Global Business & Development Law Journal

Volume 26 | Issue 1 Article 14

2-1-2013

Protecting Consumer Data While Allowing the Web to Develop Self-Sustaining Architecture: Is a Trans-Atlantic Browser-Based Opt-In for Behavioral Tracking the Right Solution?

Erica M. Scott

Protecting Consumer Data While Allowing the Web to Develop Self-Sustaining Architecture: Is a Trans-Atlantic Browser-Based Opt-In for Behavioral Tracking the Right Solution?

Erica M. Scott∗

TABLE OF CONTENTS

I. INTRODUCTION

Sally loves to shop for shoes. One day, she noticed that a pair of shoes she had been eyeing popped up on her favorite news site. "The Internet is psychic!" she screamed, surprised. Sorry Sally, it is not magic, it is just behavioral, or targeted, advertising.

Collection of data about an Internet user's browsing habits helps companies to display ads in which she is interested. The revenue from her purchases

∗ J.D. candidate, 2013, University of the Pacific, McGeorge School of Law; B.A. and B.S. Loyola Marymount University, 2007. I would like to thank my faculty advisor, Michael Vitiello, for his thoughtful comments, instructive grammar lessons, and general support while I was writing this piece.

sponsors the free content that she craves. She is not charged a dime to read the news, but she is giving up her privacy in her digital footprint.[1] The digital footprint is what the user sees and does on the Internet.[2] How should the user be informed about who is tracking and collecting data on her online behavior and how that data is being used? And what country should write the rules in an age where websites see traffic from users across national borders and personal data can be sent around the globe in a fraction of a second?

Online Behavioral Advertising ("OBA") has become an increasing concern of privacy rights activists,[3] consumers,[4] industry representatives,[5] and legislators[6] in the past ten years[7] in the United States[8] and the European Union.[9] Recently, the European Union has been evaluating how to regulate behavioral tracking, such as explicit consumer opt-in or opt-out[10] of data collection.[11] This Comment evaluates the proposed EU[12] and U.S. schemes and suggests that an international browser-

1. *See* Caroline McCarthy, *Survey: Advertisers Should Acknowledge Targeted Ad Concerns*, CNET NEWS (July 2, 2008, 1:20 PM), http://news.cnet.com/8301-13577_3-9983177-36.html.

2. *Id.*

3. Nate Anderson, *Privacy Groups Pitch "Don't Track Me" Ad Server Blacklist*, ARSTECHNICA (Oct. 31, 2007, 6:37 PM), http://arstechnica.com/old/content/2007/10/privacy-groups-propose-do-not-track-list.ars.

4. *See* Elinor Mills, *Don't Like Targeted Ads? Opt Out Says Online Ad Group*, CNET NEWS (Feb. 24, 2001, 11:45 AM), http://news.cnet.com/8301-10784_3-9877604-7.html.

5. *Id.*

6. Emily Steel, *Lawmakers Draft Web-Ad Privacy Safeguards*, WALL ST. J. (May 4, 2010), http://online.wsj.com/article/SB10001424052748703612804575222601908300456.html.

7. *See, e.g.*, Evan Hansen, *Perspective: Net Privacy and the Myth of Self-regulation*, CNET NEWS (Oct. 16, 2001, 4:00 AM), http://news.cnet.com/Net-privacy-and-the-myth-of-self-regulation/2010-1071_3-281580.html?tag=mncol;6n.

8. *See* Jacqui Cheng, *Privacy Groups: Behavioral Opt-out System "Insufficient and Ineffective,"* ARSTECHNICA (Sept. 8, 2011, 5:20 PM), http://arstechnica.com/tech-policy/news/2011/09/privacy-groups-behavioral-opt-out-system-insufficient-and-ineffective.ars.

9. *See Brussels to Tighten Data Protection Rules*, EURACTIV.COM (Sept. 8, 2010), http://www.euractiv.com/infosociety/brussels-tighten-data-protection-rules/article-186779; *EU Data Protection Directive*, ELECTRONIC PRIVACY INFO. CENTER, http://epic.org/privacy/intl/eu_data_protection_directive. html (last visited Oct. 24, 2011); Hunton & Williams, L.L.P., *European Commission Postpones Revision of the General Data Protection Directive*, PRIVACY & INFO. SECURITY L. BLOG (Aug. 3, 2010), http://www.Hunton privacyblog.com/2010/08/articles/european-commission-postpones-revision-of-the-general-data-protection-directive/.

10. An opt-out program forces users to take action to be *removed* from advertisers' lists or databases used to target advertisements to the individual user's tastes. By default the user's data is included in a list or database. An opt-in program, however, is the opposite; a user must take action to have her data *included* in a list or database. The National "Do Not Call" Registry, where an individual desiring to remove herself from telemarketers' lists can register, is an opt-out solution. NATIONAL DO NOT CALL REGISTRY, https://www.donotcall.gov/ (last visited Feb. 14, 2012). Once registered, the individual's home number should be "scrubbed" from call lists. *Id.* Telemarketers are required to periodically update their databases to conform to the Do Not Call Registry. *Id.* In 2008, the Act creating the Registry was updated to allow registrants to remain permanently on the list. *Id.*

11. *European Self-Regulation for Online Behavioral Advertising: Transparency and Control for Consumers*, INTERACTIVE ADVER. BUREAU EUR. (Apr. 27, 2011), http://www.iabeurope.eu/media/51925/iab%20europe%20oba%20framework_merged%20ii.pdf.

12. *Europe's Online Advertising Industry Releases Self-Regulation Framework*, INTERACTIVE ADVER.

level opt-in that engages the consumer, explicitly communicates to them that their data is being collected, and presents transparent options to decline data collection, is a practicable and efficient solution to online tracking privacy concerns. The browser-level opt-in must be combined with legislative efforts to make data collection, retention, and disclosure practices more transparent. Part II simplifies the basics of the digital footprint: how the footprint is generated; how the footprint is stored; and how a user's digital footprint is used in online behavioral advertising. It discusses how browsing behavior is tracked, who retains, sells or buys browsing data, and the data's potential beneficial and harmful uses. Part III presents a brief introduction to the landscape of existing legislation in the United States and the European Union that govern data collection for the purposes of advertising. Part IV discusses pending legislation in both locations and the merits or failings of these proposed solutions. Part V suggests a unified trans-Atlantic solution and evaluates three options for dealing with behavioral tracking of user Internet activity: industry self-regulation, governmental regulation, or a combination of the two.[13] This Comment suggests that transparent, browser-based user controls with the maximum "default" privacy level, regulated by government but implemented at the industry level, are the appropriate solution. This browser-level implementation must be combined with stricter guidelines for data retention and protection policies, auditing of compliance, mandatory reporting of breaches, and harsh penalties if those databases are breached and personal data is let into the "wild," that is, outside of the user's or any authorized second party's control.[14]

II. MECHANICS OF ONLINE BEHAVIORAL ADVERTISING

The average Internet user perceives the computer as a magic box where things happen with the wave of a mouse.[15] It can be difficult to understand the mechanics of data transmission and aggregation, that is, how the websites a user visits can "know" about her activity past and present, because the transmission is invisible to the user. This section simplifies the digital footprint basics: how advertisers save, process, and use that footprint for online behavioral advertising.

BUREAU EUR. (Apr. 14, 2011), http://www.iabeurope.eu/news/self-regulation-framework.aspx.

13. *See Browser Firms Plan 'Do Not Track' Systems*, BBC NEWS, (Jan. 25, 2011), http://www.bbc.co.uk/news/technology-12275750; s*ee also Cookie Law Deferred for One Year*, BBC NEWS, (May 25, 2011), http://www.bbc.co.uk/news/technology-13541250.

14. *See* Viviane Reding, Vice-President, European Comm'n & E.U. Justice Comm'r, Speech on Building Trust in the Digital Single Market: Reforming the EU's Data Protection Rules (Nov. 28, 2011), *available at* http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/11/814.

15. David M. Compton et al., *The Prediction of Perceived Level of Computer Knowledge: The Role of Participant Characteristics and Aversion toward Computers*, INFORMING SCI., 2002, at 220, 221.

A. Digital Data and the Cost of Internet Advertising

Information is money[16] and in the digital age, data is the new pollution.[17] For decades, data regarding consumers' likes and dislikes has been collected.[18] Catalog companies and credit card providers notoriously use this data to create targeted ads.[19] Online activity, however, is a new and promising resource, but the digital runoff has a much longer half-life than data collected via other methods.[20] Consumer data can now be collected in ever-increasing depth and more parties are becoming involved in its collection, aggregation, analysis, and storage.[21] This large amount of cyberspace-generated data is detailed, subject to accurate search, and durable.[22]

The ability to collect more information about consumers leads to more effective advertisements and higher revenue for ad companies.[23] Internet ad revenues rose to a record $14.9 billion in the first half of 2011.[24] Consumers accustomed to the freedom of the Internet rarely understand that there are invisible price tags attached to every click.[25] Ads pay for the free content that consumers have come to expect on the Internet.[26] In the quest for a financial model supporting a free Web, advertisers, search engines, and even Internet Service Providers ("ISPs")[27] have tapped into user data to target advertisements to individuals.[28] And now, without it, advertising lobby groups say that the free

16. Declan McCullagh, *Web Monitoring for Ads? It May Be Illegal*, CNET NEWS (May 19, 2008, 1:10 PM), http://news.cnet.com/8301-13578_3-9947499-38.html (stating that in 2008, online advertising was "roughly a $45 billion-a-year business").

17. Open Rights Group, *Bruce Schneier Security Q & A*, VIMEO (Dec. 4, 2009), http://vimeo.com/8062617; *Data Usage & Control Primer: Best Practices & Definitions*, INTERACTIVE ADVER. BUREAU, 1 (May 2010), http://www.iab.net/media/file/data-primer-final.pdf.

18. *Data Usage & Control Primer: Best Practices & Definitions*, *supra* note 17, at 1.

19. *Id.*

20. *Id.*

21. *Id.* at 2.

22. Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 STAN. L. REV. 1193, 1199 (1998).

23. *Data Usage & Control Primer: Best Practices & Definitions*, *supra* note 17, at 3.

24. *Internet Ad Revenues at Nearly $15 Billion in First-Half 2011, Up 23%, Second Quarter 2011 Breaks Record Again*, INTERACTIVE ADVER. BUREAU (Sept. 28, 2011), http://www.iab.net/about_the_iab/recent_press_releases/press_release_archive/press_release/pr-092811.

25. *See* Caroline McCarthy, *Study: Like It Or Not Behavioral Ad Targeting Works*, CNET NEWS (Mar. 24, 2010, 9:01 AM), http://news.cnet.com/8301-13577_3-20001069-36.html (quoting a 2010 press release from the Network Advertising Initiative ("NAI") executive director Charles Curran).

26. *Id.*

27. McCullagh, *supra* note 16 (noting that some Internet Service Providers have systematically intercepted customers' Web browsing via a process called deep-packet inspection: "Because deep packet inspection can, barring the use of encryption, monitor everything that a customer does online, a broadband provider is in the enviable position of being able to know exactly what each customer is doing. The odds of successful monetization are high.").

28. *See* McCarthy, *supra* note 25.

services and content on the Internet will dry up.[29] Supporting free content with third-party paid advertisements is not novel to consumers.[30]

In presenting products that appeal to the individual, the advertiser hopes that more users will click through to the advertised webpage, article, or digital storefront.[31] One study showed that behaviorally targeted ads turn 6.8 percent of click-through users into buyers.[32] When compared to the 2.8 percent buyer-yield generated by non-targeted ads, behavioral targeting is more than twice as effective.[33] The more user-tailored the ad, the higher the "click-through rate" ("CTR").[34] A higher CTR means greater revenues.[35] Although behavioral advertising is the "vanguard of online marketing," because it generally leads to more sales than do random ads,[36] consumers and privacy groups are concerned that there is insufficient transparency in collection, use, and sale of the data.[37] The problem is that an undisclosed third-party ad company, whose name does not appear in website content or in the URL, is monitoring an individual user's online activities.[38]

B. Distribute Your Cookies and Collect Them Too

Ad companies collect user data via cookies.[39] Cookies are small text files that keep track of a user's online patterns and preferences.[40] Furthermore, they

29. Louise Story, *A Push to Limit the Tracking of Web Surfers' Clicks*, N.Y. TIMES (Mar. 20, 2008), http://www.nytimes.com/2008/03/20/business/media/20adco.html?_r=1&ref=media&oref=slogin.

30. *See* MDoherty, *What Would Happen if Advertising Didn't Exist?* TRUTH IN ADVERTISING (Aug. 5, 2012, 12:32 PM), http://trueadvertise.wordpress.com/2011/07/08/what-would-happen-if-advertising-didn%E2%80%99t-exist/.

31. *See* Elinor Mills, *New York Lawmaker Wants Opt-In Online Ad Tracking*, CNET NEWS (Mar. 20, 2008, 11:03 AM), http://news.cnet.com/8301-10784_3-9899587-7.html#ixzz1Z1Z6gNNy.

32. McCarthy, *supra* note 25.

33. *Id.*

34. Omer Tene, *Privacy: The New Generations*, 1 INT'L DATA PRIVACY LAW 15, 16 (2011) (the CTR is rather self-explanatory. It is the number of users who see an ad and click on it).

35. *Id.*

36. Mills, *supra* note 31.

37. Emily Steel, *Lawmakers Draft Web-Ad Privacy Safeguards,* WALL ST. J. (May 4, 2010), http://online.wsj.com/article/SB10001424052748703612804575222601908300456.html.

38. *Frequently Asked Questions,* NETWORK ADVERTISING INITIATIVE, http://www.network advertising.org/managing/faqs.asp#question_2 (last visited Oct. 21, 2011).

39. Id. ("Cookies are small chunks of data created by a Web server, delivered through a Web browser, and stored on a user's computer. They provide a means for Websites the user visits to keep track of online patterns and preferences, as well as identify the user as a return visitor. Cookies make the personalization of Web experiences possible. Network advertisers use cookies to track users' Web preferences and characteristics and tailor ads for them.").

40. Nicholas C. Zakas, *HTTP Cookies Explained*, NCZONLINE (May 5, 2009, 9:00 AM), http://www.nczonline.net/blog/2009/05/05/http-cookies-explained/ (standard cookies are plain text files; they are not executable programs and thus harmless in and of themselves).

identify users as return visitors to a specific website[41] by recording a web browser's visit to a webpage or interaction with specific web content.[42] Cookies record data such as basic registration information (favorite username or zip code), behavioral data, and user location.[43]

Ad servers analyze this data to make inferences about the consumer's preferences, including habits and hobbies.[44] User-specific information is funneled into a "segment," which is a user group defined by similarity in demographic, market, or interest-related attributes.[45] Ad servers determine segment membership based on online browsing activity or "declared"[46] information such as age or gender.[47] Companies like Netflix, an online DVD and streaming video service, use group data to predict a particular user's likes and dislikes.[48] "Inferred data is the result of statistical software prediction based on one or more user attributes."[49] The general idea is that if the user is a woman, she likes things that other women like.[50] Netflix, for example, could know that the user is female and infer that she might like to watch movies that other female users have put into their queue of movies to rent.[51] Aggregating many individuals' behaviors into prediction software allows more variable attributes to be analyzed.[52] This affects profits because it can increase the accuracy of the prediction or inference by three to four percent.[53] This inference system assumes that two people who like the same video game, for example, will also like the same kind of tee-shirt.[54] This method of determining what, to whom, and where to advertise requires vast amounts of personal data.[55] Collecting this data is called mining.[56] These vast personal profiles, packaged into databases and marketed wholesale, can be

41. *Frequently Asked Questions*, *supra* note 38.

42. *Data Usage & Control Primer: Best Practices & Definitions*, *supra* note 17, at 4.

43. *Frequently Asked Questions*, *supra* note 38; *Data Usage & Control Primer: Best Practices & Definitions*, *supra* note 17, at 5.

44. *Frequently Asked Questions*, *supra* note 38.

45. *Data Usage & Control Primer: Best Practices & Definitions*, *supra* note 17, at 3.

46. In this case "declared" means "voluntarily disclosed" such as when a user creates an online profile with a website or answers non-anonomized survey questions. *Id*.

47. *Id.*

48. *See* Remus Titiriga, *Social Transparency Through Recommendation Engines and its Challenges: Looking Beyond Privacy*, 15 ECON. INFORMATICS J. 147, 148 (2011), *available at* http://ssrn.com/ abstract=1944728.

49. *Data Usage & Control Primer: Best Practices & Definitions*, *supra* note 17, at 3.

50. *Id.*

51. *Id.*

52. *See* Titiriga, *supra* note 48, at 148.

53. *Id.*

54. *Id.*

55. *Id.*

56. *See* Julia Angwin, *The Web's New Goldmine: Your Secrets*, WALL ST. J. (July 30, 2010), http://online.wsj.com/article/SB10001424052748703940904575395073512989404.html.

overlaid with specific transactional data including what a user reads, buys, or thinks about and allows for a "rich and telling portrait of the individual."[57]

C. Anonymity and the Depth of Data Collection

A central concern for users and regulators alike is whether the scale of modern data aggregation poses a security risk for individuals whose data is collected and stored. Thus, an important consideration in data privacy analysis is whether the data held by an aggregator can be linked to a particular user. Consider the following situation with a generic data "Aggregator," like Google, and a generic "User" accessing the Internet from Sacramento, California. All Aggregator knows about User is that it (not she or he) likes to shop for shoes and go to Sacramento Kings games. There is no serious concern about a breach to the individual's privacy because Aggregator cannot connect User to the real person living in Sacramento, California at 12345 Maple Hill Drive. The advertising lobby emphasizes that browsing data is collected and stored anonymously.[58] But the term "anonymous" may be deceptively secure.[59]

Anonymous data, also called "non-personally identifiable information" ("Non-PII"),[60] is generated from tracking online activity. This includes email, searches, clicking a link on a webpage or an ad, as well as commercial transactions like buying a book on Amazon or even just putting it in the digital cart.[61] Non-PII, however, can be merged or linked to "personally identifiable information" ("PII")[62] or information collected from a survey, offline purchase record, census or registration form, thus eliminating user anonymity.[63] In fact, "deanonymizing" individuals buried in anonymized data is possible and rather simple for an experienced hacker.[64]

Advertising networks say that the raw data collected for online behavioral tracking is anonymous.[65] But more often than not, "anonymous" really means

57. Kang, *supra* note 22, at 1239 (advertising segments can be narrowed "all the way down to one person"); Angwin, *supra* note 56.

58. *Frequently Asked Questions*, *supra* note 38 ("Information that is anonymous or not linked to a particular person." Used for Online Behavioral Advertising ("OBA") "by network advertisers, this data consists mostly of click-stream information (sites user have visited or links user have clicked) compiled as you move across different web sites or a single site.").

59. Arvind Narayanan, *There Is No Such Thing as Anonymous Online Tracking*, CTR. FOR INTERNET AND SOC'Y (July 28, 2011, 12:38 PM), http://cyberlaw.stanford.edu/node/6701.

60. *Frequently Asked Questions*, *supra* note 38.

61. *Data Usage & Control Primer: Best Practices & Definitions*, *supra* note 17, at 4.

62. Personally identifiable information (PII) includes data used to identify, contact or locate a person, including name, address, telephone number, or email address. *Frequently Asked Questions*, *supra* note 38.

63. *Id.*

64. Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. REV. 1701, 1701 (2010).

65. Identifying information, such as user name or IP address, is not collected. The data is linked only to a numbered cookie on the user's computer. *Frequently Asked Questions*, *supra* note 38.

"pseudonymous."[66] "Pseudonymous" is a more appropriate term according to Arvind Narayanan, a Ph.D. behind the "Do Not Track" proposal.[67] He points out that user-identification affects tracking that has already taken place and future tracking.[68] A user need only be identified once along the browsing timeline in order to track her behavior.[69] Users facilitate deanonymization[70] of their own data when they use unique IDs such as their primary email address or user name from their favorite social network.[71]

In addition to the skepticism of researchers about the anonymity of collected data, users also need to be concerned about leakage.[72] Leakage occurs when private information is transmitted from a first-party site to a third-party server who may not be identified or known to the user.[73] As many as three-quarters of the most popular websites monitored in one study leaked sensitive information such as user IDs or email addresses.[74] Some leakage was unknown to the first-party website, but generally all leakage occurred without the knowledge or consent of the user herself.[75] An example of this leakage is a popular website that sent its users' gender, zip code, and music interests directly to DoubleClick.net when users chose songs to play for free.[76] Another example of significant third-party leakage is the dating site OkCupid.[77] Johnathan Mayer, a graduate

66. Narayanan, *supra* note *59* (pointing to a famous cartoon drawn in 1993 for the New Yorker by Peter Steiner entitled "On the Internet Nobody Knows You're A Dog," as an example of the false notions of anonymity held by Americans, and Internet users in general).; *see* Peter Steiner, *On the Internet Nobody Knows You're a Dog*, THE NEW YORKER, July 5, 1993, at 61, *available at* http://www.unc.edu/depts/jomc/academics/dri/idog.html. As of 2000, the cartoon was the most reproduced cartoon ever printed by The New Yorker; Glenn Fleishman, *Cartoon Captures the Spirit of the Internet*, N.Y. TIMES (Dec. 14, 2000), http://www.nytimes.com/2000/12/14/technology/cartoon-captures-spirit-of-the-internet. html.

67. Arvind Narayanan is one of the many researchers behind the "Do Not Track" project, which develops and promotes universal web tracking opt-out solutions for user's browsers. The "Do Not Track" project likens itself to the National Do Not Call Registry. DO NOT TRACK, http://donottrack.us/ (last visited Feb. 16, 2012); *see* DO NOT CALL REGISTRY, *supra* note 10.

68. Narayanan, *supra* note *59*.

69. *Id.*

70. Ohm, *supra* note 64, at 1706.

71. *See* Balachander Krishnamurthy, Konstantin Naryshkin, & Craig E. Willis, *Privacy Leakage Vs. Protection Measures: The Growing Disconnect*, 1 (May 26, 2011), http://www2.research.att.com/~bala/papers/w2sp11.pdf (unpublished article presented at Web 2.0 Security & Privacy 2011 Conference in Oakland, CA); *see also* Narayanan, *supra* note 59. There are an increasing number of websites which allow the user to sign in with her Google, Twitter, or Facebook account login. *See, e.g.*, PINTEREST, https://pinterest.com/login/?next=/ (last visited Feb. 16, 2011).

72. Narayanan, *supra* note *59*.

73. Krishnamurthy, Naryshkin, & Willis, *supra* note 71*,* at 2. In the study, "56% of the sites directly leak pieces of private information," such as whether or not the user "likes" a given item or the comment a user makes on a photo, and the result grows to 75% if one includes user ID information. *Id.*

74. *Id.* at 1.

75. *Id.*

76. *Id.* at 6.

77. Johnathan Mayer, *Tracking the Trackers: Where Everybody Knows Your Username*, CTR. FOR INTERNET & SOC'Y (Oct. 11, 2011, 8:06 AM), http://cyberlaw.stanford.edu/node/6740.

researcher in law and computer science at Stanford University, found that OkCupid leaked usernames to twenty-seven third-parties.[78] The website also leaked other profile information to two advertising data providers.[79] The leaked information included: age, pets, children, frequency of drug and alcohol use, education, ethnicity, gender, income, language, religion, relationship status, and ZIP code, all without the users' knowledge or consent.[80] Leakage demonstrates the scope of the data-control problems the user is faced with each time she logs on to the Internet. The user voluntarily exchanges her information for services from the first-party website, but receives no comparable compensation from third-parties to whom her data is leaked. The user cannot mitigate the risk of misuse by third-parties of whom she has no knowledge.

Apart from the clearly non-anonymous nature of a user's email address and zip code, even behavioral data can be deanonymized by linking consistent use to persistent, individually numbered, cookies placed on the users' computer.[81] Blocking cookies, however, is not a complete solution to deanonymizing of aggregated data.[82] There are two other methods of identifying users through anonymous data through their IP addresses and browser fingerprints.[83]

Each Internet-enabled device (e.g., mobile phone, tablet, or computer) is assigned a dynamic[84] Internet Protocol ("IP") address that identifies the device's geographic location rather than the user's identity.[85] While this identifier changes periodically, for short periods of time, the anonymity provided is weak.[86] Internet Service Providers ("ISP"), however, may retain records of the IP address assigned to a subscriber for a specific session and retain information on session

78. *Id.*

79. *Id.*

80. *Id.*

81. *E.g.*, Angwin, *supra* note 56; Krishnamurthy, Naryshkin, & Willis, *supra* note 71, at 3. The Krishnamurthy report makes it very clear that the first-party website, with whom the user believes she is communicating, is conveying her information via a cookie to a third party. Krishnamurthy, Naryshkin, & Willis, *supra* note 71*,* at 3, fig.2.

82. *See* Krishnamurthy, Naryshkin, & Willis, *supra* note 71*,* at *3.* A browser fingerprint is different than a digital footprint—he browser fingerprint is the unique stamp of a browser program when it interacts with Internet content. The digital footprint includes the browser fingerprint. *See generally* PANOPTICLICK, https://panopticlick.eff.org/ (last visited June 17, 2012).

83. Krishnamurthy, Naryshkin, & Willis, *supra* note 71, at 6.

84. "Dynamic" means that the IP address is not fixed, or device-specific. A device is assigned a different IP address each time the device connects to a computer network such as an Internet Service Provider ("ISP"). ISPs are allocated certain blocks of IP addresses. Each time a user logs onto the Internet from their home computer, the computer is assigned an IP address from among those allocated to the ISP. *See* Declan McCullagh, *House Panel Approves Broadened ISP Snooping Bill*, CNET NEWS (July 22, 2011, 1:41 PM), http://news.cnet.com/8301-31921_3-20084939-281/house-panel-approves-broadened-isp-snooping-bill/.

85. *Data Usage & Control Primer: Best Practices & Definition*s, *supra* note 17, at 4. Often, several computers share the same IP address, further anonomizing the data transactions. *Id.* However, IP address can be combined with other information to personalize the information. *See Frequently Asked Questions*, *supra* note 38.

86. Krishnamurthy, Naryshkin, & Willis, *supra* note 71*,* at 6*.*

activity, essentially eliminating any anonymity afforded by random IP assignment.[87] Not only can an ISP track user activity via IP address, with very little effort an ISP can monitor transmitted content of any kind.

Through Deep Packet Inspection ("DPI") an ISP can examine the contents of the data it transmits to and from the user.[88] DPI is the method for filtering the Internet and can be used to block certain websites or to monitor web activity much more extensively than cookies.[89] Information communicated on the Internet is sent inside "packets" that are like digital envelopes.[90] Generally, ISPs use only "shallow packet inspection" and the ISP sees only the information "on" the packet, likened to an address on an envelope.[91] DPI, then, is akin to the Post Office opening a letter and reading the contents.[92] ISPs then are able to block, change, observe, and discriminate against data in any direction.[93] DPI can be useful to prevent harmful viruses from being transmitted, but it can also be used to survey all activity and transmitted content on an individual user's computer.[94]

In 2008, Charter Communications, an American ISP, rolled out hardware for a contracting ad-server called NebuAd that used DPI to inspect the contents of transmitted packets in order to build profiles to serve targeted advertisements to ISP subscribers.[95] Angry consumers subsequently sued NebuAd into non-existence because of computer fraud concerns related to their methods of putting cookies onto subscribers' computers.[96] But ISPs retain the technical capability to conduct this type of data mining.[97] While DPI is a goldmine for investigators and advertisers,[98] an individual should be concerned about the privacy of their internet communications.

87. McCullagh, *supra* note 84. In July, 2011, the U.S. House of Representatives approved a bill requiring ISPs to retain user data such as names, addresses, credit card numbers, and IP addresses. *Id.* In 2005, the European Parliament passed legislation requiring ISPs to retain data on Internet access times and IP addresses for anywhere between six months and two years. Jo Best, *Europe Passes Tough New Data Retention Laws*, CNET NEWS (Dec. 14, 2005, 10:38 AM), http://news.cnet.com/Europe-passes-tough-new-data-retention-laws/2100-7350_3-5995089.html?tag=mncol;txt.

88. Generally this means "drilling down" into all seven layers of the packet. Nate Anderson, *Deep Packet Inspection Meets 'Net neutrality, CALEA*. ARS TECHNICA (July 26, 2007, 4:10 AM), http://arstechnica.com/hardware/news/2007/07/Deep-packet-inspection-meets-net-neutrality.ars. The 7th layer is the "application layer" where the actual message resides. *Id.*

89. *Id.*

90. *Id.*

91. *Id.*

92. *Id.*

93. Anderson, *supra* note 88.

94. *Id.*

95. *Deep Packet Inspection and Privacy*, ELEC. PRIVACY INFO. CTR., http://epic.org/privacy/dpi/ #legal (last visited Jan. 16, 2012).

96. Ryan Singel, *NebuAd Nearly Shut Down, Court Papers Say*, WIRED (May 19, 2009, 11:06 AM), http://www.wired.com/epicenter/2009/05/nebuad-venture-capital-dispatch-wsj/.

97. *See id.*

98. DPI "is used by law enforcement to grab complete copies of particular users' Internet data-streams in investigations." Nate Anderson, *Deep Packet Inspection Engine Goes Open Source,* ARS TECHNICA (Sept. 9,

D. The Dangers of Ubiquitous Data Collection

While spyware,[99] adware,[100] viruses,[101] and cookies, have become part of everyday language, privacy advocates say that users are unaware[102] of how data is collected and the extent of data collection[103] by companies they trust.[104] For example, recently irate users sued several prominent websites in United States Federal Court for using Adobe Flash-based "zombie" cookies that could not be permanently deleted via traditional browser cache deletion.[105] These Flash cookies recreate themselves after deletion and retrieve just-deleted user information in order to continue tracking the user.[106] Another advertising company, Ringleader Digital, requires a user to click on a company-specific opt-out link, which will change the user identification at the database level, in the company's control, to an opt-out ID.[107] The user is, however, still being identified by "browser identifiers, session information, device type, carrier provider, IP addresses, unique device ID, carrier user ID and web sites visited" for the purposes of "not" sending targeted advertising to the user's device.[108]

If data is stored correctly and not abused, users should not experience any negative effects from behavioral tracking.[109] Aggregated user data could,

2009, 12:31 PM), http://arstechnica.com/open-source/news/2009/09/deep-packet-inspection-engine-goes-open-source.ars.

99. Spyware is "software, installed unknowingly, that gathers information about an Internet user's browsing habits or intercepts personal data, transmitting this information to a third party for commercial gain." Spyware Definition, DICTIONARY.COM, http://dictionary.reference.com/browse/spyware (last visited Oct. 24, 2011).

100. Adware is "a type of spyware that gathers information about an Internet user's browsing habits and displays targeted or contextual advertisements." Adware Definition, DICTIONARY.COM, http://dictionary.reference.com/browse/adware (last visited Oct. 24, 2011).

101. A virus is "a segment of self-replicating code planted illegally in a computer program, often to damage or shut down a system or network." Virus Definition, DICTIONARY.COM, http://dictionary.reference.com/browse/virus (last visited Oct. 24, 2011).

102. Jacqui Cheng, *Advertisers get hands stuck inside HTML5 database cookie jar*, ARSTECHNICA (Sept. 7, 2010, 1:00 PM), http://arstechnica.com/apple/news/2010/09/rldguid-tracking-cookies-in-safari-database-form.ars.

103. *What Is The NAI Doing to Help You Protect Your Privacy?*, NETWORK ADVERTISING INITIATIVE, http://www.networkadvertising.org/managing/ (last visited Oct. 21, 2011). Much "of what occurs with online advertising isn't visible to consumers." *Id.* The average consumer has "no idea how much information is being collected about them . . . ." Story, *supra* note 29.

104. Mills, *supra* note 31. *See* Greg Sandoval, *Mimes Aren't Silent in Capitol Hill Attack on Google*, CNET NEWS (Sept. 21, 2011, 12:53 PM), http://news.cnet.com/8301-31001_3-20109685-261/mimes-arent-silent-in-capitol-hill-attack-on-google/#ixzz1Z1RADHLo.

105. Ryan Singel, *Privacy Lawsuit Targets 'Net Giants Over "Zombie" Cookies*, ARSTECHNICA (July 28, 2010, 1:24 AM), http://arstechnica.com/tech-policy/news/2010/07/privacy-lawsuit-targets-net-giants-over-zombie-cookies.ars.

106. *Id.*

107. Cheng, *supra* note 102.

108. *Id.*

109. Lance Whitney, *Consumer Groups: Online Tracking At 'Alarming Levels'*, CNET NEWS (May 4, 2010, 8:50 AM), http://news.cnet.com/8301-1009_3-20004071-83.html.

however, be damaging if "obtained by government agencies, private investigators, and others for purposes that go far beyond advertising."[110] Unclear data practices and frequent breaches of data security undermine consumer trust in an Internet economy.[111]

Because the Internet increasingly ferries vast amounts of sensitive information, such as medical or financial records, tracking all online activity represents more than just effective advertisement and increased revenue.[112] Tracking such detailed movement online implicates consumer "privacy, security and dignity."[113] Advertisers, however, have come to rely on this cornucopia of consumer data and attempting to end that reliance legislatively might be a losing battle.[114] Additionally, a complete end to behavioral tracking is not necessarily a desirable solution.[115] As was discussed above, advertisements pay for the Internet and consumers, generally, are interested in free services, content[116] and the convenience of a personal web cannot be understated.[117] Rather, a more practicable solution is establishing the rights of online consumers to be notified if their data is collected, to choose how much and what information to reveal, to be able to obtain a copy of their personal data or request that it be discarded, and to know how secure their data is when stored by websites and ad servers.[118]

Google, Inc. has responded to calls for a more "privacy-friendly service" by creating a single web page where users can see, and change, how Google tracks them along each of its services.[119] In a survey of public attitudes toward users' personal information, ninety percent of those polled agreed that there should be more laws protecting privacy.[120] Some companies like Cisco say that they only see what consumers allow.[121] While this state of affairs might seem to give the consumer power to expose private information, the user's inability to moderate retention and use of the information renders the power to expose meaningless.[122] International law must recognize and respond to this shift in Internet usage

110. *Id.*

111. Press Release, Viviane Reding Vice-President, European Comm'n & E.U. Justice Comm'r, Statement by Vice-President Reding on the European Parliament's Vote on the Voss Report (July 6, 2011), *available at* http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/11/489.

112. Whitney, *supra* note 109.

113. *Id.*

114. Story, *supra* note 29.

115. *See* Mills, *supra* note 31.

116. *Id*.

117. Jane Wakefield, *2010, The Year That Privacy Died?*, BBC NEWS (Dec. 31, 2010, 4:37 AM), http://www.bbc.co.uk/news/technology-12049153.

118. Whitney, *supra* note 109.

119. Wakefield, *supra* note 117.

120. Grove Insight, Ltd., *Findings from a Recent Poll on Internet Privacy and the Role of Congress*, GROVE INSIGHT, 2 (July 27, 2010), http://insidegoogle.com/wp-content/uploads/2010/07/ MemInternetPrivacy-0727101.pdf.

121. Wakefield, *supra* note 117.

122. *Id.*

because information is becoming the most important online commodity.[123] Leaving users' data to float on the free market in a state of nature is unlikely to foster an atmosphere where privacy is respected.[124] The general legislative *laissez-faire* attitude toward data privacy is turning around to bite the hand that has set it free with alarming frequency.[125]

III. EXISTING PRIVACY REGULATION IN THE UNITED STATES AND THE EUROPEAN UNION

An important step in creating meaningful and functional data privacy protections is to understand the landscape of existing legislation. This section presents a truncated history of data privacy legislation in the United States and the European Union. This Comment's ultimate goal suggests a unified solution that adequately reflects the legislative histories of both countries while providing sufficient data privacy protections for a new generation of commerce.

A. A Concept of Privacy on the Internet

The American concept of the individual "right to privacy," as separate from land ownership,[126] emerged over one hundred years ago.[127] In 1890, Samuel D. Warren and Louis D. Brandeis called it "the right to be let alone" in their seminal article *The Right to Privacy*.[128] The article was prompted by their frustrations concerning "intrusions into individual privacy by . . . the latest technological innovations."[129]

In 1990, the latest technological innovation was the "World Wide Web."[130] Low adoption and public use rates meant that the public was not concerned with their personal information being on the Internet because they either did not use the Internet or were unaware of its existence.[131] Twenty-one years later, however, consumers are increasingly concerned with securing important personal information.[132] In May 2011, the Pew Internet & American Life Project found that seventy-eight percent of American adults use the Internet regularly.[133]

123. *Id.*

124. *Id.*

125. *See id*.

126. Irwin R. Kramer, *The Birth of Privacy Law: A Century Since Warren and Brandeis*, 39 CATH. U. L. REV. 703, 705 (1990).

127. *See id.*

128. Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890).

129. Kramer, *supra* note 126, at 703.

130. *Internet Timeline: History of the Internet*, SANTA CLARA HIST. ASS'N, http://www.siliconvalleyhistorical.org/home/internet_timeline (last visited Oct. 24, 2011).

131. *See id.*

132. Whitney, *supra* note 109.

133. *Internet Adoption: 1995-2012*, PEW INTERNET & AM. LIFE PROJECT, http://www.pewinternet.

European Internet usage was even higher; in 2010 with seventy percent of households having Internet connections.[134] In the European Union today, seventy percent of citizens are concerned about the "misuse of their personal data" which includes use for online advertising.[135]

Where the United States has failed to promulgate meaningful data privacy legislation, the European Union has made it a priority.[136] The EU Justice Commissioner, Viviane Reding, has said that "[p]utting people back in control of their personal data is a priority" for the Commission.[137] The European Union is much more advanced, legislatively, in enacting significant data protection laws than its sister across the Atlantic.[138] In the United States there are "many privacy laws and some effective enforcement, but no comprehensive privacy law in the private sector."[139] It seems unlikely that there will be one soon.[140] Standards for private sector data privacy must be inferred from small pieces of disparate legislation, the common law, and the very absence of legislation in some sectors.[141]

B. Existing Privacy Regulation in the United States

While the public has adopted the Internet as a tool important to daily life, American policymakers have been slow to adapt and to promulgate specific legislation to protect the rights of Internet users.[142] The Electronic Communications Privacy Act ("ECPA"), promulgated in 1986, before the Internet reached beyond university campuses, is still the primary piece of legislation that affects data privacy on the Internet.[143] The ECPA is divided into three parts: the Wiretap Act,[144] the Pen Register Act,[145] and the Stored Communications Act ("SCA").[146]

org/Static-Pages/Trend-Data-%28Adults%29/Internet-Adoption.aspx (last visited July 8, 2012).

134. *Internet Usage in 2010: Households and Individuals*, EUROSTAT, 1 (2010), http://epp.eurostat.ec.europa.eu/cache/ITY_OFFPUB/KS-QA-10-050/EN/KS-QA-10-050-EN.PDF.

135. *Protection of Personal Data*, EUR. JUSTICE COMM'N, http://ec.europa.eu/justice/data-protection/index_en.htm (last visited Jan. 16, 2012).

136. Graham Greenleaf, *Global Data Privacy Laws: Forty Years of Acceleration* 3 (Privacy Laws & Bus. Int'l Report, No. 112, pp. 11-17, September 2011; UNSW Law Research Paper No. 2011-36), *available at* http://ssrn.com/abstract=1946700.

137. Press Release, Viviane Reding, Vice-President, Eur. Comm'n & E.U. Justice Comm'r,, *supra* note 111.

138. *See* Greenleaf, *supra* note 136, at 3.

139. Graham Greenleaf, *The Influence of European Data Privacy Standards Outside Europe: Implications for Globalisation of Convention 108,* 2 INT'L DATA PRIVACY L. 68, 70 (2012).

140. *Id.*

141. *Id.*

142. *See* Declan McCullagh, *Google, Facebook Go Retro in Push to Update 1986* Privacy Law, CNET NEWS (Oct. 21, 2011, 8:56 AM), http://news.cnet.com/8301-1009_3-20004071-83.html.

143. *Id.*

144. 18 U.S.C. §§ 2510-2522 (2008) (under 18 U.S.C. § 2511, interception and disclosure of wire, oral,

The Wiretap Act prohibits the intentional interception of any "wire, oral, or electronic communication,"[147] and the SCA protects information previously accessed and "stored" such as read e-mails.[148] The Wiretap Act includes an exemption for service providers.[149] Interception of wire or electronic communications can occur during "the normal course" of business "while engaged in any activity . . . necessary . . . to the rendition of . . . service"[150] as long as there is consent to the interception and it is without "criminal or tortious purpose."[151] The ECPA thus does not comprehensively regulate the private sector.[152] The collection of personal information in America by transacting parties is largely unregulated by law and the privacy of personal data left largely unprotected.[153]

The Computer Fraud and Abuse Act ("CFAA") prohibits a party from intentionally accessing a protected computer without authorization, knowingly causing "transmission of a program, information, code, or command," and as a result causing damage[154] to such a computer,[155] or accessing and obtaining "information from any protected computer if the conduct involved an interstate or foreign commerce."[156]

Courts have repeatedly held the ECPA and the CFAA do not apply to consensual transactions on the Internet because the data collection is intended for corporate use, or corporate-authorized access to marketers, in order to display ads to the individual about whom the information was collected.[157] Congress has not significantly revised the ECPA for over twenty-five years,[158] so the ECPA fails to reflect the increasing control and influence Internet entities have over personal data.[159] American legislation, as interpreted by the courts,[160] is focused on

or electronic communications is prohibited).

145. *Id.* §§ 3121-3127.

146. *Id.* §§ 2701-2711.

147. *Id.* § 2511(1)(a).

148. *See* Orin S. Kerr, *A User's Guide to the Stored Communications Act, and A Legislator's Guide to Amending It*, 72 GEO. WASH. L. REV. 1208, 1231 (2004).

149. Katherine A. Oyama, *E-Mail Privacy After United States v. Councilman: Legislative Options for Amending ECPA,* 21 BERKELEY TECH. L.J. 499, 507 (2006). ISPs receive absolute exemption regardless of purpose and thus have "total immunity from the primary surveillance law protecting stored communications." *Id.* at 508.

150. *Id.* at 507.

151. Chance v. Ave. A, Inc., 165 F. Supp. 2d 1153, 1162 (W.D. Wash. 2001).

152. Kang, *supra* note 22, at 1230.

153. *Id.*

154. 18 U.S.C. § 1030(a)(5)(A) (2008).

155. *Id.* § 1030(a)(5)(A)-(C).

156. *Id.* § 1030(a)(6).

157. *See generally In re* DoubleClick Inc. Privacy Litig., 154 F. Supp. 2d 497, 513 (S.D.N.Y. 2001).

158. Junichi P. Semitsu, *From Facebook to Mug Shot: How the Dearth of Social Networking Privacy Rights Revolutionized Online Government Surveillance*, 31 PACE L. REV. 291, 292 (2011).

159. Kang, *supra* note 22, at 1230.

protecting individuals from direct government interference and has left privacy regulation primarily to the free market[161] with the notable exception of children's data privacy.[162] The existing pieces of legislation are not coherent, but [163] rather a "patchwork of rules" that govern personal information based on content and when and where it was acquired.[164]

C. Proposed Privacy Regulation in the United States

Recently, the Department of Commerce, the Federal Trade Commission ("FTC"), and several lawmakers have discussed new legislation that would bring American privacy protection into the twenty-first century.[165] The FTC has the power to bring enforcement actions against unfair and deceptive trade practices and has negotiated consent decrees on privacy with both large and small companies.[166] As of July 3, 2012, there is no comprehensive data privacy law that provides guidance and security to Congress, the FTC, businesses, or users; although there appears to be some momentum in developing just such a law.[167]

Jackie Speier, a California Representative, has attempted to introduce such comprehensive legislation.[168] The "Do Not Track Me Online Act" would require the FTC to promulgate regulations establishing "standards for the required use of

160. *See generally id.*

161. *See* Titiriga, *supra* note 48, at 5.

162. The striking exception to the absence of legislation on data privacy generally is Congress' effort to protect children under the age of thirteen from data collection efforts directed at children. Children's Online Privacy Protection Act, 15 U.S.C.A. §§ 6501-6506 (West 1998). The Children's Online Privacy Protection Act ("COPPA") of 1998, enacted in 2000, is the only legislation on the books that purports to protect data privacy but it protects only the data privacy of young children for the primary purpose of protecting children from pornography and abuse. *Id*. Since, however, most Internet users are over thirteen, this legislation does not address the bulk of privacy issues raised by the prevalence of the Internet and behavioral tracking for advertising. *Id*. Under COPPA, it is "unlawful for any operator of a website or online service directed to children [age 12 or younger], or any operator that has actual knowledge that it is collecting or maintaining personal information from a child, to collect personal information from a child in a manner that violates the regulations prescribed under this part." *Id.* at § 312.3. For more information on COPPA, see Laurel Jamtgaard, *Big Bird Meets Big Brother: A Look at the Children's Online Privacy Protection Act*, 16 SANTA CLARA COMPUTER & HIGH TECH. L.J. 385 (2000) and Nancy L. Savitt, *A Synopsis of the Children's Online Privacy Protection Act*, 16 ST. JOHN'S J. LEGAL COMMENT. 631 (2002).

163. Titiriga, *supra* note 48, at 5.

164. *Id.; see* Greenleaf, *supra* note 136, at 3.

165. *See* DEP'T OF COMMERCE, COMMERCIAL DATA PRIVACY AND INNOVATION IN THE INTERNET ECONOMY: A DYNAMIC POLICY FRAMEWORK (2010), *available at* www.ntia.doc.gov/reports/2010/IPTF_Privacy_GreenPaper_12162010.pdf.

166. *Consumer Protection*, FED. TRADE COMM'N, http://www.ftc.gov/bcp/index.shtml (last visited June 3, 2012).

167. *See* Titiriga, *supra* note 48, at 5; Do Not Track Me Online Act, H.R. 654, 112th Cong. (2011), *available at* http://thomas.loc.gov/cgi-bin/query/z?c112:H.R.654; *Consumer Data Privacy In a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy*, THE WHITE HOUSE, http://www.whitehouse.gov/sites/default/files/privacy-final.pdf (last visited July 3, 2012).

168. H.R. 654, 112th Cong. (2011).

an online opt-out mechanism to allow a consumer to prohibit the collection or use of any covered information and to require a covered entity to respect the choice of such consumer to opt-out of such collection or use."[169] The bill applies only to those persons "engaged in interstate commerce that collects or stores online data containing covered information."[170] "Covered information" is defined with respect to an individual to include "[t]he online activity of the individual," any substantially unique identifier such as the IP address, and personal information.[171] "Online activity" includes the websites, content accessed, and the time, date, and geolocation of access.[172] It also includes the computer and "means by which online information was accessed, such as a device, browser, or application."[173] The proposed Act also calls for the FTC to promulgate regulations requiring disclosure of information collection practices and provide for enforcement by a state's Attorney General in the form of a civil action to obtain injunctive and punitive relief.[174]

The "Do Not Track Me Online Act" has been referred to the House Committee on Energy and Commerce and subsequently to the Subcommittee on Commerce, Manufacturing, and Trade.[175] It is currently in referral and has not yet been enacted, thus, any protection it may have afforded those concerned about the privacy of information collected for behavioral advertising is moot.[176] Congress' response to privacy protection, apart from un-enacted legislation currently stewing in committee, has been to negotiate one-on-one with industry giants, rather than acting to create innovative laws that protect users' data from both law-abiding companies and outlaw hackers.[177]

On February 2, 2012, Google was called before a congressional subcommittee to discuss its privacy policy.[178] The hearing was the consequence of an investigation into Google's amended privacy policy that debuted January 24, 2012.[179] The new privacy policy,[180] effective March 1, 2012, purports to "use

169. *Id.* § 3(a).

170. *Id.* § 2(2).

171. *Id.* § 2(3)(A)(i). "Personal information includes the standards: name, address, phone number, email address, and financial account or government-issued identification number." *Id.* § 2(3)(A)(iii)(I)-(VI).

172. *Id.* § 2(3)(A)(i)(I)-(III).

173. *Id.* § 2(3)(A)(i)(III), (IV).

174. *Id.* §§ 3-5. The punitive relief is capped, however, at $5,000,000 for any "related series of violations of the prescribed regulations. *Id.* at § 5(b)(3).

175. *Id.*

176. *Id.*

177. *A Golf Clap for the FTC and Facebook*, NET CHOICE (Nov. 28, 2011), http://www.netchoice. org/a-golf-clap-for-the-ftc-and-facebook/. Net Choice is "a coalition of trade associations, eCommerce businesses, and online consumers, all of whom share the goal of promoting convenience, choice and commerce on the Net." *Id.* Among NetChoice's members are Facebook, eBay, Yahoo!, and NewsCorp. *Id.*

178. Lance Whitney, *Google's Response on New Privacy Policy Ticks Off Congresswoman*, CNET NEWS (Feb. 3, 2012, 8:29 AM), http://news.cnet.com/8301-13578_3-57371165-38/googles-response-on-new-privacy-policy-ticks-off-congresswoman/.

179. Declan McCullagh, *Politicians Aim Some Pointed Privacy Questions at Google*, CNET NEWS (Jan.

information across multiple services to provide enhanced services and ads."[181] The bulk of the political questions asked as a result of the announcement of the new privacy policy were regarding what the search giant is doing to self-regulate.[182] California Representative Jackie Speier and seven other members of Congress penned a letter to Larry Page, CEO of Google, in which they expressed a belief "that consumers should have the ability to opt-out of data collection when they are not comfortable with a company's terms of service and that the ability to exercise that choice should be simple and straightforward."[183]While some governmental protection of individual privacy is better than none, the United States' legislative answer to data privacy security concerns has thus far been limited to individualized congressional hearings.[184] The seven representatives who signed the letter to Larry Page censured Google for making such alarming changes[185] to its privacy policies.[186] The representatives pointed to Google's status as an Internet giant and highlighted its responsibility to protect user privacy.[187] This letter exemplifies the legislative model that is little more than industry self-regulation punctuated by theatrical public hearings.[188]

On February 23, 2012, U.S. President Barak Obama unveiled a "Consumer Privacy Bill of Rights" as part of a report entitled "A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy."[189] This

26, 2012, 2:02 PM), http://news.cnet.com/8301-31921_3-57367059-281/politicians-aim-some-pointed-privacy-questions-at-google/?tag=mncol;txt.

180. *Policies and Principles: FAQ*, GOOGLE, http://www.google.com/policies/faq/ (last visited Feb. 17, 2012).

181. Elinor Mills, *Google Wants Ability to 'Combine' Your User Data*, CNET NEWS (Jan. 24, 2012, 2:57 PM), http://news.cnet.com/8301-31921_3-57365195-281/google-wants-ability-to-combine-your-user-data/.

182. *See* McCullagh, *supra* note 179.

183. Letter from Cliff Stearns, Henry Waxman, Joe Barton, Edward J. Markey, Marsha Blackburn, Dianne DeGette, G.K. Butterfield & Jackie Speier, Representatives, U.S. Cong., to Larry Page, Chief Exec. Officer, Google 1 (Jan. 26, 2012) (http://democrats.energycommerce.house.gov/sites/default/files/documents/Letter_Google_01.26.12.pdf); *see* McCullagh, *supra* note 179.

184. *See, e.g.*, Letter from Cliff Stearns et al. to Larry Page, *supra* note 183, at 1.

185. Google says very little has changed in their privacy policy as a result of the announcement. Google claims that the policy change clarifies and simplifies their data collection across multiple services. The policy statement was meant to explain how and when Google uses collected data to "refine and improve" the Google experience and to increase transparency in collection practices and to allow users greater control over their data. Betsy Masiello, *Setting the Record Straight About Our Privacy Policy Changes*, GOOGLE PUB. POL'Y BLOG (Jan. 26, 2012, 5:54 PM), http://googlepublicpolicy.blogspot.com/2012/01/setting-record-straight-about-our.html.

186. Letter from Cliff Stearns et al. to Larry Page, *supra* note 183, at 2.

187. *Id.*

188. Juliana Gruenwald, *Privacy Groups Hoping Study Prompts Action*, NAT'L J. (Oct. 11, 2011, 3:34 PM), http://www.nationaljournal.com/tech/privacy-groups-hoping-study-prompts-action-20111011.

189. Press Release, The White House, We Can't Wait: Obama Administration Unveils Blueprint for a "Privacy Bill of Rights" to Protect Consumers Online (Feb. 23, 2012), *available at* http://www.whitehouse.gov/the-press-office/2012/02/23/we-can-t-wait-obama-administration-unveils-blueprint-privacy-bill-rights.

"privacy blueprint"[190] acknowledges that the framework proposed "is just a beginning" but dedicates the Administration's resources to "encourage stakeholders, including the private sector, to implement the Consumer Privacy Bill of Rights."[191] Although the report does not detail how data privacy policies should be implemented or enforced, the Administration's press release accompanying the report does state as a central premise that "[c]onsumers have a right to exercise control over what personal data organizations collect from them and how they use it."[192] The Consumer Privacy Bill of Rights provides a "baseline of clear protections for consumers and greater certainty for businesses."[193] It identifies six rights that consumers hold with respect to their data: (1) transparency,[194] (2) respect for context,[195] (3) security,[196] (4) access and accuracy,[197] (5) focused collection,[198] and (6) accountability.[199]

The Consumer Privacy Bill of Rights is only one-fourth of the privacy protection package suggested by the White House.[200] Other provisions included were a stakeholder-solicitation process to develop rules governing rights in specific business contexts, FTC enforcement measures, and "greater interoperability" between the privacy frameworks of the United States and "our international partners."[201] The report, however, does not propose a method for implementing the privacy protections espoused in the Consumer Privacy Bill of Rights.[202] The plan relies on "multistakeholder processes," a phrase that means input from working groups formed of members of industry, academia, and law enforcement.[203] These multistakeholder processes would eventually culminate in a voluntary "code of conduct," adoptable by individual companies and

190. *Id.*

191. *Consumer Data Privacy In a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy*, *supra* note 167.

192. Press Release, The White House, *supra* note 189.

193. *Id.*

194. "Consumers have a right to easily understandable information about privacy and security practices." *Id.*

195. "Consumers have a right to expect that organizations will collect, use, and disclose personal data in ways that are consistent with the context in which consumers provide the data." *Id.*

196. "Consumers have a right to secure and responsible handling of personal data." *Id.*

197. "Consumers have a right to access and correct personal data in usable formats, in a manner that is appropriate to the sensitivity of the data and the risk of adverse consequences to consumers if the data are inaccurate." *Id.*

198. "Consumers have a right to reasonable limits on the personal data that companies collect and retain." *Id.*

199. "Consumers have a right to have personal data handled by companies with appropriate measures in place to assure they adhere to the Consumer Privacy Bill of Rights." *Id.*

200. *Id.*

201. *Id.*

202. *See Consumer Data Privacy In a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy*, *supra* note 167, at 23-27.

203. *Id.* at 23-24.

enforceable piecemeal by the FTC under its authority to prosecute deceptive acts or practices.[204]

The White House proposal acknowledges that the United States lacks comprehensive legislation enforced by a competent department of the Executive.[205] Instead, Internet privacy policy and data collection practices are defined by a self-interested industry[206] built on the profit margins of advertising.[207] The White House's proposal is not law, however, and merely functions as a call to legislate.[208]

D. Privacy Regulation in the European Union

While American data privacy legislation has lagged,[209] European legislators have taken a more involved role.[210] European legislation protects the user from invasion, by any person or entity, of the individual "right to privacy."[211] In 1973, Sweden enacted the first comprehensive national data privacy law with the Data Privacy Act.[212] In the 1980's, the Council of Europe began to consider measures for member states to adopt.[213] In 1981, the Council of Europe opened the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data ("Convention 108") for signature.[214] By 1995, most member states had signed or acceded to Convention 108 and it produced the EU Directive on Data Protection ("Directive").[215] The Directive commanded that

204. The enforcement power is found at Section 5 of the FTC Act and is codified at 15 U.S.C. Section 45. *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy*, *supra* note 167, at 27.

205. "Consumers have a right to expect that organizations will collect, use, and disclose personal data in ways that are consistent with the context in which consumers provide the data." *See* Press Release, The White House*, supra* note 189.

206. U.S. law includes "narrowly targeted privacy laws aimed at specific sectors such as finance and health" but does not address enough. Juliana Gruenwald, *U.S. Firms Wary of EU's Proposed Privacy Changes*, INSIDE GOOGLE (Jan. 25, 2012, 10:15 AM), http://insidegoogle.com/2012/01/u-s-firms-wary-of-eus-proposed-privacy-changes/.

207. *See, e.g.*, John M. Simpson, *Is Google Adding a Default Security Setting?*, INSIDE GOOGLE (Aug. 9, 2011, 4:44 PM), http://insidegoogle.com/2011/08/is-google-adding-a-default-security-setting/.

208. *See Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy*, *supra* note 167, at 35.

209. *See* McCullagh, *supra* note 142.

210. Titiriga*, supra* note 48, at 5.

211. *Id.*

212. Greenleaf, *supra* note 138, at 1.

213. *Id.* at 3.

214. *Council of Europe Privacy Convention*, ELEC. PRIVACY INFO. CTR., http://epic.org/privacy/intl/coeconvention/ (last visited Jan. 16, 2012).

215. Though Turkey signed the Convention it has never acceded to the Convention. San Marino has neither signed nor acceded to the Convention. Though Bulgaria was a member in 1995 it did not assign the Convention until 1998. Malta signed the Convention in 2003 and Poland in 1999. Only Turkey, San Marino, and Russia have not entered the Convention into force as of August 25, 2012. *Status of the Convention for the*

each of the member nations create both conforming privacy laws and a Data Protection Authority to protect and investigate attacks against citizens' privacy.[216] The "Article 29 Directive" establishes a "Working Party on the Protection of Individuals with regard to the Processing of Personal Data."[217] Since accession, several Protocols have been added to Convention 108 in order to refine and develop the law.[218] In 2008, the Council of Europe announced its desire that Convention 108 and its Optional Protocol become global agreements that would be adopted by many nations.[219] Worldwide, seventy-six countries have enacted data privacy laws,[220] and many have modeled their laws on the European approach contained in Convention 108 and its outgrowth, the Data Protection Directive of 1995.[221] The Data Protection Directive of 1995 is the "most influential international instrument" on data privacy.[222] Continuing to be a model for other countries, in March 2012, the European Union hosted a conference in Washington D.C. designed to reinforce transatlantic dialogue between the European Union and the United States.[223]

E. Proposed Privacy Regulation in the European Union

Efforts to refine privacy legislation, for the European Union itself, with respect to the collection of personal data continue.[224] On January 25, 2012, the European Commission proposed to reform the 1995 rules in order to strengthen

Protection of Individuals with regard to Automatic Processing of Personal Data

CETS No.: 108, COUNCIL OF EUR., http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=108&CM=&DF=&CL=EN (last visited Aug. 24, 2012) *Data Protection Day*, COUNCIL OF EUR., http://www.coe.int/t/dghl/standardsetting/dataprotection/Data_protection_day_en.asp (last visited July 24, 2012); COMM. ON CULTURE, SCI. & EDUC., PROTECTION OF PRIVACY AND PERSONAL DATA ON THE INTERNET AND ONLINE MEDIA 2, 9-10 (2011), *available at* http://www.assembly.coe.int/CommitteeDocs/2011/RihterviepriveeE.pdf; Press Release, Council of Eur., Data Protection Day: Guaranteeing Individuals' Privacy Rights (Jan. 28, 2011) (on file with author), *available at* https://wcd.coe.int/ViewDoc.jsp?id=1738201.

216. Titiriga*, supra* note 48, at 5.

217. Directive 95/46/EC, of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, art. 29, 1995 O.J. (L 281) 31, 50, *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML.

218. *See* Greenleaf, *supra* note 138, at 7.

219. *Id.*

220. *Id.* at 1.

221. *Id.* at 3.

222. Graham Greenleaf, *Global Data Privacy Laws: 89 Countries, and Accelerating* 6 (Queen Mary Univ. of London, Sch. of Law, Legal Studies Research Paper No. 98/2012), *available at* http://ssrn.com/abstract=2000034. In fact, non-European countries can obtain a "decision that their laws provide an 'adequate' level of protection of privacy." This decision allows personal information (user data) collected inside the E.U. to "flow" to "organisations in… [other] countries." *Id.*

223. *EU Conference: Privacy and Protection of Personal Data,* EUR. JUSTICE COMM'N, http://ec.europa.eu/justice/events/eu-us-data/index.html (last visited July 8, 2012).

224. *See id.*

privacy rights, boost the digital economy, and modernize the Data Protection Directive.[225] The press release recognized that the Internet knows no geographic borders.[226] The release pointed out that Article 8 of the EU Charter of Fundamental Rights provides the "right to personal data protection in all aspects of life," including while shopping.[227] The announcement was accompanied by a regulation establishing a general EU framework for data collected and used in criminal investigations.[228]

The proposed rules will save businesses operating in the European Union an estimated 2.3 billion euros per year.[229] The savings is accomplished through eliminating paperwork and bureaucracy and increasing self-reporting duties such as mandatory reporting of serious security breaches within twenty-four hours.[230] Additionally, the rules call for user transferability, or a right to data portability, of data from one service provider to another and a power to demand the data be deleted, a "right to be forgotten."[231]

It is important to note that the rules have not been adopted and they are only proposals up for discussion.[232] But even if the proposals are adopted by the member states, the new regulation would take effect two years after adoption.[233]

IV. PROPOSED UNIFORM BROWSER-LEVEL OPT-IN SOLUTION

Privacy policy begins with the individual user. Generally, the individual user is not in a position to make decisions about personal data because of the technical and abstract nature of data collection.[234] In the online behavioral advertising paradigm an individual user shares a bit of information about herself. Sharing may be inadvertent or by conscious choice.[235] Yet some proposals, such as a measure passed recently in the Netherlands, for a new model of data privacy

225. Press Release, Eur. Justice Comm'n, Commission Proposes a Comprehensive Reform of Data Protection Rules to Increase Users' Control of Their Data and To Cut Costs for Businesses (Jan. 25, 2012) (on file with author), *available at* http://europa.eu/rapid/pressReleasesAction.do?reference=IP/12/46&format=HTML&aged=0.

226. *Id.*

227. *Id.*

228. *Id.*

229. *Id.*

230. *Id.*

231. *Id.*

232. *Id.*

233. *Id.;* On July 1, 2012, the Article 29 Working Party adopted a new Opinion in which it states that cloud service providers will be subject to the EU Data Protection Directive. *Article 29 Data Protection Working Party: Opinion 05/2012 on Cloud Computing,* EUR. JUSTICE COMM'N (Jan. 25, 2012), http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf.

234. *See* Omar Tene & Jules Polonetsky, *Privacy in the Age of Big Data: A Time for Big Decisions*, 64 STAN. L. REV. ONLINE 63, 67 (2012), *available at* http://www.stanfordlawreview.org/online/privacy-paradox/big-data.

235. *Id.* at 64.

control hold explicit consent out as the Holy Grail of privacy protection.[236] Not all non-consensual sharing is bad[237] and not all data should be treated as personal.[238] In order to create a functional data protection framework, the scope of protected data should be clearly defined.[239] But the possible outcomes and consequences for "data flow" and individual privacy are just beginning to be discussed.[240]

A trans-Atlantic solution to data privacy protection is desirable for businesses and users whose Internet commerce transverses geographical boundaries billions of times each day.[241] It is also desirable for governments on both sides of the Atlantic because they have a common problem: *how* to effectively protect individual data privacy.[242] Legislative resources and diverse experience with failed and successful privacy protection measures can lead to more comprehensive and uniform law, uniformity that would be good for businesses that are unsure of how to comply with differing standards across their Internet holdings.[243] This would mean that companies who benefit from transnational Internet traffic could implement one set of privacy policies and meet all international requirements.[244] A uniform system could save companies a

236. *See Dutch Politicians Vote To Implement Opt-In For All Third Party Cookie Tracking, As Digital Media Companies Consider Their Next Move*, EXCHANGE WIRE (June 22, 2011), http://www.exchangewire.com/blog/2011/06/22/dutch-politicians-vote-to-implement-opt-in-for-all-third-party-cookie-tracking-as-digital-media-companies-consider-their-next-move/; *IAB Europe Urges EU Member States to Consider Negative Impact of an Overly Strict Consent for Cookies*, INT'L ADVERTISING BUREAU EUR., http://www.iabeurope.eu/news/iab-europe-urges-eu-member-states-to-consider-negative-impact-of-an-overly-strict-consent-for-cookies.aspx (last visited Feb. 18, 2012); A FUTURE EUROPEAN NEW SITE UNDER THE WRONGFUL TRANSPOSITION OF THE LAW, http://www.cookiedemosite.eu/ (last visited Feb. 18, 2012) (click on "Experience an Overly Strict Law Now").

237. *See* Tene & Polonetsky, *supra* note 234, at 64.

238. *Id.*

239. *Id.* at 63, 66.

240. *Id.*

241. *See How Will the EU's Data Protection Reform Make International Cooperation Easier?,* EUR. JUSTICE COMM'N (Jan. 25, 2012), http://ec.europa.eu/justice/data-protection/document/review2012/factsheets/5_en.pdf. On March 19, 2012, the European Union and the United States held a joint tele-conference in Washington D.C. and Brussels. *EU Conference: Privacy and Protection of Personal Data*, *supra* note 223. The teleconference "provided a forum for US [sic] and EU stakeholders from public and private sectors to obtain comprehensive, accurate and up-to-date information on EU data protection principles and the ongoing reform, and to discuss US [sic] and EU perspectives focusing on commercial privacy." *Id.* U.S. Secretary of Commerce John Bryson and European Commission Vice-President Viviane Reding issued a joint statement on data protection that same day. *See* Press Release, Europa, EU-U.S. Joint Statement on Data Protection by European Commission Vice-President Viviane Reding and U.S. Secretary of Commerce John Bryson, (Mar. 19, 2012) (on file with author), *available at* http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/12/192. The Press Release noted that "The European Union and the United States are global leaders in protecting individual freedoms, including privacy, while at the same time fostering innovation and trade that are so critical to the world economy." *Id.*

242. *See generally* Greenleaf, *supra* note 136.

243. *How Will the EU's Data Protection Reform Simplify the Existing Rules?*, *supra* note 241.

244. U.S. firms are concerned that the European Union's proposed privacy changes "could be costly for them to comply with and may hamper innovation." Gruenwald, *supra* note 206; *but see How Will the EU's Data Protection Reform Simplify the Existing Rules?*, *supra* note 241.

good deal of money in consulting and legal fees.[245] A uniform system, well-researched and with an eye on protecting companies' revenue streams and the individual whose data flows into those streams, is the solution.

This Comment proposes that a trans-Atlantic uniform system, legislated and implemented by the United States and the European Union in tandem, is the most efficient method of protecting data privacy in the context of online behavioral advertising. This uniform system would be communicated to the user at the browser-level with an opt-in mechanism.

Data retention policies, clearly communicated to the user, should be written to provide clear and concise levels of protection to different kinds of information based on the information's sensitivity and possibility of deanonymization.[246] There should also be a "right to be forgotten," that is, a right to revoke consent to use or retain information, circumscribed only by contract and equity principles and technological limitations.[247]

Data policies should be enforced against first *and* third-party aggregators.[248] First-party aggregators, the websites users believe are receiving their information, should have a duty to disclose to whom a user's information will be disclosed, for what purposes, and for how long it will be retained by the third-party.[249] There should be accessible civil remedies, damages and equitable relief, for breaches of privacy policies.[250]

A. Why at the Browser-Level?

Currently, browser-level data control options are limited and industry-defined.[251] Until very recently,[252] what was offered to and understood by the majority of users rarely extended beyond clearing out the browser cache or

245. Gruenwald, *supra* note 206; *but see How Will the EU's Data Protection Reform Simplify the Existing Rules?*, *supra* note 241.

246. *See* Ohm, *supra* note 64, at 1701.

247. *See* Press Release, Eur. Justice Comm'n, *supra* note 225.

248. *See* Krishnamurthy, Naryshkin, & Willis, *supra* note 71.

249. *Id.*

250. *See* H.R. 654, 112th Cong. §§ 3-5 (2011), *available at* http://thomas.loc.gov/cgi-bin/query/z?c112:H.R.654.IH:.

251. These options, including "covert browsing" and greater clarity in system defaults, are expanding rapidly but are still limited by the individual efforts of competing browser providers. *See, e.g.*, Rainey Reitman, *Mozilla Leads the Way on Do Not Track*, ELEC. FRONTIER FOUND. (Jan. 24, 2011), https://www.eff.org/ deeplinks/2011/01/mozilla-leads-the-way-on-do-not-track; Leslie Meredith *Rethinking Browsers: Add-ons Make the Difference*, TECH NEWS DAILY (Feb. 16, 2012, 2:39 PM), http://www.technewsdaily.com/3821-rethinking-browsers-add-ons-difference.html; Tom Krazit, *Google's Chrome Browser Gets Do-not-track Feature*, CNET NEWS (Jan. 24, 2011, 10:38 PM), http://news.cnet. com/8301-30684_3-20029348-265.html; *Do Not Track FAQ*, MOZILLA, http://dnt.mozilla.org/ (last visited Feb. 18, 2012).

252. These options began appearing in updated browser offerings around 2011. *See supra* note 251 and accompanying text.

turning off and deleting cookies.[253] The browser is also the portal for accessing the Internet. The average user cannot access the Internet without a browser and it is the one user-constant in the browsing experience. The average non-technical user sees only the browser as she shops, reads, or watches on the Internet. The user does not see ISPs, DNS servers, or cloud servers.[254] In order to provide the user the best information of what data privacy entails, specifically what she is sacrificing when she accepts the privacy policy of a website, it is necessary to present the pertinent information where she would expect to find it. Protecting data privacy begins with the individual and should meet the user in the liminal space between user and Internet, wherever the user is located.

Browsers are transnational.[255] Apple's Safari, Google's Chrome, Mozilla's Firefox, and Microsoft's Internet Explorer, among others, are localized in dozens of countries.[256] Servers, cloud or otherwise, may be located in one country but accessed in another, precluding territorial management of data practices.[257] The transnational nature of the Internet means that any successful plan needs to be implemented at a level where all countries have equal access.[258] Because browser options are rather limited and all companies are effectively doing business in any country in which their browser is localized, the browser-providers are more easily subject to the laws of the country in which they operate.[259] These companies are already regulated in multiple countries or have offices and operations subject to EU or U.S. law.[260]

However, the browser should not be the only level of protection afforded to data because the browser-based blocking mechanisms cannot protect against "leakage" by visited websites to third-party advertisers.[261] While the mechanism for selecting a level of data privacy control should be implemented at the browser level, the law must require transparency in data collection practices from first-party websites.[262] This means requiring first-party websites to disclose data

253. *See* Seth Rosenblatt, *Does Your Browser Feed the Cookie Monster--Or Starve It?*, CNET NEWS (Feb. 18, 2012, 4:00 PM), http://download.cnet.com/8301-2007_4-57380680-12/does-your-browser-feed-the-cookie-monster-or-starve-it/.

254. *See* Reitman, *supra* note 251.

255. *See, e.g.*, GOOGLE CHROME, https://www.google.com/chrome (last visited Feb. 19, 2012).

256. *See, e.g.*, *Safari Features,* APPLE, http://www.apple.com/safari/features.html#international (last visited Feb. 18, 2012); GOOGLE CHROME, *supra* note 255 (click on the "Select a language" drop down menu to see a list of approximately forty-eight available languages); *Download a Firefox That Speaks Your Language,* MOZILLA, http://www.mozilla.org/en-US/firefox/all.html (last visited Feb. 18, 2012); *Internet Explorer 9 Now Available in 93 Languages*, IE BLOG (May 25, 2011, 2:10 PM), http://blogs.msdn.com/b/ie/archive/2011/05/25/internet-explorer-9-now-available-in-93-languages.aspx.

257. *How Will the EU's Data Protection Reform Simplify the Existing Rules?, supra* note 241.

258. *Id.*

259. *Id.*

260. *See Why Do We Need an EU Data Protection Reform?,* EUR. JUSTICE COMM'N (Jan. 25, 2012), http://ec.europa.eu/justice/data-protection/document/review2012/factsheets/1_en.pdf.

261. *See* Krishnamurthy, Naryshkin, & Willis, *supra* note 71.

262. *Id.*

retention policies in contracts with aggregators to whom they sell data.[263] The browser-providers are not in a position to monitor or enforce data privacy controls on first-party websites, and this proposal does not suggest they be required to do so.[264] Rather, browsers should be programmed in a manner that makes it clear to the user when transactions for private information are taking place and when such information is being communicated. Browsers should provide mechanisms to control the *covert access* that first-party websites or third-party aggregators, regardless of legitimacy, have to the user. This concept is already being put into place by browser providers but should be subject to a technologically-adaptable framework for ensuring that users are adequately protected regardless of their browser choice.[265]

B. Why Opt-In?

Browsers and first-party websites have an advantage over the user in asserting their desired system preferences because few users are technologically savvy enough to modify browser preferences.[266] Users are inclined, cognitively, to accept the default.[267] The default provisions, after all, represent the informed choices of persons with superior computer-related knowledge. The defaults are designed by expert programmers, whom users are inclined to trust because of their superior knowledge. The availability of an opt-in button or preference pane, without more, does not provide adequate security for the user.[268]

It is important that legislators take into account varying levels of privacy afforded to different kinds of information. Information less central to advertising and more sensitive, that is prone to deanonymization, should be controlled separately. The user should be able to see not just that a website or third-party *is* collecting information, but *what* information is being collected.[269]

A default profile could be baked into the browser. The default profile would give away exactly the information the user feels comfortable with and no more. When a visited website wishes to use information available in the profile, the

263. *Id.*

264. *See generally* Tene & Polonetsky, *supra* note 234.

265. *See, e.g.*, *Safari Features, supra* note 256; *Incognito Mode: Browse in Private,* GOOGLE CHROME, http://support.google.com/chrome/bin/answer.py?hl=en&answer=95464 (last visited Feb. 19, 2012); *Private Browsing*, FIREFOX HELP, http://support.mozilla.org/en-US/kb/Private-Browsing (last visited Feb. 19, 2012); *InPrivate Browsing*, MICROSOFT WINDOWS, http://windows.microsoft.com/en-US/internet-explorer/products/ie-9/features/in-private (last visited Feb. 19, 2012).

266. *See* Tene & Polonetsky, *supra* note 234.

267. *Id.*

268. Scientists "have shown that, simply by providing users a *feeling* of control, businesses encourage the sharing of data, regardless of whether or not a user has actually gained control." *Id.*

269. The fact that a website knows a user's dog's name is Spot might not be as upsetting to a sense of privacy and safety as knowing the website and its market affiliates, know her social security number and mother's maiden name.

user is prompted for approval and can select which fields may be automatically populated and for how long the information can be retained. For example, while visiting a shoe website the user allows the site to remember shoe size so that all shoes presented on the site are the user's size.

The default profile would function like a cookie, only the website cannot store types of information the user does not allow. The default profile would be a wall through which the website could not reach without explicit authorization. To facilitate interaction with websites the user accesses daily, time limits could be set on the access to the data. For example, the user gives authorization to use the shoe size information for two months after which the right to store and use the data expires and the user must be prompted again for permission. Certain trusted websites could be given permanent access to certain information. For example, Yahoo! Weather could always be permitted to see the user's zip code to more conveniently present the user with the most relevant forecast. The most important aspect of the proposal is that the opt-in must be clear and comprehensive and the opt-in choice must be respected by browser-providers and first-party websites and third-party aggregators.

Respecting a user's choice to opt-in would also entail respecting a subsequent opt-out. Users must have the right to revoke consent, to revoke the opt-in, at any time.[270] Revoking the opt-in would prevent future tracking and require that collected data be destroyed.[271] The right should be limited only as far as technology will allow.[272] Revocation would trigger the "right to be forgotten" and bind the first-party and any third-parties with whom the first-party has contracted to sell or manage the gathered information.[273] The "right to be forgotten," first presented in the recent EU proposal for updating EU privacy law, must be enforced and protected as far as technologically and economically possible.[274] While the cost for respecting the opt-in and subsequent opt-out of a user will not be insignificant, it is important to maintain consumer confidence in the Internet.

V. CONCLUSION

Going into 2012, national governments across the globe are struggling with how to balance innovation and the rapid evolution of information technology with the persistent demand for user control.[275] Personal information is a resource

270. *See* Press Release, Eur. Justice Comm'n, *supra* note 225.

271. *See generally id.* The data should be destroyed unless the website has contractually negotiated a right to continuing using it. This requires a separate bargaining power in contract discussion that is outside the scope of this paper.

272. *See generally id.*

273. *Id.*

274. *Id.*

275. *See* Press Release, Eur. Justice Comm'n, *supra* note 225.

over which third-party advertisers, first-party websites, and the users themselves want some measure of control.[276] Finding a balance between competing interests is complicated and requires the intervention of disinterested parties who have no financial stake in the level of protection afforded to the individual's data privacy. This means that a comprehensive program of legislation enforced and monitored by competent government agencies is necessary. And the transnational nature of the businesses and consumers engaged in Internet commerce demands that the solution recognize that borders do not make for good Internet policy.[277]

In 2009, privacy expert Daniel Solove reported that U.S. Supreme Court Justice Antonin Scalia said he was "untroubled by internet tracking" and felt it was "not offensive" because what he bought was not a secret unless it was shameful.[278] In response, a Fordham University law professor, Joel Reidenberg, assigned his privacy law class to compile a dossier of personal information on Justice Scalia, culled entirely from sources available to the public.[279] The dossier was fifteen pages long and included Justice Scalia's home phone number, a list of his favorite movies and food, and his wife's personal email address.[280] Though he is a public figure, and a good amount of the information was pulled from published interviews and articles, Justice Scalia was *offended* by the compilation of the data.[281] Public figures and celebrities are not the only ones who have to worry about the aggregation of personal data. A quick search of a publicly-available directory will reveal a disturbingly accurate and detailed profile about most users.[282]

The invasion of privacy, bit by byte, seems innocuous when a user is alone in front of a computer. Users have a false sense of intimacy when communicating through their computers.[283] They may be alone in the room or the house where they access the internet. They feel a sense of anonymity when browsing the web in a coffee shop where no one knows them.[284] This method, solitude, of keeping things private is ineffective in the digital age where even reading a book requires

276. *See* Gruenwald, *supra* note 188.

277. *See* Press Release, Eur. Justice Comm'n, *supra* note 225.

278. Daniel Solove, *Justice Scalia's Conception of Privacy*, CONCURRING OPINIONS (Jan. 29, 2009, 1:36 AM), http://www.concurringopinions.com/archives/2009/01/justice_scalias_1.html. *See also* Kashmir Hill, *What Fordham Knows About Justice Scalia*, ABOVE THE L. (Apr. 22, 2009, 5:30 PM), http://above thelaw.com/2009/04/what-fordham-knows-about-justice-scalia/.

279. Hill, *supra* note 278.

280. *Id.*

281. Jonathan Turley, *Scalia Slams Fordham Law Professor for Privacy Invasion*, RES IPSA LOQUITUR (Jul. 7, 2012, 6:46 PM), http://jonathanturley.org/2009/04/30/scalia-slams-fordham-law-professor-for-privacy-invasion/.

282. *See, e.g.*, *Find People,* WHITE PAGES, http://www.whitepages.com/person (last visited Feb. 18, 2012).

283. *See* Angwin, *supra* note 56.

284. *Id.*

servers, networks, cloud storage, and satellites scattered around the globe.[285] Even the idea that a person or company may know *something* about a user is not the same as realizing *how much* they know. Nor is it the same as seeing that information complied in a dossier.

Online behavioral advertising is disturbing to the user because she sees her activities, her thoughts, her desires, projected back at her. The illusion of privacy and anonymity is shattered. And the feeling of being watched and catalogued is unnerving.[286] The computer remembers things the user has done that she cannot remember and will not forget things she wants forgotten.[287] Her personal interaction with her computer and the Internet is personalized *for* her but not *by* her. And she may not like being confined on the Internet by the choices she has made. Modern (Western) society sees the Internet as a free space where physical boundaries are meaningless and anonymity allows the user to be anything she wants to be.[288] In reality, the expertise of data-manipulators has practically eliminated anonymity on the web.[289] Mathematically, deanonymizing individuals requires only a few details about their lives.[290] One researcher says that anyone can be identified with only thirty-three bits of data.[291]

Today, everyone on the Internet knows you are a dog.[292]

285. *Id.*

286. *Id.*

287. *Id.*

288. *See* Victoria Akinsowon, *Online Anonymity is Ugly - But it's Vital for Free Speech*, THE TELEGRAPH (Jul. 7, 2012, 7:00 PM), http://www.telegraph.co.uk/technology/internet/9413040/Online-anonymity-is-ugly-but-its-vital-for-free-speech.html.

289. Zip codes and birthdays are particularly mathematically "valuable." Angwin, *supra* note 56. ZIP codes and birthdays are frequently required even for the most simple of Internet exchanges. *Id.*

290. *Id.*

291. *Id.* A "bit" (binary digit) is the basic unit of information in computing. *Bit Definition*, DICTIONARY.COM, http://dictionary.reference.com/browse/bit (last visited Feb. 19, 2012). A bit is expressed in binary notation, the language in which computers store information, as either a "0" or a "1." *Binary Notation Definition*, DICTIONARY.COM, http://dictionary.reference.com/browse/binary+notation (last visited Feb. 19, 2012). Information is encoded as an eight-unit string of "0s" or "1s" is called a "byte." *Id.*

292. *And Here's a "Reality" Check*, Response to *On The Internet, Nobody Knows You're a Dog*, U.N.C. CHAPEL HILL: SCH. JOURNALISM & MASS COMM., http://www.unc.edu/depts/jomc/academics/ dri/idog.html (last visited Feb. 18, 2012); *but see* Steiner, *supra* note 66.