-0619248?ie=UTF8&nodeId=468496 (last visited May 13, 2009).

46. Bob Tedeschi, *Gifts.com Doesn't Know Your Aunt Sally. But the Company Is Betting its Search Engine Can Recommend a Nice Present for Her*, N.Y. TIMES, Mar. 21, 2009, at C1 ("Since Amazon.com is the most popular retail site for gift shoppers—having garnered nearly 14 percent of all online sales in the fourth quarter of 2004. . .").

47. *Id.*

48. Milina, *supra* note 18, at 264.

49. Cate & Staten, *supra* note 6.

50. Milina, *supra* note 18, at 261.

online profiling to offer products that are better and more accurately tailored to consumer demands.[51] Armed with these advantages, a company "can increase its profit margins while passing valuable savings along to consumers."[52] Targeted advertising also encourages new competitors, manifested by a "number of new businesses [that] have sprung up in recent years premised on providing new goods and services to consumers in exchange for, or in reliance on, information about them."[53]

There are also indirect benefits for consumers. Fred Cate and Michael Staten, academic scholars specializing in privacy law and market economics, respectively, point out that profiling prevents fraud and creates an efficient credit market.[54] Specifically, they note that:

> In 1997, 82 percent of automobile loan applicants received a decision within an hour; 48 percent of applicants received a decision within 30 minutes. In most instances, these decisions can be made no matter where in the United States the consumer lives or the request is initiated. Many retailers open new charge accounts for customers at the point of sale in less than two minutes. . . .[55]

Thus, Internet users are pulled by opposing concerns. On the one hand, exciting and profitable endeavors are funded through behavioral advertising. On the other hand, large amounts of potentially sensitive information are vacuumed up and sold in the open market. Unfortunately, users may not have the ability to decide which behavioral advertising methods are acceptable and which are not. Because the benefits and burdens of online profiling are so significant and widespread, this conflict calls for an overarching plan to increase privacy on the Internet while maintaining an environment conducive to e-commerce.

II. Private Solutions

To resolve this dilemma, some scholars argue that privacy should be enforced through civil litigation by creating a property right in personal data[56] or by using tort law to remedy harms from exploited information.[57] These proposals offer flexibility by implementing standards on a case by

---

51. *Id.*
52. *Id.* at 262.
53. Kent Walker, *Where Everybody Knows Your Name: A Pragmatic Look at the Costs of Privacy and the Benefits of Information Exchange*, 2000 Stan. Tech. L. Rev. 2, 9 (2000).
54. Cate & Staten, *supra* note 6.
55. *Id.* (citing Consumer Bankers Association, *1998 Automobile Finance Study*, at 19).
56. *E.g.*, Mell, *supra* note 2; Murphy, *supra* note 2.
57. *E.g.*, Litman, *supra* note 2.

case basis. In addition, judicial interpretation could create these rights instead of legislative action—arguably avoiding "the interference of interest groups, lobbyists, and re-election campaigns."[58] Creating a private right may force those who want the data to bargain for it and provide clear disclosure to users.

However, several characteristics of civil litigation make this option less than ideal. As an initial matter, allowing people to negotiate away private rights in personal data may legitimatize data collection practices—an outrageous result for those "who consider information privacy to be a fundamental civil right."[59] Even if this objection is overcome or ignored, there are several other factors which cast doubt on the efficacy of a private solution.

First, civil litigation proceeds one case at a time. Deciding conflicts on a case by case basis may simply be too slow. Individual cases can take several years to resolve, especially since appellate courts will probably chime in when expanding the law. This timeframe is out of sync with the rate of technological developments. By the time courts limit deep packet inspection, for example, other monitoring methods, such as the Smartphone, will have stepped into the vacancy. Class action lawsuits could hasten the process, but judges may be reluctant to certify classes with privacy injuries because of the "individual nature of the harm and damages."[60]

Second, each case will be decided within a specific context and, due to the complex nature of interactions on the web, many cases may have to be decided before developing broad protections. Some scholars, in fact, doubt effective protection could ever result through this process,[61] and believe that "litigation should not be the primary enforcement mechanism for citizens who can rarely afford to sue . . . a large commercial enterprise."[62]

Third, implementing standards on a case by case basis will probably result in rights that vary in scope across jurisdictions. This is incompatible with a national (if not global) Internet community. While it is possible for judges in different states to come to a general consensus, the

---

58. 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, 115 (2002). However, elected judges may still be subject to many of the same political influences.

59. Pamela Samuelson, *Privacy as Intellectual Property?*, 52 STAN. L. REV. 1125, 1142 (2000).

60. Seth Safier, *Between Big Brother and the Bottom Line: Privacy in Cyberspace*, 5 VA. J.L. & TECH. 6, ¶ 108 (2000).

61. *See* Nehf, *supra* note 36, at 58-66.

62. *Id.* at 68 (citing David H. Flaherty, *Controlling Surveillance: Can Privacy Protection Be Made Effective?*, *in* TECHNOLOGY AND PRIVACY: THE NEW LANDSCAPE 167, 174 (Philip E. Agre & Marc Rotenberg eds., MIT Press 1998)).

more probable scenario is that small but significant differences will exist. This forces firms to adopt the policy of the most protective region. In theory, there is nothing wrong with this approach—the strictest policy might be the best one. But it is more likely that the most protective policy will be less than ideal because, generally, the more strict the policy, the greater the dampening effects on e-commerce.[63] While privacy concerns may justify some limitations on e-commerce, the "race to the bottom" described above would effectively ignore e-commerce concerns. In the end, omitting one side of the debate is unlikely to produce an ideal solution.

Fourth, forcing companies to individually negotiate with each visitor to their website, as a means to avoid later litigation, may be too costly.[64] Profiling works best with aggregation, and requiring each company to develop the infrastructure to navigate through billions of negotiations and honor billions of individual requests would be, as one scholar observed, a "bookkeeping nightmare."[65] Thus, a private cause of action would add significant transaction costs to a system designed to function without them.[66] Granting a private cause of action would compel companies to bear the brunt of a complete system overhaul and would likely reduce the existing menu of consumer benefits.

Overall, protecting privacy through civil litigation is an attractive idea, but might be less effective than legislative and regulatory solutions in protecting personal privacy. In addition, expanding private rights may pose considerable threats to the economic benefits of online profiling. Therefore, on the whole, it seems that creating a private right of action would significantly impair the vibrant e-commerce industry without doing enough to protect personal privacy.

III. Self-Regulation and Legislative Solutions

Since expanding private rights seems unlikely to successfully balance privacy and e-commerce, a more public solution, such as self-regulation or legislation, may be appropriate. Unfortunately, the current form of self-regulation, as described below, does not appear to adequately protect privacy either. Yet self-regulation offers too many benefits to be completely discarded. Similarly, legislative solutions also

63. *See* Noel Cox, *The Relationship Between Law, Government, Business, and Technology*, 8 Duq. Bus. L.J. 31, 35 (2006).

64. Samuelson, *supra* note 59, at 1135.

65. Litman, *supra* note 2, at 1298.

66. *See* Samuelson, *supra* note 59, at 1137.

promise valuable advantages, but, despite broad support, may not be able to protect privacy without suffocating e-commerce.

A. *Self-Regulation*

For at least the last decade, industry self-regulation has operated as the main mechanism for protecting privacy on the Internet.[67] During this time, hundreds of profitable businesses rapidly grew by using new methods and technologies. These firms then created many of the benefits currently enjoyed today. This e-commerce explosion flourished because companies, both new and established, could efficiently implement innovations under the flexible principles provided by self-regulation.[68] Maintaining adaptable standards is important because even more breakthroughs appear to be on the horizon.

Self-regulation works by placing decision-making power on those closest to the technology and business methods. This protects future opportunities better than other approaches because those with actual experience are more likely to know what innovations are possible than judges or Congress. Empowering those closest to technology also creates standards which can respond more quickly to innovation because people with field experience generally have a better understanding of what has changed. Without an adaptable solution, regulations may have the unfortunate effect of restricting innovation or channeling research efforts into existing technology at the expense of presently unforeseen opportunities.[69]

While self-regulation seems well-equipped to preserve economic benefits and open doors to future innovation, the question remains as to whether it can sufficiently protect personal privacy. On one hand, companies seem to have a strong incentive to protect personal privacy. Even the implication that a business sells the personal data it collects from customers could tarnish its goodwill.[70] In fact, "business consulting firms now routinely encourage the adoption and promotion of privacy policies

---

67. *See* FTC STATEMENT ON BEHAVIORAL ADVERTISING, *supra* note 3, at 7–10.

68. *Id.* at 12–13 ("[S]elf-regulation . . . affords the flexibility that is needed as business models continue to evolve.").

69. *See* Milina, *supra* note 18, at 272–74; *see also* AUTOMOTIVE PANEL, NATIONAL RESEARCH COUNSEL, THE COMPETITIVE STATUS OF THE U.S. AUTO INDUSTRY: A STUDY OF THE INFLUENCES OF TECHNOLOGY IN DETERMINING INTERNATIONAL INDUSTRIAL COMPETITIVE ADVANTAGE 86 (Nat'l Acad. Press 1982) ("[T]ightening regulatory requirements forces companies to divert discretionary resources into programs to improve existing technologies, in effect entrenching the current technology within the industry.").

70. *See* James P. Nehf, *Shopping for Privacy Online: Consumer Decision-Making Strategies and the Emerging Market for Information Privacy*, 2005 U. ILL. J.L. TECH. & POL'Y 1, 10–11 (2005).

as a way to present a positive client image."[71] Others claim that self-regulation works because it has already resolved several privacy problems. For example, in 1999, IBM and others influenced many in the industry to publish privacy statements.[72] Since then, self-regulation caused several firms to change their behavioral advertising plans[73] and drove others out of the market after public outcries over privacy invasions.[74]

On the other hand, while companies clearly understand that success "depend[s] on their ability to allay consumer concerns about security and privacy,"[75] today's thriving market rewards companies who collect data while remaining invisible. This skewed incentive structure inspires firms to be less transparent and avoid consumer complaints by hiding their behavior, instead of actually taking measures to ensure adequate protection.

Privacy policies, for example, appear to manifest greater transparency but actually reveal very little. These policies are usually unintelligible, "[f]ull of 'electronic boilerplate,'" and "often includ[e] a clause that reserves the company the right to change its user data standards at any time."[76] Unless a person rereads the policy with each visit, he or she will never know what information that company records.[77] These policies also fail to disclose how data will be used, making it impossible for users to object to bad practices. Without knowing how data is collected and sold, poor practices are difficult, if not impossible, to prohibit.[78]

Even if self-regulation brings greater transparency, relief often comes only after public outcry. James Nehf, an internationally recognized expert in consumer privacy law, observed that "[r]equiring a public protest each time a privacy invasion occurs is not an effective privacy

71. *Id.* at 2.

72. *See* Kim Girard, *IBM to Pull Web Ads over Privacy Concerns*, CNET NEWS, Mar. 31, 1999, http://news.cnet.com/2100-1023-223745.html; Nehf, *supra* note 70, at 3 (noting that self-regulation functions through informal coordination to protect privacy).

73. *See* Hahn & Layne-Farrar, *supra* note 5, at 108–10 (citations omitted) (summarizing changes by Equifax, AOL, CVS, RealNetworks, DoubleClick, and others); *see also* FTC STATEMENT ON BEHAVIORAL ADVERTISING, *supra* note 3, at 5–6.

74. *See* Alissa Cooper, *Backing Down on Behavioral Advertising*, CENTER FOR DEMOCRACY AND TECHNOLOGY, Oct. 13, 2008, http://blog.cdt.org/2008/10/13/backing-down-on-behavioral-advertising/ ("NebuAd is currently revisiting its business plans, while Adzilla has shuttered its North American operations altogether.").

75. Robert W. Hahn & Anne Layne-Farrar, *Is More Government Regulation Needed to Promote E-Commerce?*, 35 CONN. L. REV. 195, 201 (2002).

76. Hotaling, *supra* note 1, at 552 (citing Wayne R. Barnes, *Rethinking Spyware: Questioning the Propriety of Contractual Consent to Online Surveillance*, 39 U.C. DAVIS L. REV. 1545, 1604 (2006)).

77. Nehf, *supra* note 36, at 63.

78. *Id.* at 62.

policy. People should not have to start a public relations campaign whenever a dangerous privacy plan is exposed."[79]

This illustrates another problem with self-regulation—little or no actual enforcement. Meaningful self-regulation must include effective policing.[80] While the FTC does treat violations of a company's own privacy policy as a deceptive business practice,[81] it cannot reach those who do not voluntarily publish policies. In addition, FTC enforcement has been "sporadic" at best.[82] The FTC currently lists only twenty-five enforcement actions brought in this area under Section 5 of the FTC Act.[83]

Involving independent certification companies, like TRUSTe,[84] might solve the enforcement issue. TRUSTe's program certifies websites which conform to TRUSTe's privacy policies. Those websites which pass the certification process are then authorized to display the TRUSTe seal. TRUSTe also monitors certified websites to ensure continuing compliance.[85] But to be successful, companies must actually adopt certification standards. Currently, there is little evidence of widespread implementation. One scholar reports that TRUSTe has certified only a relatively small number of websites, and that "[a]mong the ten most popular websites, the majority lacked TRUSTe seals."[86]

Even if certification standards are widely adopted, the certification procedure may suffer from fatal flaws. For example, "the most popular seal programs do not perform regular and rigorous audits on their client's web sites to ensure that the web seal standards are being satisfied."[87] These defects may ultimately result in greater harm if users release more personal information under the expectation that the company offers robust privacy protection.

---

79. *Id.*

80. *See* Joe Mandese, *Online Privacy: IAB Pushes for Self-Reg*, MEDIAPOST NEWS, Sept. 22, 2008, http://www.mediapost.com/publications/?fa=Articles.showArticleHomePage&art_aid=91078 (quoting Eileen Harrington, then Deputy Director (now Acting Director) of the Bureau for Consumer Protection, Federal Trade Commission).

81. *See* 15 U.S.C. § 45 (2006) (prohibiting unfair or deceptive acts or practices).

82. Marcy E. Peek, *Information Privacy and Corporate Power: Towards a Re-Imagination of Information Privacy Law*, 37 SETON HALL L. REV. 127, 156 (2006).

83. FEDERAL TRADE COMMISSION, PRIVACY INITIATIVES, http://www.ftc.gov/privacy/privacyinitiatives/promises_enf.html (last visited Mar. 30, 2009).

84. TRUSTE, http://truste.org (last visited Mar. 17, 2009).

85. TRUSTE, TRUSTE PROGRAM SHEET, http://www.truste.org/pdf/TRUSTe_Programs_Sheet.pdf (last visited Mar. 19, 2009).

86. Oussayef, *supra* note 32, at 128 (citations omitted).

87. Nehf, *supra* note 36, at 65.

In addition, some argue that data breaches are proof that self-regulation will never work.[88] Once data is stolen or released, it can be sold and resold quickly, making it nearly impossible to trace the information back to the original leak. This prohibits accountability when specific injuries occur. "Without accountability, market forces cannot effectively curb harmful behavior."[89]

The successes of self-regulation are ultimately limited both in number and scope. While some scholars plead for more time before passing judgment,[90] it seems that self-regulation does not, and likely will not, do enough to protect personal privacy. The incentive structure supporting self-regulation seems to have at least two major problems: misguided incentives and ineffective policing. Self-regulation offers great promise for future innovation and a vibrant Internet industry. But, overall, this promise is not enough to outweigh its failure to protect personal privacy.

B. *Legislation*

The apparent failure of self-regulation to address privacy problems has caused many to turn to Congress for a solution. Enacting regulation through a federal statute can provide a nationwide standard, robust privacy protection, and a timely solution. In addition, legislative solutions have the ability to clearly identify acceptable practices, which can lower legal uncertainty and enable greater investment.

However, some claim that legislation will never pass, either because Congress lacks political consensus or because the online advertising industry has too much lobbying influence.[91] Whether or not this was true in the past, the specter raised by the possibility of ISP surveillance seems to have sparked a flurry of action in Congress. On May 16, 2008, Representatives Edward Markey and Joe Barton wrote to Charter Communications, an ISP, and asked it to postpone plans to track user activity.[92] Later, on August 1, John Dingell, Joe Barton, Edward Markey, and Cliff Steams, on behalf of the U.S. House of Representatives' Committee on Commerce and Energy, wrote a letter

88. *See* Marcey L. Grigsby, Book Note, *Seeking Privacy: Examining a Role for the Fiduciary in Protecting Personal Information*, 50 N.Y.L. SCH. L. REV. 1031, 1035–36 (2005) (reviewing DANIEL SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE (2004)).

89. Nehf, *supra* note 36, at 65.

90. Milina, *supra* note 18, at 284–85.

91. *See, e.g.*, Litman, *supra* note 2, at 1287.

92. Letter from Edward Markey and Joe Barton, Representatives of MA and TX respectively, to Neil Smit, President and CEO, Charter Communications (May 16, 2008), *available at* http://markey.house.gov/docs/telecomm/letter_charter_comm_privacy.pdf.

to 33 network operators, asking them to explain their current and future policies regarding data collection practices.[93]

In the Senate, on September 25, 2008, the Committee on Commerce, Science, and Communication held a hearing on Broadband Providers and Consumer Privacy.[94] There, representatives from AT&T,[95] Time Warner,[96] Verizon,[97] and Public Knowledge,[98] a Washington, DC-based public interest group,[99] addressed the Committee to identify concerns about online profiling by ISPs.

These recent events indicate that there may be enough political momentum and excitement over privacy concerns that a new law may be forthcoming. Specifically, Representative Barton, the ranking Republican on the House Energy and Commerce Committee stated "[a] broad approach to protecting people's online privacy seems both desirable and inevitable."[100] Others predict that the change in political control will result in legislative action.[101] Meanwhile, individual states, such as New York, Connecticut, and Massachusetts, have already begun work on enacting their own laws to protect consumer privacy.[102]

In addition, concerns about legislation dying at the hands of industry lobbying may have diminished. Many of the top Internet entities, such as Google,[103] Microsoft,[104] and the Interactive Advertising

---

93. Letter from John Dingell, Joe Barton, Edward Markey, and Cliff Steams, Representatives of MI, TX, MA, and FL respectively, to 33 Network Operators (August 1, 2008), *available at* http://energycommerce.house.gov/Press_110/110-ltr.080108.AOL-TILetters.pdf.

94. *Broadband Providers and Consumer Privacy: Hearings before the S. Comm. on Commerce, Science and Communication*, 110th Cong. (2008), *available at* http://commerce.senate.gov/public/index.cfm?FuseAction=Hearings.Hearing&Hearing_ID=778594fe-a171-4906-a585-15f19e2d602a.

95. *Id.* (statement of Dorothy Attwood, Senior Vice President, Public Policy, & Chief Privacy Officer, AT&T, Inc.), *available at* http://commerce.senate.gov/public/_files/AttwoodTestimony.pdf.

96. *Id.* (statement of Peter Stern, Executive Vice President, Chief Strategy Officer, Time Warner Cable), *available at* http://commerce.senate.gov/public/_files/PeterSternTestimony.pdf.

97. *Id.* (statement of Thomas J. Tauke, Executive Vice President of Verizon), *available at* http://commerce.senate.gov/public/_files/ThomasTaukeTestimony.pdf.

98. *Id.* (statement of Gigi B. Sohn, President, Public Knowledge), *available at* http://commerce.senate.gov/public/_files/SohnTestimony.pdf.

99. Public Knowledge, http://www.publicknowledge.org (last visited Nov. 18, 2008).

100. David Kaplan, *Google, Others Discuss Their Ad Targeting Secrets; Push for Legislation Is "Bipartisan"*, PAIDCONTENT.ORG, Aug. 12, 2008, http://www.paidcontent.org/entry/419-google-others-discuss-their-ad-targeting-secrets-push-for-legislation.

101. Hotaling, *supra* note 1, at 562.

102. Dominique R. Shelton, *Online Behavioral Advertising—Key to Internet Monetization or Privacy Probes?*, PRIVACY & INFO. L. REP., July-Aug. 2008, at 12, *available at* http://privacylaw.wildman.com/article/Online_Behavioral_Advertising.pdf.

103. Letter from Google to the House Energy and Commerce Committee (Aug. 8, 2008), *available at* http://energycommerce.house.gov/Press_110/Responses%20to%20080108%20TI%20Letter/110-ltr.080108responseGoogle.pdf.

104. *See* Shelton, *supra* note 102.

Bureau,[105] have recognized the value of a legislative solution and, to varying degrees, support such a proposal.

While a legislative solution may be inevitable, whether it can sufficiently protect privacy and preserve e-commerce remains uncertain. Legislation ultimately entails line drawing by those who are removed from the actual technology.[106] This hinders Congress' ability to create accurate and successful solutions.[107] Precision is important in this situation because an under-inclusive law may cement poor practices and neglect privacy altogether. At the same time an over-inclusive law brings high compliance costs that could "cripple . . . development and hurt consumers in the long run."[108] A poorly drafted law may also entrench and ultimately limit technological developments.[109] Given e-commerce's complete dependence on technology, "the worst thing a company might hear a person say is, 'We are from the government. We are here to help.' "[110]

Congress can hold hearings to become better informed, but hearings probably will not provide legislators with the same level of knowledge about, for example, computers and informational systems that those practicing in the field have already acquired through experience.[111] Congressional hearings often involve carefully worded speeches which might not accurately reflect current practices or future intentions.[112] Such testimonies may be less helpful than actual experience for forming specific policies.

Moreover, legislative line drawing causes problems in and of itself. Precise boundaries are nearly impossible to fix around online interac-

105. Renee Boucher Ferguson, *A Battle Is Brewing over Online Behavioral Advertising*, eWEEK.COM, March 27, 2008, http://www.eweek.com/c/a/Enterprise-Applications/A-Battle-Is-Brewing-Over-Online-Behavioral-Advertising-Market.

106. Nehf, *supra* note 36, at 58 ("One of the problems with privacy laws and regulations is that they are usually written by policy makers who lack thorough knowledge about the operation of computers and information systems.").

107. *See* Nehf, *supra* note 70, at 43 ("Efficiency determinations are difficult to make legislatively.").

108. Milina, *supra* note 18, at 272–74.

109. *Id.*

110. *Id.* (citing Fernando Piera, *International Electronic Commerce: Legal Framework at the Beginning of the XXI Century*, 10 CURRENTS: INT'L TRADE L.J. 8 (2001)).

111. Nehf, *supra* note 36, at 58 ("One of the problems with privacy laws and regulations is that they are usually written by policy makers who lack thorough knowledge about the operation of computers and information systems.").

112. For recent reports of allegedly misleading or ambiguous congressional testimony, see Dan Eggen & Paul Kane, *Gonzales: "Mistakes Were Made"*, WASH. POST, Mar. 14, 2007, at A01; Roy Mark, *Yahoo Counsel Denies Misleading House Committee*, eWEEK.COM, Nov. 3, 2007, http://www.eweek.com/c/a/IT-Infrastructure/Yahoo-Counsel-Denies-Misleading-House-Committee/; Wallace Matthews, *Long, Misleading Clemens Report to Bore Congress*, NEWSDAY (New York), Jan. 29, 2008, at A53.

tions because they are so varied and complex.[113] Even if drawn perfectly—an unlikely scenario—these lines will only work on existing practices. The next wave of innovations in technology and business methods quickly changing clarity into confusion.

In summary, the current political atmosphere suggests that there may be widespread support for a legislative remedy.[114] Unfortunately, the limitations inherent in a typical legislative solution restrict it from adequately addressing interests of both privacy and e-commerce. Notwithstanding these problems, the legislative process has the potential to produce an ideal regulatory scheme if it is modified to become better informed and flexible—characteristics best found in self-regulation. As one scholar observed, "a flexible approach that combines market forces, industry efforts, and law enforcement is far superior to broad legislation in addressing consumer concerns about online profiling, while simultaneously preserving its unprecedented benefits."[115] By incorporating characteristics of self-regulation, a modified legislative solution can protect both personal privacy and the opportunities enabled by online profiling.

IV. A MODIFIED SOLUTION

As discussed above, self-regulation provides flexibility and commercial success but seems to suffer from a poor incentive structure and inadequate enforcement. Legislation can provide enforcement and mandate nation-wide policies, but Congress may be too far removed from actual technology and business practices to draft a law sharp enough to cut away privacy harms without slicing into the benefits of online profiling. A modified legislative approach, as explained below, can leverage existing political momentum to protect personal privacy without stifling Internet-based industry.

Under this approach, Congress first announces its intention to enact a law protecting online privacy and provides a set time period (say, one year) in which companies can voluntarily implement privacy policies. Then, at the end of the year, companies can submit their policies with related data to Congress. After reviewing the various schemes, Congress

113. *See* Nehf, *supra* note 70, at 43–44 ("Although the deliberative process allows for many factors to be considered, ex ante mandatory terms are difficult to tailor precisely to specific contextual situations. . . . Privacy practices and online interactions between consumers and firms are varied and complex.").

114. *See supra* notes 92–105 and accompanying text.

115. Milina, *supra* note 18, at 286.

selects the policy which best protects privacy, and implements that standard as a baseline across the nation.[116]

Those companies which fall below this standard will have to modify their practices to conform to the new law. This, in effect, gives a head start for the winning company who can then acquire network effects and short term gains. These rewards act as incentives to encourage participation.

During the year-long window, companies are likely to compete with each other on privacy standards, since only the best policy wins the prize. Another advantage is that these rewards grow with greater privacy protection. The higher the privacy bar set by the winning company, the greater its windfall as other firms will have to make larger investments (with greater delays) to implement the new legal standard.

This approach improves the legislative process by enabling Congress to enact a law based on transparent records, rather than merely relying on edited testimony. Looking at established policies and observed facts removes much of the vagueness associated with simple hearings. In fact, this process creates incentives for firms not just to appear good before Congress and consumers, but to actually be good. Firms can enjoy the victor's spoils only if they fully disclose their practices and intentions. Those who try to win while obscuring their data collection practices will lose their head start because they too will eventually have to conform to the new, higher standard.

In addition, each company has a long-term, vested interest in preserving a vibrant e-commerce industry. Profiling firms are unlikely to implement privacy policies that create unprofitable business models. By choosing from a number of industry-implemented options, the privacy baseline enacted by Congress is less likely to suffocate e-commerce and eliminate the positive dividends of online profiling.

There are, of course, several drawbacks to this plan. For example, anti-competitive behavior is always an issue when allowing firms to set standards for their own industry. This risk may be higher here because the increased transparency and cooperation may facilitate the formation and perpetuation of an anti-competitive agreement. Overall, however, open disclosure will likely help curb anti-competitive behavior by allow-

116. The idea of comparing various approaches to a problem has been implemented in many situations. One famous example is Justice Brandeis' dissent: "[A] single courageous State may, if its citizens choose, serve as a laboratory; and try novel social and economic experiments without risk to the rest of the country." New State Ice Co. v. Liebmann, 285 U.S. 262, 311 (1932) (Brandeis, J., dissenting). Current scholars interpret this statement as "saying that state experimentation produces beneficial knowledge, and that states should therefore be permitted and encouraged to experiment to the greatest possible extent." James A. Gardner, *The New Judicial Federalism: A New Generation Symposium Issue: The "States-as-Laboratories" Metaphor in State Constitutional Law*, 30 VAL. U. L. REV. 475, 478 (1996).

ing regulators greater insight into which activities are for privacy regulation, and which activities are agreements for other purposes.

One specific worry is that competitors will combine and agree to keep all standards low so that Congress is forced to adapt a poor policy. However, such an agreement would require cooperation by hundreds of companies and is therefore unlikely to succeed due to coordination difficulties and the ever-present desire of individual firms to cheat on a collusive agreement.[117] Additionally, Congress could also indicate that it will implement a strict privacy regime unless sufficient standards are provided through the competition process.

Moreover, any agreement to keep standards low may merely prompt new companies, such as ISPs, to enter the advertising market with a higher privacy standard. A low industry standard creates a high incentive for a company to step in, take the positive publicity of setting the most protective policy, and quickly gobble up market share from existing companies. A concerted arrangement could attempt to include all potential entrants, such as ISPs, but the logistics of successfully identifying and incorporating every potential entrant into an agreement makes this scenario improbable.

However, allowing Congress such flexibility in choosing a solution may result in a choice based more on lobbying efforts than privacy protection. One critique of legislative involvement is that it "may result in a framework that entrenches the interests of the major Internet companies that can muster influence in Washington."[118]

Nevertheless, under the proposed plan, Congressional decisions are based on actual practices with observed data—sources more objective than mere testimony. This may remove some of the wiggle room that lobbyists exploit, and is likely to result in greater accountability to the public overall. This scenario makes lobbying dollars less influential and could increase participation by opening the door for smaller companies to get a jump on large corporations. While there are valid concerns about allowing Congress to pick a winner in any situation, the increased transparency and accountability under this plan may mitigate these problems.

Another concern is that legislation can be too inflexible to deal with evolving technology. Setting baselines, even ones based on actual practices, still requires line-drawing and may entrench existing technology. To avoid these problems, Congress can give the FTC authority to create and maintain a safe harbor, whose boundaries are initially formed by the best practices selected by Congress. The FTC would then evaluate

117. *See* Christopher R. Leslie, *Trust, Distrust, & Antitrust*, 82 TEX. L. REV. 515, 557–62 (2004).

118. Nehf, *supra* note 70, at 42.

industry standards on a regular basis and modify the safe harbor provisions to include the best industry practices across various technologies. Besides incorporating the benefits of privacy competition mentioned above, a safe harbor provision maintained by the FTC can provide evolving privacy standards and allow for long-term competition on privacy terms. Overall, this solution offers the flexibility needed to adequately protect privacy and e-commerce.[119]

Unfortunately, the transparency associated with this proposal may be its greatest weakness as well as its greatest strength. Wide disclosure to the public means competitors can access the information too. For example, a company that implements a protective policy may see others quickly follow to eliminate any head start the modified policy could give. Worse still, a company might anticipate this behavior and not move in the first place. Nevertheless, even if there is no market-based reward, there are still important incentives to motivate companies to compete. One reward is to have a federal statute proclaiming that your privacy policy is the best and completely legal. This will bring significant positive publicity as well as removing uncertainty for investors.

Overall, this modified solution is attractive because it combines the benefits of legislation, such as a nationwide standard, governmental enforcement, and a timely solution, with the flexibility and industry knowledge found in self-regulatory solutions. In addition, this approach brings greater transparency and adapts the incentive structure to encourage firms to compete on privacy grounds. By implementing this solution, Congress can capitalize on the current political momentum and properly address the privacy problems without destroying the benefits of online profiling.

CONCLUSION

Online profiling offers consumers unprecedented benefits but also poses disturbing threats to personal privacy. Efforts to address privacy problems should be carefully tailored to avoid suffocating a thriving e-commerce community. Unfortunately, current suggestions for reform tend to favor privacy at the expense of e-commerce or are unlikely to protect privacy in any meaningful way. Meanwhile, privacy concerns appear to be serious enough to muster broad political support for a legislative remedy, despite the defects associated with traditional legislation.

---

119. *See id.* at 54 ("Compared to a broad-based legislative approach, the ebb and flow of an incremental, evolutionary process is less likely to set inefficient norms in stone, and adjustments can be made over time as businesses obtain and manipulate personal information in increasingly sophisticated ways.").

Congress can capitalize on the existing political momentum and advance the interests of both privacy and e-commerce by enacting a legislative scheme which incorporates aspects of self-regulation. This modified approach creates incentives for companies to compete on privacy grounds by implementing the most protective policy into a legally enforceable baseline. In addition, Congress can give authority to the FTC to maintain a safe harbor whose boundaries are formed through a similar competitive process.

This proposed solution is ideal because it allows society to harvest the rewards of online profiling and skirt the privacy pitfalls present in the practice today. It significantly improves the legislative approach by enabling greater transparency and by empowering those closest to technology to draft legal standards. This approach also creates flexible regulation that can better respond to evolving technologies then the typical legislative process. By combining the benefits of legislation and self-regulation, this solution includes the characteristics necessary to ensure both personal privacy and a thriving e-commerce community.