Regulating Online Behavioral Advertising, 44 J. Marshall L. Rev. 899 (2011)

Steven C. Bennett

Follow this and additional works at: https://repository.law.uic.edu/lawreview

Part of the Computer Law Commons, Consumer Protection Law Commons, Internet Law Commons, Marketing Law Commons, and the Privacy Law Commons

Recommended Citation
Steven C. Bennett, Regulating Online Behavioral Advertising, 44 J. Marshall L. Rev. 899 (2011)

https://repository.law.uic.edu/lawreview/vol44/iss4/2

This Article is brought to you for free and open access by UIC Law Open Access Repository. It has been accepted for inclusion in UIC Law Review by an authorized administrator of UIC Law Open Access Repository. For more information, please contact repository@jmls.edu.
Online behavioral advertising ("OBA"), sometimes known as profiling or behavioral targeting, can be used by on-line publishers and internet marketers to increase the efficiency and effectiveness of their advertising campaigns. OBA works by collecting data on a user's behavior on the Internet including browsing habits, search queries, and website viewing history. OBA generally seeks to increase the relevance of advertising displayed to the user, based on data collected about the user, with the aim of increasing the strength of the connection between advertising efforts and purchasing behavior.

Recently, the Federal Trade Commission ("FTC"), the Department of Commerce ("DOC"), and congressional leaders have suggested a need for more intensive regulation of OBA. The chief objective of such regulation is to ensure that consumer privacy is protected and that abuses of consumer information do not occur. Others have suggested that self-regulation, or a system of public and private litigation aimed at addressing excesses in OBA practices, may better address these central concerns while maintaining the economic viability of OBA. This Article examines such regulatory efforts and suggests that they illustrate some of the key issues of national regulatory policy, including questions regarding the best means to balance evolving notions of privacy against the similarly dynamic needs of our information-based economy.

I. ORIGINS OF ONLINE BEHAVIORAL ADVERTISING

The Internet, in its most essential form, was conceived as early as 1962. By 1985, Internet technology supported a broad com-
munity of researchers and developers, and was ready for commercial development. In September 1988, the first Interop trade show was held. In 1991, U.S. government restrictions on commercial uses of the Internet were lifted, and the worldwide web, using HTML 1.0 and hypertext, was released. The hyperlink system made “surfing” the web appealing to millions of people. In 1994, a web browser called Mosaic (later re-named Netscape) appeared, with the capability of reading text and displaying images in the same browser. By 1995, the essential backbone for the modern worldwide web was in place.

“Banner” advertisements first appeared in the early 1990s. By the late 1990s, “pop-up” advertisements became prevalent. Sponsored searches, where advertisers paid for preferred positions in response to searches, also became a norm in Internet marketing. Today, over one billion people use the Internet, and U.S. online sales alone approach $1 trillion per year.

By the late 1990s, serious concerns began to appear regarding “online profiling,” the practice of aggregating information about consumer preferences and interests by tracking their movements online. This practice, said to be “rapidly expanding and evolving,” held the promise, even at that time, to “re-invent the marketing process.” The essential purpose of online profiling, from its inception, was to record online behavior for the purpose of producing targeted advertising. Such targeted advertising could take into account prior online behavior in order to present consumers with goods and services they were most likely to buy. Online profiling could provide information on what sites the user visited, what products and services they viewed, and what purchases they made. From such behavior, essential personal attributes relevant


4. Id. at 273.


7. See Shen, supra note 6 (discussing how simple online searches of personal matters, such as medical diagnoses, serve as an avenue by which online behavior may be gauged and tracked).
Regulating Online Behavioral Advertising
to advertising could be derived.\(^8\) By 2005, Google and other services had developed technology designed to "personalize" advertisements with "behavioral targeting," based on "prior search queries, prior search results, [and] demographic, geographic, psychographic and activity information."\(^9\)

II. How Online Behavioral Advertising Works

The most basic form of OBA, "first-party behavioral advertising," allows a website to keep track of a user's pattern of use of the site.\(^10\) Using a "cookie" on the user's computer, the site can assure that, when the user returns to the site for another session, the site will recognize the user and serve appropriate advertising and content recommendations. The site may add information to the user's profile, such as zip code, age and gender, based on the user's queries during the course of site visits. Where a user opens an account with the site—to shop or to receive free information, such as a newsletter—the site may obtain additional information, such as an identifying email address, which can be added to the user's profile.\(^11\)

"Third-party" OBA expands the collection of data across multiple and varied site operators.\(^12\) Where multiple site operators contract with advertising networks to sell advertising space, they typically permit the network to place their own cookies on user computers, permitting the network to track user behavior across multiple sites. The advertising network, moreover, may obtain additional identifying information, such as an email address, from a site operator and use it to accumulate additional profile information gathered from public sources or from other data aggregators. Recently, some Internet Service Providers ("ISPs") have combined with advertising networks to provide networks with

\(^8\) Id.


\(^10\) See Simple Behavioral Advertising, CTR. FOR DEMOCRACY & TECH. (Oct. 27, 2009), http://www.ctd.org/privacy/targeting/simple.php (providing scenarios by which behavioral advertising works when a user is both logged in and not logged in to a site).

\(^11\) Id.

\(^12\) See Behavioral Advertising Across Multiple Sites, CTR. FOR DEMOCRACY & TECH. (Oct. 27, 2009), http://www.ctd.org/content/behavioral-advertising-across-multiple-sites (explaining how "third-party" behavioral advertising is accomplished).
information about their subscriber's behavior online.\(^1\) All of this information can be employed to provide the user with “targeted”
advertisements,\(^1\) aimed at increasing user interest and re-
sponse.\(^1\) Indeed, some commentators suggest that OBA may be a
critical element of effective marketing on the Internet.\(^1\) Yet, con-

\(^1\) Id. In 2008, the Senate Committee on Commerce, Science and Trans-
portation held hearings on online advertising, which focused (among other
things) on the increasing role of ISPs in OBA. See Anna Gould, Hearing Highlight:
Senate Commerce Committee Holds Hearing on the Privacy Implica-
tions of Online Advertising, EDUCAUSE (July 9, 2008), http://www.educause.
edu/blog/agould/HearingHighlightsSenateCommerce/1677
40 (providing a summary of the testimony provided at the Privacy Implica-
tions of Online Advertising hearing, Privacy Implications of Online Advertis-
ing: Hearing Before the S. Comm. on Commerce, Sci., and Transp., 110th
Cong. (June 8, 2008)). The hearings suggested that “deep packet inspection” by
ISPs could potentially reveal all of the websites a consumer visits, not simply
those connected to a particular advertising network.

\(^2\) One form of OBA deliberately places advertisements before users “out
of context.” The user may demonstrate (through web browsing behavior) interest
in a subject (such as purchase of a new truck). When the user becomes in-
volved in another search (such as foreign travel) the advertising network may
display a truck advertisement, with the deliberate intent of making the adver-
tisement “surprise” the user, and thus produce a more profound effect. See Terri Wells,
How And Why Behavioral Advertising Works, SEOCHAT, 2 (Nov. 1,
Behavioral-Advertising-Works/ (citing study showing more than one hundred
percent increase in “action” rate, in response to surprise OBA).

\(^3\) One recent study, commissioned by the Network Advertising Initiative,
suggested that users were more than twice as likely to click on a targeted ad-
vertisement than more generally distributed advertisements. See Caroline
McCarthy, Study: Like it or Not, Behavioral Ad Targeting Works, CNET.COM
conducted by Howard Beales, former director of FTC Bureau of Consumer Pro-
tection); Howard Beales, The Value of Behavioral Targeting, NETWORKADVERTISING.ORG (Apr. 8, 2010), http://www.
networkadvertising.org
/pdfs/Beales_NAI_Study.pdf. Contrary evidence also exists. One recent survey
suggested that “obtrusive” forms of OBA may “make viewers feel like their
privacy is being invaded—and turns them off.” Avi Goldfarb & Catherine
Tucker, Online Display Advertising: Targeting and Obtrusiveness, ROTMAN
UNIV. (2010), http://www.rotman.utoronto.ca/~agoldfarb/GoldfarbTuc
ker/obtrusiveness.pdf; see Caroline McCarthy, Survey: Advertisers Should
Acknowledge Targeted Ad Concerns, CNET.COM (July 2, 2008),
http://news.cnet.com/8301-13577_3-9983177-36.html (noting that significant
percentages of users online are aware that their browsing activities may be
monitored; less than one-quarter of users express approval of such tracking);
see also David Myron, Why Should Consumers Surrender Privacy?, CUSTOMER
p/articles/mi_hb5679/is_201101/ai_n568_26779/ (discussing a survey that
shows only 14% of respondents believe advertisements are relevant, and ma-
ajority believe that, if they are not relevant, “why should they surrender their
personal data for something they consider useless?”).

\(^4\) See Behavioral Targeting: An Effective Marketing Strategy, BEHAVIORAL TARGETING (Oct. 7, 2010), http://behavioraltargeting.biz/behav-
ioral-targeting-an-effective-marketing-strategy/ (suggesting that OBA tech-
cerns about privacy related to OBA have grown throughout the past decade.\textsuperscript{17}

A variety of additional OBA methods may develop.\textsuperscript{18} Advertising networks may soon routinely develop behavioral profiles for entire groups of people; for example, profiles may be developed for families.\textsuperscript{19} As technologies converge, and Internet services are increasingly provided over cellular telephones and other mobile devices, the ability to locate consumers physically—as can be done through GPS functions—may also generate location-based adver-

\textsuperscript{17} In July 2010, the Wall Street Journal began a series of articles on OBA practices, noting (among other things) that “people are becoming anonymous in name only” (given the increasing ability to aggregate and mine consumer data), that, through a process called “scraping,” companies had begun to “harvest online conversations and collect personal details from social-networking” and other sites, and that some companies were “pirateering” by gathering and selling data accumulated by placing cookies on other sites’ content, without consent from the sites or users. See generally Julia Angwin & Tom McGinty, \textit{Sites Feed Personal Details to New Tracking Industry}, \textsc{Wall St. J.}, July 30, 2010, http://online.wsj.com/article/SB1000142405274870397700457593173432219064.html; Emily Steel & Julia Angwin, \textit{On The Web’s Cutting Edge, Anonymity in Name Only}, \textsc{Wall St. J.}, Aug. 4, 2010, http://online.wsj.com/article/SB1000142405274870329490457593585532109190198.html; Julia Angwin & Steve Stecklow, \textit{“Scrapers” Dig Deep for Data on Web}, \textsc{Wall St. J.}, Oct. 12, 2010, http://online.wsj.com/article/SB10001424052748703358504575543847121788.html; Jessica E. Vascellaro, \textit{Websites Rein in Tracking Tools}, \textsc{Wall St. J.}, Nov. 9, 2010, http://online.wsj.com/article/SB100014240527487039578057602730678670278.html (providing further discussion on OBA practices).

\textsuperscript{18} In addition to the marketing techniques associated with OBA, the technologies used in OBA are changing. For example, in addition to “cookies” on a user's computer, websites may employ “web bugs,” also known as “GIFs,” tiny graphic image files (different from cookies) which also can monitor user behavior. Web bugs are more difficult to detect (and remove) than cookies. \textit{The Web Bug FAQ}, \textsc{NTHelp}, http://www.nthelp.com/OEtest/web_bug_faq.htm (last visited Oct. 2, 2011); see \textit{Are You Protecting Your Personal Information from Newer Online Risks?}, Univ. Fed. Credit Union (Dec. 2010), http://getreal.ufcu.org/index.php?option=com_content&view=article&id=583:are-you-protecting-your-personal-information-from-newer-online-risks&catid=36:remarks-report&Itemid=108 (referencing web bugs, web beacons, flash cookies and other new methods of monitoring web behavior).

\textsuperscript{19} See \textit{Behavioral Targeting Trends 2010}, \textsc{Behavioral Targeting} (Apr. 5, 2010), http://behavioraltargeting.biz/behavioral-targeting-trends-2010/ (targeting may include “family size, gender, age and income to perfectly accommodate not only the needs of the individual but also his family; taking into consideration their purchasing power.”).
Advertising, keyed to where a person is at any given moment. Advertising has begun to appear in online games, social media, blogs and mobile applications. The techniques of behavioral advertising, moreover, increasingly embody "psychographic" studies, aimed at linking objective demographic characteristics—age, gender, and Internet use—with more abstract characteristics like peer group interests, ideas, and opinions. Marketing experts may examine psychographic data to determine which groups are most likely to buy specific goods and services.

III. EARLY EFFORTS AT REGULATION OF ONLINE BEHAVIORAL ADVERTISING

The FTC has long recognized that "privacy is a central element of the FTC's consumer protection mission." The FTC's primary legislative mandate is to enforce the Federal Trade Commission Act, which prohibits unfair methods of competition and unfair or deceptive acts or practices that affect interstate commerce. The FTC also has enforcement authority over a number of additional statutes, including the Truth in Lending Act, the Fair Credit Billing Act, and the Gramm-Leach-Bliley Act.

The FTC held its first public workshop on online privacy in
1995 and thereafter conducted a number of hearings and issued a series of privacy-related reports. In 1999, the FTC held its first public workshop on "online profiling" (related to OBA), co-sponsored by the Department of Commerce, and issued a report to Congress in 2000. The FTC recognized the potential benefits that online profiling might offer to internet users: cookies can store names and passwords so that users need not sign in each time they access a site; cookies allow consumers to set aside items in an electronic shopping cart while they decide whether and what to purchase; cookies allow personalized home pages with local news and weather, and other matters of importance to the individual user; cookies permit sites to offer recommendations of new products and services that may interest the customer; and cookies allow businesses to revise their design and layout periodically, to make them more interesting. Additionally, the FTC found that: profiling avoids waste of advertising money in marketing to consumers who have "no interest" in the products and services offered; targeted advertising can help to "subsidize free content" on the Internet; targeted advertising can "improve a consumer's web experience" by avoiding "bombard[ment]" by the same (uninteresting) advertisements; and targeted advertising can help small companies "more effectively break into the market, by advertising only to consumers who have an interest in their products or services.

The FTC found, however, that weighed against these benefits were "widespread" concerns about collection of personal data, including: the "most consistent and significant concern," that behavioral profiling may be "conducted without consumers' knowledge"; the risk of "extensive and sustained" monitoring, "across a multitude of seemingly unrelated web sites and over an indefinite period of time," permitting "cumulation over time of vast numbers of seemingly minor details" to produce personal profiles that are "quite comprehensive and, to many, inherently intrusive"; the easy ability to "associate previously anonymous profiles with particular


29. Id. at 8-9
30. Id. at 8-9.
individuals”; the difficulty of some consumers in discerning how to change their computer browser settings to refuse cookies, or to determine when cookies have been employed; the danger that unauthorized parties could gain access to personal data, “by purchasing the data or hacking into it”; the risk that companies might “unilaterally change” their operating procedures; the fear that companies might use profiling to determine prices and terms for goods and services through a process called “weblining” that is comparable to “redlining” in the real estate and financial markets; and the concern that “fear of online monitoring will discourage valuable uses of the Internet that are fostered by its perceived anonymity” such as the pursuit of information on sex, sexuality, health, abortion, and other controversial issues.31

The FTC 2000 Report recognized the Commission’s “longstanding support” of industry self-regulation, but suggested that “real challenges to creating an effective self-regulatory regime” existed for the “complex and dynamic” online advertising industry.32 On balancing the benefits of OBA against the concerns expressed, a majority of the FTC commissioners recommended a combination of industry self-regulation and “backstop” legislation to “set forth a basic level of privacy protection for all visitors to consumer-oriented commercial Web sites with respect to profiling.”33

The FTC noted a “set of core fair information practice principles,” including: notice to consumers about information collection practices; choice for consumers as to whether and how much information may be collected; access to information so that consumers can contest the accuracy and completeness of data collected; security to assure that information collected is free from unauthorized use; and enforcement through a reliable mechanism, to impose sanctions for noncompliance with fair information practices.34 The FTC majority recommended that Congress establish a legisla-

31. *Id.* at 10-13; see *id.* at 16 (“[T]he electronic marketplace will not reach its full potential unless consumers become more comfortable browsing and purchasing online.”).

32. *Id.* at 1. The FTC applauded the formation of a Network Advertising Initiative (“NAI”), representing nearly ninety percent of the online advertising industry and all of the leading network advertisers. *Id.* at 22. The FTC found that NAI’s proposed fair information practice principles (based on the principles that FTC itself espoused) presented “a solid self-regulatory scheme.” F.T.C., ONLINE PROFILING: A REPORT TO CONGRESS PART 2 12 (June 2000), available at http://www.ftc.gov/os/2000/07/onlineprofiling.pdf [hereinafter, FTC 2000 REPORT (PART II)]. Nevertheless, a majority of the FTC commissioners suggested that self-regulation could not address “recalcitrant and bad actors, new entrants to the market, and drop-outs from the self-regulatory program.” *Id.* at 10.


34. *Id.* at 1-2.
tive framework in "general terms," outlining these principles, and allow an implementing agency to "promulgate more detailed standards." The Commission, however, was not unanimous on the need for legislation. One FTC commissioner, dissenting from the majority recommendations, noted, "we do not have a market failure here that requires legislative solution." The dissent suggested that "industry initiatives and technological changes" could "alleviate concerns" about online profiling, and that the FTC should "give these promising developments a chance before resorting to the heavy hand of government intervention."  

IV. INTERVENING REGULATORY EFFORTS

Despite calls for legislative solutions, Congress chose not to act in the area of online behavioral advertising. The FTC, however, maintained its focus on OBA practices. In 2006, the FTC held three days of public hearings on "Protecting Consumers in the Next Tech-ade." OBA practices received considerable attention at those hearings. In 2007, the FTC continued its hearings, this time focusing on "Behavioral Advertising: Tracking, Targeting and Technology." In advance of the hearings, the FTC inquired whether companies were following self-regulatory practices and whether such principles were "still relevant" in light of changes in the market.


At the conclusion of the 2007 hearings, the FTC announced its own set of "Proposed Principles," meant to "encourage more meaningful and enforceable self-regulation" associated with OBA.42 The FTC made clear that, to the extent that companies adopted such principles or other self-regulatory standards, "a company must keep any promises that it makes with respect to how it will handle or protect consumer data," or risk FTC enforcement actions.43 The FTC Proposed Principles, largely tracking fair information practices the FTC had long espoused (notice, choice, access, and security), also suggested a need for limits on the period for retention of consumer information.44 FTC Commissioner Jon Leibowitz, commenting at the 2007 FTC town hall meeting on OBA practices, noted the "white heat" of the issues and suggested that company privacy policies had failed to solve the problem of consumer notice and choice because many such policies were "essentially incomprehensible."45 Commissioner Leibowitz also noted the "creative" approach offered by a "Do Not Track" system but did not specifically recommend that approach.46

In 2008, the Network Advertising Initiative ("NAI"), first formed in 2000, updated its self-regulatory principles for OBA privacy practices. The NAI principles focused on notice, choice, use limitation, access, reliability, and security—all issues that have drawn consistent FTC concern.47 By 2009, NAI membership accounted for approximately eighty-five percent of OBA-related ac-

43. Id. at 5.
44. See id. at 4 (stating that retention of data appropriate "only as long as is necessary to fulfill a legitimate business or law enforcement need"). The FTC expressed particular concern about the handling of "sensitive" data (such as health condition, sexual orientation, or children's activities online). Id. at 5.
46. Id. at 7. The "Do Not Track" proposal, from the Center for Democracy and Technology (and others) would create a "Do Not Track" list, available on the FTC website, to "block" sites on the list from tracking internet activity of users who chose to join the program. CTR. FOR DEMOCRACY & TECH. ET AL., CONSUMER RIGHTS AND PROTECTIONS IN THE BEHAVIORAL ADVERTISING SECTOR 4 (Oct. 31, 2007), available at http://www.worldprivacyforum.org/pdf/ConsumerProtections_FTC_ConsensusDoc_Final_s.pdf.
47. NAI, 2008 NAI PRINCIPLES: THE NAI'S SELF-REGULATORY CODE OF CONDUCT 3 (2008), available at http://www.networkadvertising.org/networks/2008%20NAI%20Principles_final%20for%20Website.pdf (stating that the NAI is committed to "maintaining self-regulation with respect to notice, choice, use limitation, access, reliability, and security.").
tivity.\textsuperscript{48} In 2009, moreover, NAI initiated a program of compliance review, “to prevent member companies from merely ‘signing up’ for compliance without actually aligning [their] policies and practices” with the NAI code of conduct.\textsuperscript{49} NAI claimed that the breadth of company participation in its self-regulatory program permitted NAI to “develop and deploy industry-wide technological and policy solutions” to address consumer concerns “more rapidly and flexibly . . . than legislative or regulatory approaches.”\textsuperscript{50} Critics of the NAI code, such as the Center for Democracy & Technology, noted that even “robust” self-regulation of OBA “does not obviate the need for a baseline federal privacy law covering data collection and usage of all kinds . . . .”\textsuperscript{51}

In early 2009, the FTC staff issued a comprehensive report (“2009 Report”) on OBA practices and recommended revisions to the FTC’s self-regulatory principles.\textsuperscript{52} The FTC concluded that “first-party” OBA (“by and at a single web-site”) is “more likely to be consistent with consumer expectations, and less likely to lead to consumer harm” than other forms of OBA.\textsuperscript{53} Accordingly, the FTC concluded that its self-regulatory principles “need not cover these practices.”\textsuperscript{54} By contrast, “third-party” OBA, involving the sharing of data through advertising networks, required FTC attention, because “the consumer may not understand why he has received ads from unknown marketers,” and “may not know whom to contact to

\textsuperscript{49.} Id. at 4-5.
\textsuperscript{50.} Id. at 7.
\textsuperscript{51.} Ctr. for Democracy & Tech., Response, 2008 NAI Principles: The Network Advertising Initiative’s Self-Regulatory Code of Conduct for Online Behavioral Advertising, 1 (Dec. 16, 2008), available at http://www.cdt.org/privacy/2008 1216_NAIresponse.pdf. Among other things, CDT criticized the NAI approach to consumer opt-out of OBA programs, suggesting that, “[s]ince the industry cannot agree on a better opt-out mechanism . . . it is incumbent on the government to help them do so . . . by instituting a “Do Not Track” list, or by forcing them to move to a more informed consent standard.” Id. at 3 (citing Ctr. for Democracy & Tech. et al., supra note 46).
\textsuperscript{52.} F.T.C., FTC STAFF REPORT: SELF-REGULATORY PRINCIPLES FOR ONLINE BEHAVIORAL ADVERTISING iv (2009) [hereinafter, FTC 2009 REPORT].
\textsuperscript{53.} Id. at iii. Further, “contextual advertising,” which is “based on a consumer’s current visit to a single web page or a single search query,” and which “involves no retention of an ad or search result,” is also “likely to be less invasive” than other forms of OBA. Id. Such advertising, where a consumer visiting an online seller’s site might “receive a recommendation for a product based upon the consumer’s prior purchases or browsing activities at that site,” the FTC concluded, was a practice the consumer was “likely to understand,” and put the consumer in a “better position to raise any concerns” about collection and use of such data (or “avoid the practice altogether by taking his business elsewhere”). Id. at 26-27.
\textsuperscript{54.} Id. at iii.
register his concerns or how to avoid the practice."\[^{55}\] The FTC noted that the "traditional notion" of what constitutes personally identifiable information ("PII"), such as a name, postal address, Social Security Number, or driver's license number is "becoming less and less meaningful," as it becomes possible to "link or merge non-PII with PII," to "identify an individual consumer based on information traditionally considered to be non-PII," and users "become identifiable" when "linked by a common identifier."\[^{56}\] Thus, the FTC expressed particular concern that a "highly detailed and sensitive" profile of an individual user could "fall into the wrong hands or be used later in combination with even richer, more sensitive, data."\[^{57}\]

The FTC, in announcing the 2009 Report, noted its plans to continue to "evaluate self-regulatory programs" and conduct investigations into industry practices.\[^{58}\] The FTC described the 2009 Report as part of a "continuous dialogue" with industry, consumer, and privacy advocates, meant to "stop unfair or deceptive practices" while avoiding a "stifling [of] innovation so that responsible business practices could develop and flourish."\[^{59}\] The FTC recognized the "need to balance the potential benefits" of OBA practices against "privacy concerns" and the possibility that imposition of regulations "could interfere with a developing and rapidly changing marketplace."\[^{60}\] The FTC stated that it was "encouraged by recent steps by certain industry members" but suggested "significant work remains."\[^{61}\] In particular, the FTC noted concerns that the NAI self-regulatory code was "too limited" because it only applied to network advertisers, because of lack of effective enforcement of the code and because of "its cumbersome and inaccessible opt-out system."\[^{62}\] The FTC noted the possibility, "as an alternative to the existing self-regulatory models," of the creation of a "Do Not Track" list, "modeled after the FTC's national 'Do Not Call' [telephone] registry . . . ."\[^{63}\]

FTC Commissioner Leibowitz, concurring in the 2009 Report,

---

55. Id. at 27.
56. FTC 2009 REPORT, supra note 52, at 20-22 & n.47.
57. Id. at 23. The FTC suggested that self-regulatory principles should include within their scope "any data . . . that reasonably could be associated with a particular consumer or with a particular computer or device." Id. at 25 (noting that NAI principles embody this scope of protection).
59. FTC 2009 REPORT, supra note 52, at 4.
60. Id. at 18-19.
61. Id. at 47. The FTC "call[ed] upon industry to redouble its efforts in developing self-regulatory programs, and also to ensure that any such programs include meaningful enforcement mechanisms." Id.
62. Id. at 10, 14.
63. Id. at 10, n.24.
commented that “industry needs to do a better job of meaningful, rigorous self-regulation or it will certainly invite legislation by Congress and a more regulatory approach by our Commission.”

Indeed, Commissioner Leibowitz suggested that “[a] day of reckoning may be fast approaching” and that industry might have one “last clear chance” to show that self-regulation could “effectively protect” consumer privacy in the “dynamic” online market. Commissioner Leibowitz, in particular, suggested that a “Do Not Track” system for OBA deserved “serious consideration” as an alternative to self-regulation.

Just a few months after the FTC issued its 2009 Report, a coalition of industry groups published “Self-Regulatory Principles for Online Behavioral Advertising.” These principles, drafted by the American Association of Advertising Agencies, the Association of National Advertisers, the Direct Marketing Association, the Interactive Advertising Bureau, and the Council of Better Business Bureaus, focused on areas that the FTC had identified as desirable for industry self-regulation, including: notice and education for consumers, easier consumer “opt-out” tools, and more significant restrictions on behavioral profiling by ISPs. One commentator, describing the new principles as an “extraordinary show of industry cooperation,” suggested that the alternative to self-regulation, some form of legislation, was unlikely to “remain relevant or even defensible in the face of innovation and technology which could not be predicted . . . .”

Further refinements of these self-regulatory

---


65. Id. at 1-2.

66. Id. at 1. Commissioner Leibowitz also noted the “welcome development” of internet browser design to give consumers tools to “control the amount of information they share online.” Id. For additional information on privacy protection features of browsers, see Browser Privacy Features: A Work in Progress, CTR. FOR DEMOCRACY & TECH. (Dec. 7 2010), http://www.cdt.org/browserreport2010.


principles followed in 2010.69

V. RECENT REGULATORY DEVELOPMENTS

In 2009, Jon Leibowitz became Chairman of the FTC.70 Late in 2009, the FTC commenced a three-part roundtable series, "Exploring Privacy," meant to review virtually every aspect of consumer privacy in the modern technological and business environments.71 Chairman Leibowitz, in introducing the series, called the inquiry a "watershed moment in privacy"72 and stated that the "time is ripe" for the FTC to "build" on its 2009 OBA principles and "take a broader look at privacy writ large."73 Chairman Leibowitz suggested that because "consumers don't read privacy policies"74 and "traditional notions of PII" no longer applied—given the "unbelievable" advances in technology" that permit companies to "store and crunch massive amounts of data relatively cheaply"—the FTC's "notice and choice regime" and "harm-based approach" had not worked "quite as well as we would like . . . ."75

The FTC's roundtable series included many experts who suggested that the "notice and choice" privacy governance model has become increasingly irrelevant76 because consumers have little

Self-Regulatory%20Principles%20-%20Rosenbaum%20Article.pdf (suggesting that "traditional regulation" may not "make sense," given changes in roles of advertisers, use of wireless and mobile devices, convergence of computing and television, and rise of online gaming).


71. Exploring Privacy: A Roundtable Series, F.T.C. (last visited June 17, 2011) (providing that FTC inquiry was meant to "explore the privacy challenges posed by the vast array of 21st-century technology and business practices that collect and use consumer data," including "online behavioral advertising").


73. Id.


75. Id. Chairman Leibowitz professed to have an "open" mind on the "complex" issues presented, in seeking a "better way to protect privacy." Id.

76. Despite that conclusion, David Vladeck, Director of the FTC Bureau of Consumer Protection, noted that OBA was "not an area in which we want to
understanding of how their data is used and transferred, notices are not effective for communicating with consumers, and privacy-enhancing technologies have met with little consumer acceptance.\(^7\) Indeed, by May 2010, Chairman Leibowitz suggested that “[t]he consent half of ‘notice and consent’ rarely reflects a consumer’s conscious informed choice,” because “few of us can comprehend the amount of personal data we’ve left open for capture on the Internet, and disclosure forms are most often written by lawyers,” making them lengthy and wordy.\(^7\)

VI. THE EUROPEAN UNION APPROACH

In June 2010, the Article 29 Working Party, a European Union (“EU”) advisory body composed of representatives from the EU member states, issued a detailed opinion on the appropriate means to obtain consent from users to conduct behavioral advertising.\(^7\) The EU Opinion focused on OBA “across different websites,” as opposed to mere contextual advertising within the confines of a single site.\(^8\) The EU Opinion criticized “opt-out” mechanisms, be-

---


\(^8\) See John Eggerton, FTC Not Interested in Regulating Behavioral Ads if Industry Can Do Job, BROADCASTING & CABLE (May 12, 2010), http://www.broadcastingcable.com/article/452590-Leibowitz_FTC_Not_Interested_in_Regulating_Behavioral_Ads_If_Industry_Can_Do_Job.php.

---

77. See id. at 4 (noting EU concerns of data tracking across multiple websites). Thus, for “third-party” cookies and other behavior tracing mechanisms, the EU Opinion stated: “i) consent must be obtained before the cookie is placed and/or information stored . . . and ii) informed consent can only be obtained if prior information about the sending and purposes of the cookie has been given to the user.” Id. at 13 (emphasis in original). Further, “consent must be revocable.” Id.
cause “users lack the basic understanding” of data collection practices, and “consent means active participation of the data subject,” as opposed to non-reaction (failure to opt-out).\textsuperscript{81}

The EU Opinion recommended that privacy notices be “as user friendly as possible,” placing “a minimum of information directly on the screen, interactively, easily visible and understandable . . . .”\textsuperscript{82} The EU Opinion welcomed “creativity” in this area, as by using icons concerning privacy, with links to additional information.\textsuperscript{83} The EU Opinion also called for “clear and unambiguous reminders” of monitoring, for users who may become unaware that monitoring is still taking place.\textsuperscript{84} Such reminders would also “help control whether [users] want to continue or revoke their consent.”\textsuperscript{85} Finally, the EU Opinion cited “targeting of data subjects” based on “sensitive information”—such as sexual preference or political activity—which “opens the possibility of abuse.”\textsuperscript{86} For these categories of information, a “separate, affirmative prior indication” of consent to gather data would be required, and “in no case would an opt-out consent mechanism meet the requirement of the law.”\textsuperscript{87}

The EU Opinion concluded that, “[s]o far, the ways in which industry has provided information and facilitated individuals to control whether they want to be monitored have failed.”\textsuperscript{88} The Opinion noted that industry had made “some efforts to complement existing law with self-regulation,” but found that there is “a long way to go,” and suggested that “[i]ndustry should step up efforts to comply with the reinvigorated applicable laws.”\textsuperscript{89} The

\begin{footnotes}
\footnotetext[81]{See id. at 15 (noting issues with cookie-based opt-out mechanisms). The EU Opinion also insisted that any consent given must be limited in time, such that OBA data would be “deleted or anonymised once the necessity for retaining it has expired.” Id. at 20 (finding that the data controller “needs to be able to justify the necessity for a given retention period”).}
\footnotetext[82]{Id. at 18 (emphasis in original).}
\footnotetext[83]{The EU Opinion cited the work of the Future of Privacy Forum on development of privacy “icons” as one means to promote consumer education on privacy issues. See id. at 16 n.35; see also Future of Privacy Forum Releases Behavioral Notices Study, FUTURE OF PRIVACY FORUM (Jan. 27, 2010), http://www.futureofprivacy.org/2010/01/27/future-of-privacy-forum-release-behavioral-notices-study/ (suggesting that icons, coupled with simple explanations (such as “Why did I get this ad?”) can “play an important role in educating consumers”).}
\footnotetext[84]{EU OPINION, supra note 79, at 18.}
\footnotetext[85]{Id.}
\footnotetext[86]{Id. at 19.}
\footnotetext[87]{Id. at 20.}
\footnotetext[88]{Id. at 21.}
\footnotetext[89]{Id. at 22. On December 15, 2010, the European Parliament issued a resolution on the impact of advertising on consumer behaviour. EUR. PARL. DOC. (0484) T7-0484 (2010), available at http://www.europarl.europa.eu/sides/getDoc.do?type=TA&language=EN&reference=P7-TA-2010-0484. The resolution recognized that advertising “fosters competition and competitiveness,” and “constitutes an important and often crucial source of funding for a

Opinion emphasized that “[a]d network providers should swiftly move away from opt-out mechanisms and create prior opt-in mechanisms.” The exact impact of the EU Opinion has yet to be seen.

VII. THE FTC 2010 REPORT

In December 2010, the FTC staff issued a preliminary report, aimed at providing a “broad privacy framework to guide policymakers, including Congress and industry.” The Report included nearly eighty pages of analysis, plus more than sixty questions on which the FTC sought additional input. The Report did not limit its focus to behavioral advertising online. Rather, the Report

dynamic and competitive media landscape,” but that “it is still necessary to combat unfair commercial practices in the advertising field . . . ” Id. The resolution called on the European Commission (the executive body of the EU) to “update, clarify and strengthen” guidelines on unfair commercial practices, to encompass behavioral advertising, specifically, and encouraged “consultation” with various stakeholders in completing that process. Id. The resolution “[d]enounce[d] the development of ‘hidden’ internet advertising,” and “[s]tresse[d] the need for consumers to be informed fully when they accept advertising . . . ” Id. The resolution suggested a specific need to protect “vulnerable” groups (children and adolescents) and a need to promote “equality and human dignity” in advertising. Id. The resolution called for additional efforts to educate and inform consumers and other stakeholders. See id. (suggesting “information campaigns” and programs to teach children about advertising); see generally European Parliament Calls for Steps Against Intrusive New Advertising on the Internet, THE SOPHIA ECHO (Dec. 16, 2010), http://sofiaecho.com/2010/12/16/1012269_european-parliament-calls-for-steps-against-intrusive-new-advertising-on-the-internet (summarizing points addressed in resolution).

90. EU OPINION, supra note 79, at 22.
93. More than 400 public comments in response to the FTC 2010 Report are available for review at www.ftc.gov/os/comments/privacyreportframework.
94. The FTC noted that, although survey data and other evidence suggests
called for a wholesale “re-examination” of the FTC’s approach to privacy protection.95

The FTC noted that the “limitations” of the “notice-and-choice” model have become “increasingly apparent.”96 Privacy issues have become “longer, more complex,” and often “incomprehensible to consumers.”97 While many companies offer disclosure of their practices, fewer “actually offer consumers the ability to control these practices.”98 As a result, the FTC suggested, “consumers face a substantial burden in reading and understanding privacy policies and exercising the limited choices offered . . . .”99

The FTC expressed concern about consumer “lack of understanding” of privacy practices.100 Some consumers, for example, believe that the term “privacy policy” on a website means that the site protects privacy, and may not be aware that a company could share data with hundreds of affiliates, or that third parties could “combine their data with additional information obtained from other sources.”101 The FTC also suggested that “overloading privacy policies with too much detail can confuse consumers or cause them to ignore the policies altogether.”102

Further, the FTC noted that its “harm-based” approach to privacy protection “also has limitations.”103 Such an approach “focuses on a narrow set” of privacy-related harms, those that “cause physical or economic injury or unwarranted intrusion into consumers’ daily lives,” but “the actual range of privacy-related harms is much wider and includes reputational harm, as well as the fear of being monitored or simply having private information ‘out there.’”104 Thus, the FTC suggested, “[w]hen data is collected for one purpose and then treated differently, the failure to respect the

---

“a majority of consumers are uncomfortable with being tracked online,” there is “little or no information about the degree of such discomfort” or the proportion of consumers who would be willing to forgo the benefits of OBA, to avoid being tracked. FTC 2010 REPORT, supra note 92, at 29.

95. Id.
96. Id. at 19.
97. Id.
98. Id.
99. Id.
100. See id. at 25 (noting the need for transparency in privacy practices).
101. Id. at 26.
102. See id. at 27 (suggesting a need to “simplify[] consumers’ ability to exercise choices”).
103. Id. at 20.
104. Id. The harm-based model also “depends upon the ability to identify and remedy harm,” and yet “consumers may not know when they have suffered harm or the risk of harm.” Id. at 33. Moreover, the harm-based approach may be considered too “reactive,” as opposed to a structure that “prevent[s] harms from arising rather than merely providing remedies when harms occur.” Id. n.86 (quoting David J. Solove, Identify Theft, Privacy, and the Architecture of Vulnerability, 54 HASTINGS L.J. 1227, 1232 (2003)).
original expectation constitutes a cognizable harm." The FTC emphasized the "nearly ubiquitous" collection of consumer data, and that data collectors "share the data with multiple entities," due to "economic incentives [that] drive the collection and use of more and more information about consumers." The FTC also expressed concern with the increasing erosion of anonymity on the Internet.

The FTC advanced three "major elements" in its proposed new framework for consumer privacy. First, companies should promote privacy "at all stages" of the design and development of their products and services.

Second, the FTC called on companies to simplify consumer choice. One important element of this simplification involves identification of a limited set of "commonly accepted practices," for which companies "should not be required to seek consent once the consumer elects to use" a product or service. For practices that

105. FTC 2010 REPORT, supra note 92, at 20 n.49 (quoting Joel R. Reidenberg, Privacy Wrongs in Search of Remedies, 54 HASTINGS L.J. 877, 881 (2003)).

106. FTC 2010 REPORT, supra note 92, at 23-24; see id. at 24 ("[T]he more information that is known about a consumer, the more a company will pay to deliver a precisely-targeted advertisement to him."). Further, "low-cost data storage capability [may] lead companies to retain the data they collect indefinitely, which could create "incentives and opportunities to find new uses for it." Id. at 25.

107. The FTC noted that the "traditional distinction" between personally identifiable information and non-PII "has eroded," and that restrictions based on this distinction are "losing their relevance." Id. at 35-36. Further, technical developments, such as "browser 'fingerprinting' technology," have helped to "blur the line" between PII and non-PII. Id. at 36. Thus, even where companies take steps to "de-identify" data, technical advances and widespread availability of information have "fundamentally changed the notion of anonymity." Id. at 37-38 & n.106 (citing Paul Ohm, Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization, 57 UCLA L. REV. 1701 (2002)).


109. Id. at 44. Such efforts, modeled on fair information principles, include: providing "reasonable security" for consumer data, collecting "only the data needed for a specific business purpose," retaining data "only as long as necessary" to fulfill that purpose, and implementing "reasonable procedures to promote data accuracy." Id. at v. Such efforts would require "assigned personnel to oversee privacy issues" from the earliest stages of research and development, training employees on privacy, and conducting "privacy reviews" associated with new products and services. Id. at 44. Further, the FTC supported use of "privacy-enhancing technologies" to help "establish and maintain strong privacy policies." Id. at 52. In short, the FTC called for a "privacy by design" approach to "building privacy protections" into a company's "everyday business practices." Id. at v.

110. Id. at 52.

111. Id. at 53. Thus, for product and service fulfillment, internal operations (such as surveys to improve customer service), fraud prevention, legal compliance and "first-party" marketing, the FTC concluded that "requiring consumers to make a series of decisions whether to allow companies to engage in the-
require consumer choice, the FTC suggested that companies offer the choice "at a time and in a context" in which consumers make decisions about their data.\textsuperscript{112} The FTC sought comment on the most appropriate way to obtain consent from consumers.\textsuperscript{113} Apropos existing consent-gathering mechanisms, the FTC suggested that industry efforts had "fallen short."\textsuperscript{114} The FTC recommended a "Do Not Track" program, modeled on but technically different from\textsuperscript{115} its existing "Do Not Call" program.\textsuperscript{116}

\textsuperscript{112} Id. at 58. Thus, the choice mechanism should appear "at the point when the consumer is providing data," and should appear "clearly and conspicuously on the page" at which consumers provide personal information. \textit{Id.} Any information sharing that "occurs automatically" should be disclosed clearly "at the time the consumer becomes a member of the [data-sharing] service," and not merely "buried" in the company's privacy policy. \textit{Id.} at 59. The consumer decision, moreover, should be "durable," such that the consumer is "not subject to repeated additional requests" for permission to share data. \textit{Id.}

\textsuperscript{113} The FTC recognized that some commenters recommended "opt-in," while others advocated "opt-out," and still others suggested modified mechanisms, such as "mandated choice," where a consumer must make some decision before proceeding with a transaction. \textit{See id.} at 59-60 & n.142 (detailing other options to gain consent). The FTC also noted proposals for the use of a "uniform icon or graphic," and suggestions that "sensitive" information (involving children, financial and medical information, and precise geolocation data, among others) may require "additional protection," such as a means to "seek affirmative express consent" for the sharing of such information. \textit{Id.} at 60-61; \textit{see id.} at 62 (noting that "deep packet inspection" involving ISPs might also warrant "enhanced consent" due to the "scope" of information collected and relative "inability" of many consumers to choose among competing broadband services).

\textsuperscript{114} \textit{Id.} at 64. The FTC noted its longstanding call for industry to develop "just-in-time" choice for OBA, and that an effective mechanism had yet to be implemented on an industry-wide basis. \textit{Id.} Thus, the FTC suggested a "more uniform and comprehensive" consumer choice mechanism, involving a "Do Not Track" list. \textit{Id.} at 66. This system, to be implemented either by legislation or through "robust, enforceable self-regulation," might involve placing a setting on a consumer's browser to signal whether the consumer wanted to be tracked, or to receive targeted advertisements. \textit{Id.} To be effective, the system would also deploy some "enforceable requirement" that sites honor such consumer choices. \textit{Id.}

\textsuperscript{115} \textit{See Do Not Track: Universal Web Tracking Opt-Out}, www.donottrack.us (last visited Oct. 2, 2011) (summarizing "Do Not Track" system and explaining that it "differs from the "Do Not Call" registry").

\textsuperscript{116} FTC 2010 REPORT, supra note 92, at 67. Because, unlike telephone numbers, there is no "persistent" unique identifier for a computer, the FTC recommended a browser-based mechanism, through which consumers could make 'persistent' choices. \textit{Id.} The FTC also called for more "granular" options, to permit consumers to do more than "opt[]out of advertising entirely," by controlling the specific types of advertising they want to receive. \textit{Id.} at 68. The
Finally, regarding means to increase the transparency of data practices, the FTC called for efforts to simplify consumer choices. The FTC also suggested that companies provide "reasonable access" to the consumer data they maintain with access to be "proportionate to the sensitivity of the data and the nature of its use." The FTC also suggested the need for "affirmative express consent" before companies use consumer data "in a materially different manner than claimed when the data was collected." The FTC called on all stakeholders to provide "greater consumer education to increase consumer awareness and understanding" of data collection practices and their privacy implications.

Although the FTC 2010 Report was identified as a staff report, two FTC commissioners wrote separately to express their views on the significance of the Report. Commissioner William E. Kovacic suggested that, although the Report might "stimulat[e] further discussion," its recommendations (including a "Do Not Track" system) were "premature." Commissioner J. Thomas Rosch similarly expressed "serious reservations" about the proposals advanced in the Report.

FTC called for comments on how to make this new mechanism "understandable," "simple," and "standardized." Id. at 69. The FTC pointed to efforts in the financial services area, where agencies worked together to develop a "model" financial privacy notice, based on extensive research and consumer testing. Id. at 71. Such notices, it suggested—using a "layered" approach, with additional detail as the consumer chooses to inquire—can provide a "significant improvement" over prior forms of notice. Id. at 72.

The FTC noted that issues of access had been "controversial," and that access could involve cost to business, create difficulty in authenticating the identity of consumers requesting access, and pose privacy threats to consumer data. Id. at 73-74. The FTC noted the difficulty in developing "workable solutions" to "align costs of access with the benefits to consumers." Id. at 75. It noted "commendable" progress in the area, and sought further comments. Id. at 76. Under "well-settled FTC case law and policy," changes may be deceptive if such changes are not properly disclosed, and consent properly obtained. Id. at 77.

Such education, the FTC suggested, should focus (among other things) on "available tools for consumers to control the collection and use of their data." Id. at 78. See William E. Kovacic, Comm'r, Fed. Trade Comm'n, Concurring Statement to FTC 2010 REPORT, supra note 92, at D1-D4 (questioning the "expanded concept of harm" presented in the Report and noting the benefits—such as free content and relevant advertising—that could be lost if consumers routinely opted out of behavioral tracking).

See J. Thomas Rosch, Comm'r, Fed. Trade Comm'n, Concurring Statement to FTC 2010 REPORT, supra note 92, at E1-E6 (calling the Report "flawed" as a guide to Congress, Commissioner Rosch suggested that a "new framework," to replace notice and choice or harm concepts was "unnecessary" and might "overstep" the FTC's bounds, which did not extend to "reputational harm" or "fear of being monitored," but instead was limited to "deception"). Further, Commissioner Rosch suggested, the FTC had never challenged an
Supporters\textsuperscript{123} and critics\textsuperscript{124} of the FTC Report quickly lined up after announcement of the Report’s preliminary findings.\textsuperscript{125} Among particular subjects of vigorous debate were the merits of the “Do Not Track” system proposed by the FTC. Critics suggested that the system could adversely affect Internet revenues,\textsuperscript{126} lead to opt-out mechanism for consumer choice. \textit{Id.} at E2. Thus, even though the proposals might be “desirable in the abstract,” Commissioner Rosch saw no reason that companies should be “mandated” to adopt them. \textit{Id.} n.4. Indeed, Commissioner Rosch suggested that even self-regulation could prove anti-competitive, as “a way for a powerful, well-entrenched competitor to raise the bar so as to create an entry barrier to a rival . . . .” \textit{Id.} at E3. Commissioner Rosch suggested that the “notice” model for protecting privacy had “served [the] Commission long and well,” and that replacing the model with a “theoretical and untested” new model would represent “bad public policy . . . .” \textit{Id.} at E6.

\begin{itemize}
  \item \textsuperscript{123} FTC Releases Privacy Report, IAPP (Dec. 1, 2010), https://www.privacyassociation.org/publications/ftc_releases_privacy_report/ (quoting Jules Polonetsky, Co-chair of Future of Privacy Forum: The FTC “wisely left the door open to either legislative or self-regulatory solutions”); Rainey Reitman, FTC’s New Privacy Report Endorses “Do Not Track” Mechanism to Empower Online Consumers, ELECTRONIC FRONTIER FOUNDATION (Dec. 1, 2010), http://www.eff.org/deeplinks/2010/12/ftc-privacy-report-calls-attention-privacy (noting that the Report shows the FTC “ready to tackle some of the most challenging issues,” including “revolutionary approaches to defending personal privacy such as ‘Do Not Track.’”).
  \item \textsuperscript{124} See, e.g., Kashmir Hill, Brief Takeaways—and a Pretty Diagram—from the FTC’s Online Privacy Recommendations, FORBES (Dec. 1, 2010, 3:17 PM), http://blogs.forbes.com/kashmirhill/2010/12/01/brief-takeaways-and-a-pretty-diagram-from-the-ftcs-online-privacy-recommendations/ (posing the question—in considering the success of a “Do Not Track” system proposed by the FTC—“Can anti-tracking technology keep up?”); Kevin Fogarty, FTC Becomes Aware There is an Internet, ITWORLD (Nov. 17, 2010, 5:02 PM), http://www.itworld.com/legal/128061/ftc-becomes-aware-there-internet (arguing that the Report represents “a set of recommendations with roughly the same clarity, credibility and impact of a strongly worded letter from the U.N. to this year’s evil dictator asking him to please not kill and eat so many villagers”); FTC Seeks Input on Sweeping Changes to Consumer Privacy Protections: Recommendations Include Do-Not-Track and Much More, WINSTON & STRAWN, LLP (Dec. 2010), http://www.winston.com/siteFiles/Publications/Summaryof%20FTCPrivacyReport.html (suggesting that the Report marks “major change” that would “essentially create[e] an EU-like approach for all entities that collect and maintain personal information”); John J. Heitman, FTC Staff Report Signals Shifting Privacy Compliance and Enforcement Risks, TELECOM LAW MONITOR (Dec. 8, 2010), http://www.telecomlawmonitor.com/2010/12/articles/enforcement/ftc-staff-report-signals-shifting-privacy-compliance-and-enforcement-risks/ (advising that although portions of the Report were enforceable at the time of its release, “distinguishing the enforceable from the aspirational isn’t always easy.”).
  \item \textsuperscript{126} Behavioral advertising “brings in needed revenue for sites that offer news, useful information and free services.” Larry Magid, Do We Need a “Do Not Track” Tool and Will it Help?, HUFFPOST TECH (Dec. 11, 2010, 11:47
monopolization, and become technically unworkable or obsolete. Others criticized the “Do Not Track” proposal as not going
far enough to protect consumer privacy. Critics also suggested that the technology for “Do Not Track” is, at present, not completely effective. Market development of such technology, without

129. See Bianca Bosker, Why the FTC’s Online Privacy Plan Won’t Stop the Information Free-For-All, HUFFPOST TECH (Dec. 6, 2010, 4:57 PM), http://www.huffingtonpost.com/2010/12/06/ftcs-online-privacy_n_792548.html; see id. (quoting Marc Rotenberg, President of the Electronic Privacy Information Center) (“The FTC needs to think much more holistically about privacy . . . It focuses on one particular problem—online advertising—and proposes one particular solution. The threats to online privacy, as well as the possible solutions, occupy many dimensions.”); Erica Newland, “Do Not Track” Solves Only Part of the Problem, CTR. FOR DEMOCRACY & TECH. (Dec. 2, 2010), http://www.ctd.org/blogs/ericanewland/"do-not-track"-solves-only-part-problem (calling for “baseline privacy legislation” to address wider privacy issues because the “Do Not Track” proposal does not address data collection outside of behavioral advertising and “fails to address emerging challenges to online privacy: cloud computing, social networking and the growth of the app economy”).

government mandate, moreover, suggested to some critics that further regulation might not be required. Given the "potentially far-reaching" consequences of the proposal, moreover, some critics suggested, "[I]t is imperative that any new laws be carefully tailored."133

VIII. THE COMMERCE DEPARTMENT 2010 REPORT

Shortly after the FTC released its 2010 Report, the Department of Commerce issued its own report on “Commercial Data Privacy And Innovation In The Internet Economy.” The Commerce Report addressed broad privacy issues, including OBA and other practices. DOC launched its Internet privacy inquiry in

131. FTC Chairman Leibowitz, for example, applauded Microsoft’s recent announcement of new features on its browser that would permit users to stop websites and tracking companies from gathering information. See Nick Wingfield & Jennifer Valentino-Devries, Microsoft to Add Tracking Protection to Web Browser, WALL ST. J., Dec. 7, 2010, http://online.wsj.com/article/SB10001424052748703296604576005542201534546.html (quoting Chairman Leibowitz) (“This announcement proves that technology is available to let consumers control tracking...”). A Microsoft spokesman, however, indicated that the tool might be used by “far, far, less than 100 percent” of Microsoft browser users. Id. (quoting Dean Hachamovitch); Tanzina Vega, Microsoft, Spurred by Privacy Concerns, Introduces Tracking Protection to Its Browser, N.Y. TIMES, Dec. 7, 2010, http://www.nytimes.com/2010/12/08/business/media08soft.html (citing Jules Polonetsky of the Future of Privacy Forum) (“Most people would likely ignore the option altogether.”).

132. See, e.g., Romina Boccia, Do-Not-Track Instilling a False Sense of Privacy, INDEPENDENT WOMEN’S FORUM (Dec. 8, 2010, 1:45 PM), http://www.iwf.org/inkwell/show/23960.html (“Those who are concerned with being tracked have various options to rid their computers of cookies or choose web browsers that don’t allow tracking... The best way for consumers to obtain more privacy on the web is to demand privacy by exercising already existing options... ”); Kirk Sigmon, “Do not Track” Idea Nice, but Won’t Work, KIRK SIGMON (Dec. 1, 2010, 11:38 PM), http://kirkssigmon.com/2010/12/do-not-track-idea-nice-but-wont-work/ (“Most users concerned with their privacy have found “third-party” mechanisms to alleviate their worries, including ad blockers and the like. While one might argue that there is a population of users who not use these solutions but nonetheless would take up the FTC-recommended offer of privacy if given to them, this population seems like it would be too small to justify such a mass internet infrastructure overhaul... ”).


135. The Commerce Report noted that privacy concerns on the Internet go “far beyond” questions of “profiling and targeting for advertising,” and include
April 2010 with the formation of an Internet Policy Task Force. The Task Force included contributions from the National Telecommunications and Information Administration, the International Trade Administration, and the National Institute for Standards and Technology.

The Commerce Report noted that, at the inception of the commercial Internet in the 1990s, the "government imperative was to seek unrestrained growth of the Internet as an exciting new medium for free expression and commerce." In that vein, efforts to promote "voluntary, enforceable codes of conduct" regarding privacy assured that "industry codes would develop faster and provide more flexibility than legislation or regulations." The Report also noted the "sectoral" approach to privacy pursued in the U.S., which has provided important privacy protections in specific areas. The Report, however, suggested that a "new approach rapidly increasing use of "cloud" computing to store and process large amounts of information, and to move information to remote locations, beyond the "direct control" of consumers. Id. at 16.

136. The Commerce Department issued its Notice of Inquiry in April 2010, and held a Privacy and Innovation Symposium in May 2010. See id. at 2. Some twenty-five panelists participated in the Symposium, and more than seventy groups and individuals (including the FTC) provided written comments. See id., Appendix B (listing participants). Participant comments are available at www.ntia.doc.gov/comments.

137. The Commerce Report noted an “Administration-wide effort” to “articulate principles of transparency, promot[e] cooperation, empower[] individuals to make informed and intelligent choices, strengthen[] multi-stakeholder governance models, and build[] trust in online environments.” Id. at iv. Among other things, the Report noted the formation of a National Science and Technology Council Subcommittee on Privacy and Internet Policy, co-chaired by Cameron Kerry, General Counsel at the Department of Commerce and Christopher Schroeder, Assistant Attorney General for Legal Policy. See id.

138. The Report cited the “economic imperative” of effective management of online communications. Id. at 13; see id. at 13-14 (noting $3.7 trillion U.S. value of annual online transactions and $10 trillion global value). Huge percentages of Americans use the Internet on a daily basis, and a substantial number find the Internet an “integral” part of their work. Id. at 14

139. The Report noted self-regulatory efforts by online advertising trade groups, including the proposal to use an “icon” in or near online advertisements to “alert users” to information on privacy practices. Id. at 28 & n.79 (citing Am. Ass’n of Adver. Agencies, et al., Self-Regulatory Principles for Online Behavioral Advertising, IAB. (July 2009), http://www.iab.net/media/file/ven-principles-07-01-09.pdf).

140. Id. at 19-20. The Commerce Report emphasized a need for a “dynamic” approach, “recognizing the dynamic nature of both technologies and markets, and encouraging continued innovation over time.” Id. at 3. The Report also noted the “danger of locking-in outdated rules” in the form of legislation. Id. at 29.

141. The Commerce Report noted that, although the first national agency (HEW) recognized the need for “fair information practices” as early as 1973, “Congress did not extend such data privacy requirements to the private sector, and today the United States does not have generally applicable commercial
may well be necessary" in view of the increasingly "vital role" of the Internet in "daily life." The Report cited a need for "[f]oundational principles" to "strengthen commercial data privacy." The Report called for "reevaluation of current policy," because, from the consumer perspective, "the current system of notice-and-choice does not appear to provide adequately transparent descriptions of personal data use," leading to "misunderstandings" that "inhibit their exercise of informed choices."

The Commerce Report set out four main goals for U.S. privacy data privacy rules." Id. at 11. Rather, the U.S. has adopted a "flexible" approach to privacy protection, with "strong sectoral" privacy laws, in the areas of health, finance, education and information about children. Id. at 11-12. This sectoral approach permits "tailoring" to fit specific industries, but can also produce "gaps" in the privacy framework. Id. at 12. In particular, the Report noted, many "key actors," including "online advertisers" essentially operate without any "specific statutory obligations" to protect personal data. Id. at 12. Yet, the sectoral approach, some suggest, presents a "jigsaw puzzle" in which "the pieces do not always fit together." Id. at 60 ("Rather than coming up with an overall picture and then breaking it up into smaller pieces that mesh together, Congress has been sporadically creating individual pieces of ad hoc legislation."); see id. (noting that a sectoral approach "confuses consumers and creates large gaps in consumer protection"). The Report also contrasted the "different models" in other countries. Id. at 12. For example, the 1995 European Union Privacy Directive, and similar efforts in other regions, have produced laws "generally applicable to personal data, irrespective of the industry in which the data processor operates." Id. at 12.

142. The Report suggested that "changes in technology and business models" have "rendered parts of our privacy policy framework out of date." Id. at 9.

143. Id. at 20-21.

144. The Report noted that comments were "virtually unanimous" in calling for "strengthening of the U.S. commercial privacy framework, to "ensure transparency and informed consent, to provide additional guidance to business, to establish a baseline commercial data privacy framework to afford protection for consumers, and to clarify the U.S. approach to commercial data privacy—all without compromising the current framework’s ability to accommodate customer service, innovation, and appropriate uses of new technologies." Id. at 2-3.

145. Citing a "high level of online-privacy illiteracy," the Report observed that "consumers do not always understand how and with whom their information might be shared, or the potential negative implications of sharing such information." See id. at 19 & n.49 (quoting Chris Hoofnagle, Jennifer King, Su Li and Joseph Turow, How Different are Young Adults from Older Adults when it Comes to Information Privacy Attitudes & Policies?, F.T.C. (Apr. 24, 2010), http://www.ftc.gov/os/comments/privacyroundtable/544506-00125.pdf).

146. The Commerce Report noted that even "[p]lain, accessible statements" about information practices "do not necessarily bring these practices into line" with consumer expectations. Id. at 37. Thus, "purpose specification requires an organization to "state specific reasons" for collecting personal information. Id. at 38. Further, the Report recommended, "retroactive privacy policy changes," without notice of the change, and an "opportunity to consent to new uses of existing data" should be subject to enforcement actions. Id. at 39.

147. Id. at 22.
protection policy: 148 (1) to enhance consumer trust online through the recognition of “revitalized” fair information practice principles; 149 (2) to encourage the development of “voluntary, enforceable” privacy codes of conduct, through “collaborative efforts” with government; 150 (3) to encourage “global interoperability”; 151 and (4) to ensure “nationally consistent” privacy rules. 152

148. Id. at 3-7.
149. The Report suggested that fair information principles should “enhance[e] transparency, encourage[e] greater detail in purpose specifications and use limitations, and foster[] the development of verifiable evaluation and accountability programs . . . .” Id. at 30. The Report noted “lengthy and complex” disclosures that “fail to inform,” and suggested that “privacy rights depend on [consumer] ability to understand and act on” company privacy policies. Id. at 31 (documents written in “legalese” are “typically overwhelming” to the average consumer) (quotations omitted). The Report encouraged “reduced length and greater simplicity and clarity” in privacy disclosures. Id. at 33.
150. The Report suggested the need to promote development of “flexible but enforceable codes of conduct,” to address “emerging technologies and issues not covered” by current fair information practices. Id. at 41; see id. at 42 (noting risk that privacy practices may “ossify”). The Report, for example, called for a “review” of the Electronic Communications Privacy Act (“ECPA”), with a view toward “addressing privacy protection in cloud computing and location-based services.” Id. at 63 (citing ECPA, 18 U.S.C. §§ 2701 et seq. (2006)). ECPA, enacted in 1986, protects citizens against unauthorized access to communications systems, but may need to be “updated in light of recent technological changes.” Id. at 64-65 (noting that ECPA was “adopted in the mainframe computing environment” and may not be entirely relevant in “today’s environment of cloud computing, web-based email and applications, and social networking,” where “individuals and U.S. businesses use remote computing resources to a far greater extent that they did 25 years ago”).
151. The Report noted that “[d]isparate approaches” to data privacy can “create barriers” to trade, “harming both consumers and companies.” Id. at 53. The Report reviewed a host of options for “greater harmonization and international operability.” Id. at 54 (citing creation of a global privacy standard, adoption of a treaty or convention to govern cross-border data flows, an enhanced U.S. privacy framework that “can be more easily supported abroad,” increased DOC international advocacy for U.S. interests, more “focused and coordinated” U.S. government advocacy of the U.S. position internationally, creation of “accountability certifications,” such as binding corporate rules, application for “adequacy” status with the E.U., and development of a U.S. framework that “furthers harmonization” of international privacy laws, including the E.U. directive). Id. at 54-55. The Report suggested the possibility of taking harmonization work “to the next level,” by creating “binding trade commitments” to “steer the world toward global privacy protection interoperability.” Id. at 56.
152. The Report suggested the need for a “comprehensive” commercial data security breach framework, using federal preemption, to prevent the “maze” of disparate state laws from becoming “costly and burdensome” to business. Id. at 57 (quotations omitted). Any new federal privacy framework should, however, “seek to balance the desire to create uniformity and predictability across State jurisdictions with the desire to permit States the freedom to protect consumers and to regulate new concerns” from emerging technologies that could “create the need for additional protection . . . .” Id. at 61. Thus, rather than full-scale preemption of state law, the Report suggested “narrowly tailored preemption,” which might include empowering state attorneys general to en-
The Commerce Report recommended broad adoption of “Fair Information Practice Principles,”¹⁵³ to “help close gaps in current policy, provide greater transparency, and increase certainty for business.”¹⁵⁴ The Report proposed a “baseline commercial data privacy framework” built on an “expanded set” of these principles.¹⁵⁵ Such baseline privacy rules could “help bridge domestic and international frameworks” for privacy and “give both industry and consumers a framework they can understand and manage.”¹⁵⁶ A fair information framework, moreover, could “increase clarity and promote informed consent for consumers” while providing “certainty for consumers, industry, and U.S. trading partners . . . .”¹⁵⁷

The Commerce Report recommended creation of a “privacy office” within the DOC to work with other agencies, including the FTC, to “convene multi-stakeholder discussions,” and to “lead an international outreach” for development of commercial data privacy policies.¹⁵⁸ The Report suggested the use of this privacy office within the DOC to address, through multi-stakeholder discussions, “new commercial data privacy challenges as they arise . . . .”¹⁵⁹ The

force federal law. Id. at 62 & n.174 (noting that CAN-SPAM Act, 15 U.S.C. § 7706(f), permits state attorneys general to bring civil actions in federal court on behalf of citizens of a state).


¹⁵⁴. COMMERCE REPORT, supra note 134, at vii.

¹⁵⁵. The Commerce Report noted a “continuum of risks” to privacy, “ranging from minor nuisances and unfair surprises, to disclosure of sensitive information in violation of individual rights, injury or discrimination based on sensitive personal attributes that are improperly disclosed, actions and decisions in response to misleading or inaccurate information, and costly and potentially life-disrupting identity theft.” Id. at 1. Even harms at the less severe end of the spectrum can produce “significant adverse effects,” because they “undermine consumer trust” in the internet environment. Id.

¹⁵⁶. Id. at 23-24 (quotations omitted).

¹⁵⁷. Id. at 24. The Report noted that fair information practices are “well-established” both in the U.S. and in “numerous international frameworks.” Id. at 25. The Department of Homeland Security, for example, has created a comprehensive set of guidelines, including: transparency, individual participation, purpose specification, data minimization, use limitation, data quality and integrity, security and accountability and auditing. See id. at 26 and & n.72 (citing DHS guidance at www.dhs.gov). Further, OECD, the EU and APEC all have developed such principles on an international level. See id. at 25.

¹⁵⁸. Id. at 44-46; see id. at 46 n.126 (noting proposal to “conven[e] councils of interested parties throughout the U.S. . . . to help elaborate best practices and narrow perceived differences” in privacy standards) (internal quotation marks omitted).

¹⁵⁹. Id. at 47. The alternative, “rulemaking,” could “take years” and produce out-of-date rules, in an era where new uses of personal information may be “measured in weeks or months,” not years. Id.
The John Marshall Law Review

The Report suggested that the DOC privacy office work with the FTC, which would "continue to make independent policy contributions to the domestic and global privacy dialogue."\[160\] The Report also noted the recent creation of a federal interagency task force to address privacy issues.\[161\]

The Commerce Report suggested that FTC enforcement is integral to the implementation of both the law and effective codes of conduct.\[162\] To help persuade industry to expend more effort in formulating and following such codes, the Report suggested a "carrot" and "stick" approach. The "carrot" would consist of a safe harbor program—similar to the existing U.S./E.U. safe harbor system—in which voluntary codes that meet certain requirements would enjoy a presumption of compliance in order to avoid FTC enforcement. The "stick" would include an increase in the level of FTC enforcement against violations of law.\[163\] The Report suggested that "[b]aseline commercial data privacy legislation could give the FTC a specific statutory basis for bringing privacy-related enforcement actions,"\[164\] and that the FTC should "remain the lead ..."

---

\[160\] Id. at 48. The Commerce Report suggested, for example, that a DOC privacy office could enable implementation of a "Do Not Track" system, to help internet users express a "uniform and persistent choice" to "opt out of online behavioral advertising . . . ." Id. at 47 & n.129 (noting that technical mechanisms of "Do Not Track" "may take some work to implement") (internal quotation marks omitted).

\[161\] The White House announced the new interagency group in October 2010. See Cameron Kerry & Christopher Schroeder, White House Council Launches Interagency Subcommittee on Privacy & Internet Policy (Oct. 24, 2010), http://www.whitehouse.gov/blog/2010/10/24/white-house-council-launches-interagency-subcommittee-privacy-internet-policy (noting the Obama Administration’s creation of the subcommittee to bring consensus to internet policies). The subcommittee, co-chaired by representatives from the Commerce Department and the Justice Department, will operate under the auspices of the National Science and Technology Council, with input from more than a dozen cabinet-level and independent federal agencies. Id. The stated purpose of the group is to "strike the appropriate balance between the privacy expectations of consumers and the needs of industry, law enforcement and other public-safety governmental entities, and other Internet stakeholders." Id.; see also Elizabeth Montalbano, White House Unveils Internet Privacy Committee, INFORMATIONWEEK (Oct. 25, 2010, 12:05 PM), http://mobile.informationweek.com/10243/show/6050a0c3e8ec2c0e8642385b8bb60&t (describing formation and purpose of group, and noting "so far no comprehensive policy has been developed in the United States to cover consumer privacy . . . .").

\[162\] COMMERCES REPORT, supra note 134, at 43.

\[163\] Id. at 43-44.

\[164\] Id. at 51. The Commerce Report noted that auditing and accountability play a "critical role," since "the value of transparency, purpose specification, and use limitations ultimately depends on how well organizations follow the practices to which they are bound." Id. at 40. A "means of verifying" that an organization actually observes its stated limits on data use, moreover, "is essential to building and maintaining consumer trust." Id. The Report also suggested the use of "privacy impact assessments" as a way to "require organizations to identify and evaluate privacy risks . . . ." Id. at 34. Such "PIAs" could
Regulating Online Behavioral Advertising

The Commerce Report did not “express a commitment to specific policy proposals” but suggested such proposals might be considered in future white papers. The Report, however, emphasized the need to avoid “fragmented, prescriptive, and unpredictable rules,” which can “frustrate innovation and undermine consumer trust . . . .” Yet, the Report also lauded the “current framework of fundamental privacy values (with constitutional foundations), flexible and adaptable common law and consumer protection statutes, [FTC] enforcement, open government, and multi-stakeholder policy development,” which has “encouraged innovation and provided effective privacy protections.” The Report aimed to strengthen this framework, to help “maintain[] the consumer trust that nurtures the Internet’s growth,” and to encourage companies to “develop and abide by their own best practices.” The Report invited public comments on more than fifty follow-up questions and described its summary of issues as “just a beginning” meant to raise “new questions” to help “induce organizations to think through” how their information practices comport with fair information principles, but would not necessarily “impose any requirements or constraints on technical design or information practices.”

Id. at 36.
165. Id. at 51.
166. Id. at 2.
167. Id. at iii. The Report noted that “[t]he range of services, business models, and organizational structures . . . counsel against attempting to develop comprehensive, prescriptive rules” in a fair information framework. Id. at 32.
168. Id. at iii (Foreword). The Commerce Report suggested that government can “coordinate” the process of formulating “clear and sufficient” rules to protect personal data in the commercial context, “not necessarily by acting as a regulator, but rather as a convener of the many stakeholders—industry, civil society, academia—that share [an] interest in strengthening commercial data privacy protections.” Id. at vi. The Report noted that a “similar approach,” using a “hybrid, public-private system” to regulate privacy practices, first emerged in the 1990s, with early development of the Internet. Id. The Report suggested that a “renewed commitment” to this approach was required to “create a stronger commercial data privacy framework.” Id.
169. Id. at iii. The Commerce Report noted that U.S. commercial data privacy policy “is different in form from many frameworks around the world.” Id. The Report suggested a need to strengthen U.S. privacy protections to “support U.S. leadership in global commercial data privacy” policy discussions. Id.
170. Id.
171. More than one hundred public comments in response to the Commerce Report are available for review at http://www.ntia.doc.gov/comments/101214614-0614-01/.
172. COMMERCE REPORT, supra note 134, at v. The Commerce Report noted the formation of an inter-agency group to “develop principles and strategic directions based on a complete understanding of all sides” of the issues surrounding privacy and Internet policy. Id. at 66. The Report, the DOC suggested, “should be seen as one step in an ongoing conversation, rather than a
thinking on commercial data privacy."\textsuperscript{173}

Supporters of the Commerce Report applauded the proposed creation of a "privacy bill of rights."\textsuperscript{174} Critics, however, suggested that the Commerce Report was "friendl[y] to [the] industry\textsuperscript{175} and that the DOC is the wrong place for a privacy office because it is more focused on promoting U.S. business than on consumer protection.\textsuperscript{176} Observers also noted that the DOC approach could set off a turf battle with the FTC.\textsuperscript{177} Other critics suggested that the statement of settled Administration policy views." The Report intended to "spur further discussion with affected stakeholders," in order to help "develop an action plan in this important area" Id. at 69.

\textsuperscript{173} Id. at v.


\textsuperscript{177} Declan McCullagh, \textit{Commerce Dept. Suggests New Privacy Regulations}, CNET (Dec. 16, 2010, 10:52 AM), http://news.cnet.com/8301-31921_3-20025899-281.html; see also Sal Gentile, \textit{Commerce Department Calls for Online 'Privacy Bill of Rights,' but Advocates Balk}, PBS.ORG (Dec. 16, 2010), http://www.pbs.org/wnet/need-to-know/the-daily-need/commerce-department-calls-for-online-privacy-bill-of-rights-but-advocates-balk/5820/ (noting FTC comment that DOC is "focused more on encouraging innovation and job creation than regulating Internet privacy," but suggesting that the Report will "make a significant contribution" to debate about how best to "protect the privacy of American consumers") (internal quotation marks omitted).
Regulating Online Behavioral Advertising

DOC proposals could "significantly undercut the economic engine of the free Internet, namely advertising." 

IX. PRIVATE AND STATE LITIGATION

The Commerce Report noted a sharp disagreement on the role that private litigation may play in enforcing a privacy framework. On the one hand, the threat of such litigation can "provide a potent incentive for organizations to keep personal data secure." Yet, the potential for large damage awards could produce significant hurdles when companies "seek insurance and contract with other entities that handle personal data."

The use of private rights of action as a significant basis for privacy rights enforcement, to date, has not been particularly effective.

178. Rob Spiegel, Critics Fret over Commerce Dept.'s Internet Privacy Plan, E-COMMERCE TIMES (Dec. 17, 2010, 9:17 AM), http://www.ecommerctimes.com/story/71483.html?wlc=1308170198 (quoting Adam Their, senior research fellow at Mercator Center who stated that the proposals involve "embarking on a fairly serious new regulatory reign"); see also Lauren McKay, Eye on the Customer, CUSTOMER RELATIONSHIP MGMT. (Jan. 2011), available at http://www.destinationcrm.com/Articles/Editorial/Magazine-Features/Eye-on-the-Customer-72857.aspx (noting that "too many privacy regulations will hinder a company's ability to compete").

179. COMMERCE REPORT, supra note 134, at 29. Some comments warned of "significant underenforcement" of privacy interests without the private right to bring actions for privacy violations. Id. Privacy litigation, to date, has achieved some success, at least, in "rais[ing] the consciousness of Internet companies about the importance of privacy to their relationship with consumers." Seth Richard Lesser, Internet Privacy Litigation and the Current Normative Rules of Internet Privacy Protection, CTR. FOR DEMOCRACY & TECH. (Dec. 22, 2007), http://old.cdt.org/privacy/ccp/privaterightofaction2.shtml (stating that "virtually every significant Internet company has appointed an officer responsible for privacy matters," and "blatant disregard of Internet user privacy no longer appears a viable option . . ."). These lawsuits have also "heightened media attention." Id. Supporters thus suggest the "importance of a private right of action to protect whatever privacy interests exist," because "the reality is that it is often the threat of private litigation that prompts corporations to take notice." In fact the FTC has resources only to pursue the "worst privacy offenders." Id.; Kashmir Hill, Will a "Privacy Bill of Rights" Include the Right to Class Action Lawsuits?, FORBES (Dec. 20, 2010, 12:31 PM), http://blogs.forbes.com/kashmirhill/2010/12/20/will-a-privacy-bill-of-rights-include-the-right-to-class-action-lawsuits/ (explaining that "class action lawsuits over privacy violations have been one of the primary mechanisms for consumers to essentially punish companies that have done privacy wrong").

180. COMMERCE REPORT, supra note 134, at 29.

181. See Gary Clayton, Privacy and Security Litigation and Enforcement: Growing Risks for Businesses?, IRMI.COM (May 2007), http://www.irmi.com/expert/articles/2007/clayton05.aspx (noting that the lack of an "obvious private right of action" for infringement of online privacy, coupled with the "difficulty in proving damages," has "limited the litigation" in this area; but also suggesting that litigation "normally follows significant government enforcement actions," and the litigation environment "may change with new legislative and
has been the absence of any specific “statute or law creating comprehensive privacy rights.”

Thus, plaintiffs have been forced to pursue “novel theories of liability” using statutes “intended for quite limited” purposes. The ECPA statute, for example, essentially aims to extend prohibitions on illegal wiretapping to computer-based communications, but the statute is written narrowly, serving as a poor vehicle to address privacy injuries related to OBA. Additional, and relatively novel, theories—such as trespass and unjust enrichment—similarly require courts to stretch traditional concepts in order to fit the online context.

Litigation based on novel applications of existing law, however, may permit development of a common law of privacy, which


183. Id. at 2; see id. at 9-19 (summarizing cases).

184. See In re Pharmatrak, Inc. Privacy Litig., 329 F.3d 9, 21 (1st Cir. 2003) (noting “concern” about interpretation of ECPA, which was “written prior to the widespread usage of the Internet,” in a case involving “online communications”); United States v. Councilman, 245 F. Supp. 2d 319, 321 (D. Mass. 2003) (commenting that “technology has, to some extent, overtaken language”); In re Doubleclick Inc. Privacy Litig., 154 F. Supp. 2d 497, 526 (S.D.N.Y. 2001) (noting absence of evidence in legislative history that Congress intended to prohibit use of cookies on hard drives for advertising purposes). Indeed, as one court suggested, “Congress is aware” of OBA practices, and “is sensitive to the privacy concerns it raises,” as evident in the fact that Congress is considering legislation in the area, and “Congress appears to have drawn the parameters of its regulation carefully and is actively engaged in the subject matter.” Therefore, the courts should not “stray” from the limited intent of existing legislation, to find a private right of action to regulate alleged OBA wrongdoing. Id.

185. See Carome, Jain & Richards, supra note 182, at 23-34 (noting issues as to who is a “party” to communications, the meaning of the term “interception,” the narrow concept of “contents,” “consent” defense, and other obstacles to pursuing ECPA remedies). ECPA is “largely intended to deal with individual cases of intentional interception,” rather than “mass privacy torts.” Id. at 34.

186. See generally Blake T. Bilstad & Keith P. Enright, Consumer Privacy, BERKMAN CTR. FOR INTERNET AND SOCY (2001), http://cyber.law.harvard.edu/ecommerce/privacy.html (stating that “current American privacy law contains almost no general prohibitions against the collection of consumer data” and that due to absence of “specific legislation,” consumer suits have proceeded under “many different legal theories”).
can address new technologies and threats as they arise. In one recent case, litigation and attendant publicity brought an immediate change in online information-gathering practices for an offending website. Litigation based on state privacy laws, moreover, can contribute to changes in market practices. State attorneys general, for example, have increasingly stepped into the field of privacy law enforcement. Yet, levels of state government inte-


188. See Kashmir Hill, Class Action Lawsuit Filed Over YouPorn History Sniffing, FORBES (Dec. 6, 2010, 7:04 AM), http://blogs.forbes.com/kashmirhill/2010/12/06/class-action-lawsuit-filed-over-youporn-history-sniffing/ (noting that the site removed “history-sniffing” code from its operation, shortly after filing of lawsuit). Plaintiffs in that suit were represented by a law firm that has brought other suits for (alleged) improper tracking of online behavior. See also Wendy Davis, McDonald’s, CBS, Mazda and Microsoft Sued For ‘History Sniffing,’ MEDIAPOSTNEWS (Jan. 3, 2011, 8:15 AM), http://www.mediapost.com/publications/?fa=Articles.showArticle&artaid=142144 (explaining how lawsuits were brought against major companies for violation of privacy).

189. See BALLON, supra note 38 at § 26.05 (noting “proliferation” of state laws on privacy, and suggesting that “[e]ven in the absence of federal legislation,” state laws, such as California legislation, “effectively compelled businesses that operate on a national basis to post privacy policies,” which then became subject to enforcement by the FTC); see also Patricia Covington & Meghan Musselman, Recent Developments Affecting Privacy in 2007, 63 BUS. LAW. 639, 639 (2008) (noting that most expansion of data privacy and security law “took place in the laboratories of democracy—the states”); Stephen F. Ambrose, Jr. & Joseph W. Gelb, Consumer Privacy Regulation, Enforcement, and Litigation in the United States, 58 BUS. LAW. 1181, 1181 (2003) (“[P]rivacy litigation and enforcement actions from state attorneys general and private plaintiffs continued to proliferate.”).

190. See Covington & Musselman, supra note 189, at 647 (stating that the “attorneys general have been escalating their enforcement efforts with respect to privacy and data security issues”); see also David C. Vladeck, Dir., FTC Bureau of Consumer Protection, Remarks to Ohio Attorney General’s Consumer Protection Summit (Mar. 4, 2010), available at http://www.ftc.gov/speeches/vladeck/100304ohiospeech.pdf (noting that the FTC is a “relatively small agency” and to serve consumers well it must “form partnerships and leverage resources” with state attorneys general and state agencies); Meredith Fuchs & Marcus Maher, Taking Privacy Policies Seriously—State Attorneys General Are on the Case, PRIVACY OFFICERS ADVISOR (Nov. 2001), available at https://www.privacyassociation.org/assets/advisor/POA%200111.pdf (noting that state attorneys general are working to enforce privacy policies on web-
est in and resources to address privacy concerns vary, which can result in unpredictability in the degree of enforcement from state to state and inefficiency for business in responding to conflicting directions. Indeed, some commentators suggest that the FTC is in the best position to coordinate national enforcement on privacy matters. The FTC has, among other things, focused on issues of online consumer privacy for more than a decade.

X. PROPOSED LEGISLATIVE SOLUTIONS

In May 2010, Representatives Rick Boucher and Cliff Stearns released a discussion draft of a bill, aimed at requiring “notice to and consent of an individual prior to the collection and disclosure of . . . personal information relating to that individual.” In July


192. See Ronald Plesser & Stuart P. Ingis, Limiting Private Rights of Action In Privacy Litigation, CTR. FOR DEMOCRACY & TECH. (Jan. 5, 2007), http://old.cdt.org/privacy/ccp/privateRightofAction1.pdf (noting that the FTC and other agencies are “much less likely to bring lawsuits for technical violations,” and, because of limited resources, more likely to “focus their attention on situations where injury occurs”); see id. (noting that Children’s Online Privacy Protection Act and Gramm-Leach-Bliley law contained no provisions for private rights of action, and stating that “[t]he threat of FTC or other [agency] enforcement action has proven a highly effective means of ensuring compliance . . . .”). FTC Consumer Protection Division Director David Vladeck recently noted that the FTC is “always looking to partner with other enforcement agencies.” See David Vladeck, Dir., FTC Bureau of Consumer Protection, Remarks to International Association of Privacy Professionals (Dec. 7, 2010), available at http://www.ftc.gov/speeches/vladeck/101207vladeckspeechto iapp.pdf (stating that the FTC “cooperate[s] closely with the states”).

193. Since 2001, the FTC has brought at least twenty-three actions against companies that allegedly failed to provide reasonable protections for sensitive consumer information. FTC 2009 REPORT, supra note 52, at 5 n.8 (2009). It has become “fundamental FTC law and policy” that companies must “deliver on promises they make to consumers about how their information is collected, used, and shared.” Id. at 40. Thus, “a company cannot use data in a manner that is materially different from promises the company made when it collected the data without first obtaining the consumer’s consent.” Id.; See also id. nn.71-72 (citing FTC enforcement cases). More generally, the FTC has been involved in enforcing privacy laws over some forty years. See generally Jon Leibowitz, Chairman, Fed. Trade Comm’n, Remarks in Preliminary FTC Staff Privacy Report (Dec. 1, 2010), available at http://www.ftc.gov/speeches/leibowitz/101201privacyreport remarks.pdf (noting the FTC’s extensive experience in educating businesses and consumers on privacy law enforcement).

2010, Representative Bobby Rush introduced a bill, “[t]o foster transparency about the commercial use of personal information, [and] provide consumers with meaningful choice about the collection, use, and disclosure of such information . . . .” These bills and related issues were the subjects of congressional hearings in July and December 2010.

The Boucher and Rush bills both encompassed certain key common provisions. First, both bills required that companies collecting personal information about an individual disclose...
their privacy policies.\textsuperscript{200} Both bills also mandated that companies establish procedures to ensure the accuracy and security of information.\textsuperscript{201}

Second, both bills permitted companies to obtain consent to gather information through an opt-out system.\textsuperscript{202} Both bills required affirmative opt-in consent for the distribution of information to third parties, for the gathering of sensitive information about an individual, and for material retroactive changes in a company's privacy policies.\textsuperscript{203} Both bills also required affirmative consent for the collection of "all or substantially all" of a person's online activity.\textsuperscript{204}

Finally, both bills called for enforcement of the law by the FTC;\textsuperscript{205} they granted the FTC rulemaking authority to implement the law.\textsuperscript{206} In addition, both bills granted concurrent enforcement authority to each state's attorney general,\textsuperscript{207} yet established at least a limited form of federal preemption.\textsuperscript{208} The Boucher Bill excluded any private right of action based on the law,\textsuperscript{209} whereas the Rush Bill would have permitted such an action if a company "willfully fail[ed] to comply."\textsuperscript{210} The Rush Bill, moreover, established a form of safe harbor for companies that engaged in an approved self-regulatory program.\textsuperscript{211}

The FTC and the DOC weighed in on both of these bills throughout the course of hearings in 2010. The FTC generally supported the legislation but emphasized the need for "short, clear" disclosures of privacy practices, so that consumers might "compare privacy protections offered by different compa-

\textsuperscript{200} Compare Boucher Bill, § 2(5), with Rush Bill, § 2(4). Both bills also used the term "preference profile" to refer to information about a person's online behavior. Compare Boucher Bill, § 2(8). with Rush Bill, § 2(6). Both bills used the term "sensitive information" to refer to medical, race, religious, sexual orientation, financial and geolocation information. Compare Boucher Bill, § 2(10), with Rush Bill, § 2(8).

\textsuperscript{201} Compare Boucher Bill, § 3(a), with Rush Bill, §§ 101-02.

\textsuperscript{202} Compare Boucher Bill, § 4, with Rush Bill, §§ 201-02, 301.

\textsuperscript{203} Compare Boucher Bill, § 3(a)(3), with Rush Bill, § 103.

\textsuperscript{204} Compare Boucher Bill, §§ 3(a)(4), 3(b), 3(c), 6, with Rush Bill, §§ 104-05. Mere "transactional" or "operational" gathering of information (for purposes of fulfilling a consumer's requests) would not require any form of consent. Compare Boucher Bill, § 3(a)(5), with Rush Bill, §§ 103(e)-(f), 106.

\textsuperscript{205} Compare Boucher Bill, § 3(d), with Rush Bill, § 104(c).

\textsuperscript{206} Compare Boucher Bill, § 8(a), with Rush Bill, § 602.

\textsuperscript{207} Compare Boucher Bill, § 8(a)(3), with Rush Bill, § 602(c).

\textsuperscript{208} Compare Boucher Bill, § 8(b), with Rush Bill, § 603.

\textsuperscript{209} Boucher Bill, § 10, with Rush Bill, § 605(a).

\textsuperscript{202} Compare Boucher Bill, § 8(a)(5), with Rush Bill, §§ 103(e)-(f), 106.

\textsuperscript{210} Rush Bill, § 604(a).

\textsuperscript{211} See Rush Bill, §§ 401 (designating the safe harbor provision), 402 (requiring FTC approval of "Choice Program," to be eligible for safe harbor), and 403 (outlining the requirements of the self-regulatory program).
The FTC also questioned whether transfers of information between affiliates of a company should be permitted absent express consent because consumers may be unaware that some companies have a countless number of affiliates. Finally, the FTC emphasized the need for simplicity in privacy choices and suggested that the bills, which might permit multiple forms of consent-gathering mechanisms, could "add[] to consumer confusion."

The DOC suggested the need for limitations on the scope of the bills. Further, the DOC suggested that the opt-out consent requirement should not apply to "first-party" use of information and that the opt-in consent should only apply to the most sensitive data categories. The DOC also questioned the value of any private right of action and suggested that requiring extensive FTC rulemaking to implement the law could cause "needless regulatory uncertainty."


213. Id. at 22.

214. Id. The FTC emphasized the need for an understandable and simple choice mechanism, suggesting that a "Do Not Track" method, which uses a browser-based mechanism, might provide a universal choice system. See House Dec. Hrg., supra note 195, at 16-18 (statement of David Vladeck, Dir., FTC Bureau of Consumer Protection), http://democrats.energycommerce.house.gov/documents/20100722/Vladeck.Testimony.07.22.2010.pdf (stating that the FTC supports "more uniform and comprehensive consumer choice mechanism for online behavioral advertising . . .").

215. See House July Hrg., supra note 196, at 4-5 (statement of Jason D. Goldman, Counsel, Telecommcn & E-Commerce for the U.S. Chamber of Commerce), http://democrats.energycommerce.house.gov/documents/20100722/Goldman.Testimony.07.22.2010.pdf (noting that the scope of "covered information" should be limited, that there is need to establish standards of "personal information," and that the question of geolocation information should be left to self-regulatory regimes).

216. See id. at 5 (requiring that opt-out consent be obtained for "all consumers for any data that may be collected or used under any circumstances" would adversely impact businesses).

217. Id. at 6. The broad requirement for opt-in consent "profoundly alters commonly accepted business practices." Id.

218. See id. at 7 (noting valid concerns about liability provisions, such as a grant of concurrent enforcement power to states, which could "impose duplicative and potentially inconsistent findings" on businesses). The DOC noted, in particular, "the explicit grant of authority for the award of punitive damages and attorney's fees will serve to increase the likelihood that elements of the plaintiffs' class action trial bar will use this legislation as a way to increase class action litigation with little benefit" to the public. Id.

219. See id. at 7 (noting the sheer number of rulemakings required under proposed bills); See also House Dec. Hrg., supra note 195, at 7, 11 (statement of Daniel J. Weitzner, Assoc. Adm'r for Policy Analysis & Dev., Nat'l Telecommcn's & Info. Admin. for the U.S. Dept of Commerce), http://republicans.energycommerce.house.gov/Media/file/Hearings/CTCP/2010-
Supporters of the bills considered the legislation long overdue and pointed to a combination of self-regulatory efforts and safe harbor provisions as the most effective means to implement fair information practice principles. Indeed, this co-regulatory approach, supporters claimed, could provide flexibility to industry while ensuring the FTC authority to provide oversight in approving and enforcing guidelines.

Some critics, however, called on Congress to strengthen the proposals to focus on data minimization, to work with the EU to develop a meaningful global framework of privacy, and to rely on specific legislative guidelines and unlimited private rights of action to avoid the delay that rulemaking and self-regulatory efforts might engender. Other critics noted the inherent risks of regula-
tion, and suggested that a self-regulatory structure, with no private rights of action and no extensive consent requirements, would avoid the potential barrage of meritless lawsuits and economic harms that could arise under the proposed bills. The mid-term elections in 2010 clearly did not eliminate online privacy as an important issue for congressional and agency consideration. Indeed, in the lame duck session of Congress at the end of 2010, Congress passed and the President signed into law the “Restore

Online Shoppers' Confidence Act," which aims at protecting consumer financial information online.\textsuperscript{225} The new year saw additional hearings and the introduction of further legislative proposals in Congress.\textsuperscript{226} In February 2011, Representative Speier introduced "Do Not Track" legislation in Congress.\textsuperscript{227} In March 2011, the Senate Committee on Commerce, Science and Transportation conducted hearings on the state of online consumer privacy.\textsuperscript{228} In April 2011, Senators Kerry and McCain drafted and later proposed a "Commercial Privacy Bill of Rights,"\textsuperscript{229} which would establish rights to notice, consent, access

\begin{quote}
\begin{footnotesize}

\textsuperscript{226} See Statement by FTC Chairman Jon Leibowitz Regarding House and Senate Passage of Legislation to Combat Deceptive Online Sales Tactics, F.T.C. (Dec. 15, 2010), http://www.ftc.gov/opa/2010/12/negoption.shtm (applauding the Act, which prohibits data pass practices, whereby online retailers share their customers' billing information (including credit card numbers) with "third-party" sellers, who sometimes use aggressive and misleading sales tactics to charge consumers for goods they have not ordered).

\textsuperscript{227} See Kaye, supra note 224 (noting plans in both House and Senate to introduce bills on online privacy and the "Do Not Track" proposal).


\end{footnotesize}
\end{quote}
and correction of information, but would not endorse a “Do Not Track” system. Equivalent state developments may also advance. In April 2011, a California legislator introduced a bill to establish a state form of the FTC’s proposed “Do Not Track” system. And most recently, in June 2011, the Senate Committee conducted another hearing on Privacy and Date Security.

XI. ONLINE BEHAVIORAL ADVERTISING AS A CHALLENGE TO REGULATORY SYSTEMS

The controversy over OBA has raged for at least a decade, and shows little sign of abating. The persistence and intensity of


234. See Privacy and Data Security: Protecting Consumers in the Modern World: Hearing Before the Subcomm. on Commerce, Sci., & Transp., 112th Cong. (June 29, 2011), available at http://commerce.senate.gov/public/index.cfm?FuseAction=Hearings&ContentRecord_id=e2c2a2ca-91d6-48a2-b5ea-b5c4104bd977&ContentType_id=14f995b9-dfa5-407a-9d35-56cc7152a7ed&Group_id=b06c39af-e033-4cba-922-de668ca1978a (discussing issues of data breach while failing to come to an agreement on privacy laws); see also Cecilia Kang, Senate Lawmakers Call for Data Security Law, Less Certain over Privacy, WASH. POST BLOG (June 29, 2011, 12:15 PM), http://www.washingtonpost.com/blogs/post-tech/post/senate-lawmakers-call-for-data-security-law-less-certain-over-privacy/2011/06/29/AGGFTqH_blog.html (quoting Senator Pat Toomey of Pa.) (“On data security, there is broad support for a national standard... and certainly an issue that Congress is likely to address legislatively in the near future. ... On the broad issue of privacy, I'm not sure there's a broad consensus. I'm sure no one on the committee wants to break the Internet.”).

235. See Juan Martinez, Marketing Mauraders or Consumer Counselors?
the debate over OBA regulation suggests much about the dilemmas of government regulation in the modern age. Privacy, like many other aspects of modern culture, is a matter of some subjectivity, and attitudes toward privacy have changed over time.


237. See ROBERT ELLIS SMITH, BEN FRANKLIN'S WEB SITE: PRIVACY AND CURIOSITY FROM PLYMOUTH ROCK TO THE INTERNET 8 (2000) (noting that modern attitudes toward privacy are largely a reaction to technologies, such as cameras, telephones and other methods that make physical privacy alone less relevant in determining the limits of privacy concerns); Eve M. Caudill & Patrick E. Murphy, Consumer Online Privacy: Legal and Ethical Issues, 19 J. OF PUB. POLY & MKTG. 7 (2000) (noting that “[m]arketers have long collected data to assist in making decisions,” and “[p]rivacy as it relates to consumer information is not a new problem in marketing,” but “anonymity changes when consumers move onto the Internet. No longer are their shopping behaviors available only in the aggregate” to marketers); see also Jake Nevrla, Voluntary Surveillance: Privacy, Identity and the Rise of Social Panopticism in The Twenty-First Century, COMM-ENTRY (2009-2010), http://www.unh.edu/communication/medias/pdf/commentary/Comm-entry2010.pdf ("Societal norms have inevitably adapted to this new medium of communication and the level of surveillance that has come with it . . . . [S]ociety has become increasingly immersed in the culture of perpetual sharing.").
Some consumers may be “privacy fundamentalists” while others may be “privacy pragmatists.” Depending on how the question is asked, consumers may express greater or lesser concerns about privacy, and greater or lesser interest in obtaining low-cost (or free) content. Conversely, the precise value of targeted infor-

238. Dr. Alan Westin, who has conducted dozens of privacy surveys, essentially coined the terms “privacy fundamentalist” and “privacy pragmatist.” Alan F. Westin, Social and Political Dimensions of Privacy, 59 J. SOC. ISSUES 431 (2003), available at http://www.privacysummersymposium.com/reading/westin.pdf. Westin’s methodology is more refined than these simple terms suggest, and his results have been the subject of some academic criticism. See Ponnurangam Kumaraguru & Lorrie Faith Cranor, PRIVACY INDEXES: A SURVEY OF WESTIN’S STUDIES, CARNEGIE MELLON UNIV. SCH. OF COMPUTER SCI. 20 (Dec. 2005), http://reports-archive.adm.cs.cmu.edu/anon/isri2005/CMU-ISRI-05-138.pdf (concluding that many of the questions from Westin’s surveys included pejorative terms like “fundamentalist” to refer to privacy advocates and that the questions “were usually asked in the context of studies commissioned by corporations that intended to use the results as part of their efforts to influence the public policy process.”).

239. Compare Joseph Turow, Jennifer King, Chris Jay Hoofnagle, Amy Bleakley & Michael Hennessy, Contrary to What Marketers Say, Americans Reject Tailored Advertising and Three Activities that Enable It, GRAPHIC8NYTIMES.COM (Sept. 2009), http://graphics8.nytimes.com/packages/pdf/business/20090929-Tailored_Advertising.pdf (stating that 66% of adults surveyed answered “no” to question: “Do you want websites you visit to show you ads that are tailored to your interests?”) with Zogby International, Results From Interactive Survey, EDUC. WEEK (Aug. 24, 2010), www.edweek.org/media/finalsadultstopline8-24-10updated.pdf (finding that forty-five percent of adults and fifty-one percent of parents answered “no” to the question: “Would you prefer to pay for services currently provided for free on search engines and social networking sites in lieu of having information about you sold to advertisers?”). One commentator, noting the discrepancies in such polls, observed: “The methodology of opinion polls necessarily affects respondents’ mental calculations, rendering polls not just easily manipulated but inherently unreliable as indicators of real preferences . . . . The easiest way to bias the results of a poll is to omit any mention of the trade-offs at issue.” Berin Szoka, Privacy Polls v. Real-World Trade-Offs, THE PROGRESS & FREEDOM FOUNDATION (Nov. 2009), http://www.pff.org/issues-pubs/ps/2009/ps5.10-privacy-polls-tradeoffs.html; see also H. Brian Holland, Internet Expression in The 21st Century: Where Technology and Law Collide: Privacy Paradox 2.0, 19 WIDENER L.J. 893, 893 (2010) (describing “privacy paradox” in which individual stated intentions about privacy protection differ from actual behavior); Alessandro Acquisti, Privacy in Electronic Commerce and the Economics of Immediate Gratification, PROCEEDINGS OF THE 5TH ACM CONFERENCE ON ELEC. COMMERCE (2004), available at http://www.heinz.cmu.edu/~acquisti/papers/privacy-gratification.pdf (noting “dichotomies” between expressed attitudes on privacy and behaviors in commerce); see generally Alessandro Acquisti & Jens Grosslags, Privacy Attitudes And Privacy Behaviors, in ECONOMICS OF INFORMATION SECURITY 165-178 (L. Jean Camp ed. 2004) (addressing how despite the number of technologies that have been created to help protect consumer privacy online, many remain unsuccessful); Il-Horn Hann, I.Kai-Lung Hui, Tom S. Lee & I.P.L. Fng, The Value of Information Privacy: Evidence from the USA and Singapore, INTL CONFERENCE ON INFO. SYS. (2002), avail-
formation to advertisers may vary and is the subject of some academic uncertainty.\textsuperscript{240} The degree of individual need for external privacy protection—beyond consumer education—is also subject to some debate.\textsuperscript{241} Consumer education and the development of ad-blocking technologies may affect the degree of need for external regulation


\textsuperscript{241} Thus, as some commentators note, the sophistication of Internet users has grown over time. See Eugene M. Bland, Gregory S. Black \& Kay Lawrimore, \textit{Determinants of Effectiveness and Success for Ebay Auctions}, 4 COASTAL BUS. J. 1, 5 (Spring 2009), http://www.coastal.edu/business/cbj/pdfs/articles/spring2005/bland_black_lawrimore.pdf ("In general, consumers are becoming increasingly sophisticated and have higher expectations than consumers in the past. Marketers can expect consumers who make purchases over the Internet to be even more sophisticated than average consumers. These consumers are computer literate and they are aware of the dangers of purchasing items over the Internet, both in trusting the seller to deliver the product as represented and in making payment and exposing personal information on the Internet."); Miya Knights, \textit{Web 2.0}, IET COMMCS ENG'R, Feb. 1, 2007, at 30, 30 ([U]sers have become more savvy as online tools have become more challenging and complex"); see generally Alfred Kobsa, \textit{Privacy-Enhanced Web Personalization, in THE ADAPTIVE WEB: METHODS AND STRATEGIES OF WEB PERSONALIZATION} 628 (Peter Brusilovsky ed., 2007), http://www.ics.uci.edu/~kobsa/papers/2007-AWBS-privacy-kobsa.pdf (discussing numerous surveys that demonstrate that computer users are very concerned about privacy on the Internet). Further, "reputational" penalties to firms that violate consumer trust "may be among the strongest protections available to consumers." THOMAS LENARD \& PAUL RUBIN, \textit{PRIVACY AND THE COMMERCIAL USE OF PERSONAL INFORMATION}, 42 (2002); see id. at xvii ("The Internet speeds up collection of information about consumers, but it also enables consumers to more easily obtain information about firms' activities on the web."); see also Zhulei Tang, Yu Hu \& Michael Smith, \textit{Gaining Trust Through Online Privacy Protection: Self-Regulation, Mandatory Standards, or Caveat Emptor}, J. MGMT. INFO. SYS., Mar. 1, 2008, at 153, 156, available at http://repository.cmu.edu/cgi/viewcontent.cgi?article=1048&context=heinzworks&sei-redir=1&search=%22Gaining+Trust+Through+Online+Privacy+Protection:+Self-Regulation,+Mandatory+Standards,+Or+Caveat+Emptor%22 (stating that trust is "particularly important" in online markets; to maintain trust, online firms must send "unambiguous signals" to consumers, regarding their intention of protecting privacy).
Similarly, various forms of anonymization may become available, to help consumers avoid unwanted tracking. The regulation of privacy, moreover, necessarily involves a wide array of private groups and government entities have focused on campaigns to promote consumer understanding of online privacy issues. See, e.g., About The Privacy Rights Clearinghouse, PRIVACY RIGHTS CLEARINGHOUSE, http://www.privacyrights.org/about_us.htm (last visited Oct. 2, 2011) (describing mission to “[r]aise consumers’ awareness of how technology affects personal privacy” and “[e]mpower consumers to take action to control their own personal information by providing practical tips on privacy protection.”); TRUSTe, http://www.truste.com/ (last visited Oct. 2, 2011) (“Presenting privacy policies, notices, and choices with more Transparency—in ways that are more easily accessible and understood by consumers; Providing consumers with Choices—options and control—over the use of their personal information; Helping companies and organizations remain Accountable to the privacy obligations they make as well as to consumer choices.”). Many companies—out of fear of government-imposed solutions, or as a way to instill consumer confidence in the use of their sites—have contributed their own efforts at consumer education. See Amy Schatz, Regulators Rethink Approach to Online Privacy, WALL ST. J., Aug. 5, 2009, http://online.wsj.com/article/SB124949972905908593.html (“Internet companies and advertisers . . . have already been trying to stave off government intervention with self-regulatory efforts such as consumer education campaigns and more transparent privacy policies.”); Donna K. Peoples, Instilling Consumer Confidence in E-Commerce, SAM ADVANCED MGMT. J., Sept. 22, 2002, at 26, available at http://findarticles.com/p/articles/mi_hh6698/is_4_67/ai_n28957647/ (noting industry education campaigns to “help consumers understand how to protect their privacy online.”). In supplementing these efforts, most browser purveyors have developed technologies to restrict unwanted digital advertising. See generally Jillian Vallade, AdBlock Plus and the Legal Implications of Online Commercial-Skipping, 61 RUTGERS L. REV. 823 (2009) (noting increased use of ad-blocking technology); Lucian Parfeni, Mozilla Announces 100 Million AdBlock Plus Downloads, SOFTPEDIA (Nov. 17, 2010), http://news.softpedia.com/news/Mozilla-Announces-100-Million-AdBlock-Plus-Downloads-167008.shtml (“every major browser” has built software extensions to block advertising). Ad-blocking technologies, moreover, may increasingly give consumers the ability to choose (through “white-listing”) precisely which kinds of advertising they receive. Clint Ecker, Safely Whitelist Your Favorite Sites and Opt Out of Tracking, ARS TECHNICA (Mar. 11, 2010), http://arstechnica.com/business-guides/2010/03/safely-whitelist-your-favorite-sites-and-opt-out-of-tracking.ars. Nevertheless, some research suggests “consumers often lack information to make privacy sensitive decisions and, even with sufficient information, are likely to trade off long-term privacy for short-term benefits.” Alessandro Acquisti & Jens Grossklags, Privacy and Rationality in Individual Decision Making, IEEE SEC. & PRIVACY, Jan. 2005, at 26, available at http://www.dtc.umn.edu/weis2004/acquisti.pdf; Jens Grossklags & Alessandro Acquisti, When 25 Cents is Too Much: An Experiment on Willingness-to-Sell and Willingness-to-Protect Personal Information, WORKSHOP ON THE ECON. OF INFO. SEC. (WEIS) (2007), http://weis2007.econinfosec.org/papers/66.pdf (describing study that shows clear preference for money over data among a majority of participants even when monetary exchange is “very small”).
trade-offs between protection of privacy versus potentially increased burdens to consumers, or loss of free content (or both).\textsuperscript{244} Regulation to protect privacy could also affect innovation and create barriers to entry into the digital market.\textsuperscript{245}

In short, given these uncertainties, a pure "cost versus benefit" analysis of privacy regulation may become impossible.\textsuperscript{246} Yet, web surfing behavior is to surf anonymously. This can be accomplished by using an anonymous proxy server that randomizes your IP address as you browse the web.

\textsuperscript{244} See Hal R. Varian, \textit{Economic Aspects of Personal Privacy, in INTERNET POLY \& ECON.}, 101 (2009), \textit{available at} http://people.ischool.berkeley.edu/~hal/Papers/privacy/ ("[C]onsumers will rationally want certain kinds of information about themselves to be available to producers and will want other kinds of information to be secret."); UK Office of Fair Trading, \textit{Online Targeting of Advertising and Prices: A Market Study}, OFFICE OF FAIR TRADING (May 2010), http://www.oft.gov.uk/shared_oft/business_leaflets/659703/OFT1231.pdf ("Behavioural advertising has benefits to consumers. Improving the targeting of advertising decreases suppliers' advertising costs and increases revenues for web-publishers. This increased efficiency feeds through to reduced costs for consumers, for example by enabling free access to content. Consumers are also less likely to receive advertisements that are not of interest to them."); Kent Walker, \textit{Where Everybody Knows your Name: A Pragmatic Look at the Costs of Privacy and the Benefits of Information Exchange}, 2000 STAN. TECH. L. REV. 2, 2 (2000), \textit{available at} http://stlr.stanford.edu/pdf/walker-information-exchange.pdf (noting that withholding of personal information may reduce benefits for individuals and society); see generally CHRIS ANDERSON, \textit{FREE: THE FUTURE OF A RADICAL PRICE} 112-18 (2009) (noting impact of internet advertising on no-cost content).

\textsuperscript{245} See Kent Walker, \textit{The Costs of Privacy}, 25 HARV. J. L. \& PUB. POLY 87, 88-89 (2001) (laws regulating privacy may "chill the creation of beneficial collective goods" and reduce consumer choice); See Lenard \& Rubin, \textit{supra} note 241, at xxii (restrictions on advertising may curtail opportunities for competitive entry, since "advertising typically benefits new entrants and small firms more than it does large, established firms"); JOHN E. CALFEE, \textit{FEAR OF PERSUASION: A NEW PERSPECTIVE ON ADVERTISING AND REGULATION} 96 (1997) ("Advertising's promise of more and better information also generates ripple effects in the market. These include enhanced incentives to create new information and develop better products . . . . [M]arkets with advertising are far superior to markets without advertising.").

\textsuperscript{246} See James P. Nehf, \textit{The Limits of Cost-Benefit Analysis in the Development of Database Privacy Policy in The United States}, in RISK AND CHOICE IN CONSUMER SOC'Y 143 (Iain Ramsay et al. eds., 2007) (arguing that cost-benefit analysis "should be de-emphasized and relegated to a 'helpful but not determinative' status"). Indeed, some claim that cost-benefit analysis as a whole provides little effective guidance to regulation. See John S. Applegate, et al., \textit{Reinvigorating Protection of Health, Safety and the Environment} 3 (Ctr. on Progressive Reform, White Paper # 901, 2009), http://www.progressivereform.org/articles/SunsteinOIRA901.pdf ("As practiced in the real world, cost-benefit analysis has proved hopelessly indeterminate—that is, cost-benefit analysis has proved incapable of eliminating those ambiguities and uncertainties that are of such a magnitude that they render it impossible to calculate the costs and/or benefits of a proposed regulation with sufficient specificity to allow any meaningful comparison."); David M. Dreisen, \textit{Regulatory Reform: The New Lochnerism?}, 36 ENVTL. L. 603, 607 (2006) ("Da-
cost-benefit analysis is engrained in the American system of government, and may become more prominent in light of recent political events.\textsuperscript{247} 

\textit{See also} FRANK ACKERMAN \& LISA HEINZERLING, \textit{PRICELESS: ON KNOWING THE PRICE OF EVERYTHING AND THE VALUE OF NOTHING} 233-34 (2004) ("Cost-benefit analysis of environmental policies trivializes the very values that gave rise to those policies in the first place."); Matthew D. Adler \& Eric A. Posner, \textit{Rethinking Cost-Benefit Analysis}, 109 YALE L.J. 165, 167 (1999) ("The reputation of cost-benefit analysis... among American academics has never been as poor as it is today, while its popularity among agencies in the United States government has never been greater."). Others, however, suggest that cost-benefit analysis, at a minimum, can be useful, when setting priorities and evaluating potential candidates for the use of regulatory resources. See E. Donald Elliott, \textit{Only a Poor Workman Blames His Tools: On Uses and Abuses of Benefit-Cost Analysis in Regulatory Decision Making About the Environment}, 157 U. PA. L. REV. 178, 182-84, 188 (2009) (cost-benefit analysis is "inherently imperfect," but "there are no perfect techniques for making complex policy decisions"); Robert W. Hahn, \textit{The Economic Analysis of Regulation: A Response to the Critics}, 71 U. CHI. L. REV. 1021 (2004) ("Summary measures of the impacts of regulation have made important contributions to our understanding of the regulatory process."). To a large extent, moreover, firms already must engage in cost-benefit analysis, as they weigh the value of privacy-and security-enhancing techniques—whether mandated by government, or voluntarily adopted to improve consumer confidence—against the costs of implementing such techniques. See generally DEBRA S. HERRMANN, \textit{COMPLETE GUIDE TO SECURITY AND PRIVACY METRICS: MEASURING REGULATORY COMPLIANCE, OPERATIONAL RESILIENCE, AND ROI} 351 (2007) (noting that organizations differ as to their approach to implementing privacy regulations); Edmund L. Andrews, \textit{Threats and Responses: Liberty and Security; New Scale for Toting Up Lost Freedom vs. Security Would Measure in Dollars}, N.Y. TIMES, Mar. 11 2003, http://www.nytimes.com/2003/03/11/us/threats-responses-liberty-secur-ity-new-scale-for-toting-up-lost-freedom-vs.html (describing the White House Office of Management and Budget requests for economic data from experts regarding the costs of privacy and liberty lost due to tighter security measures). 

In light of the uncertainty as to the best course for regulation of OBA practices, the first question becomes: Should there be any regulation at all? Typically, justification for regulation starts with the observation that some market failure has occurred that prevents cure, or at least mitigation, of a significant problem. Market failures may take many forms: externalities, such as by-products of economic activities like pollution; information deficiencies, such as the inability of average consumers to investigate whether food and drugs are safe; irrationality, such as tendencies toward abuse of addictive, harmful substances; and distributive justice, such as the need to curb discriminatory behaviors. The

---


Legislatures and regulators have long been confronted with uncertainty in decision-making, and have developed an array of tools to respond. See Judith Jones, Regulatory Design for Scientific Uncertainty: Acknowledging the Diversity of Approaches in Environmental Regulation and Public Administration, 19 J. ENVTL. L. 347, 347 (2007) (noting range of regulatory design tools to respond to scientific uncertainty). Yet, cultural attitudes toward government power, and confidence in the ability of government to cure all “social ills” have certainly changed over time. See Jerry L. Mashaw & David L. Harfst, Regulation and Legal Culture: The Case of Motor Vehicle Safety, 4 YALE J. ON REG. 257, 261 (1987) (noting that Vietnam, Watergate, the Challenger disaster and other events have “lowered” expectations of government ability to deal with complex problems).

See Thomas M. Lenard & Paul H. Rubin, In Defense of Data: Information and the Costs of Privacy, TECH. POL’Y INST., 50 (May 2009), http://www.techpolicyinstitute.org/files/in%20defense%20of/o20data.pdf ("Regulation should be undertaken only if the market is not functioning properly."). That regulation may involve both a social concern (protection of privacy) and an economic interest (Internet commerce) does not change the analysis of “market failure” as an essential basis for regulation. See Richard B. Stewart, Regulation in a Liberal State: The Role of Non-Commodity Values, 92 YALE L.J. 1537, 1590 n.1 (1983) ("[E]conomic' regulation . . . includes [both] price, service, and entry regulation to control market power or economic rents, and 'social' regulation (including environmental protection, consumer protection and health and safety . . . regulation), that seek to correct other 'market failures.'").

See Joseph E. Stiglitz, Government Failure vs. Market Failure: Princi-
most common explanations for OBA regulation center on “externalities”—the tendency of ecommerce to create vast quantities of personal data, which may be abused\(^2\) and lack of information—consumer inability to read and understand privacy policies and the mechanics of online information gathering.\(^2\) To a lesser extent, in using the developing science of “behavioral economics,” some argue that consumers act irrationally, in trading off the distant, unknown harms of privacy invasion for the convenience and low cost of the online environment.\(^2\) According to this view, consumers require at least a nudge toward making better choices when using the Internet.\(^2\) Others suggest that this view of consumer irra-


252. See Aleecia M. McDonald, Footprints Near the Surf: Individual Privacy Decisions in Online Contexts 154-55 (Dec. 1, 2010) (unpublished Ph.D dissertation, Carnegie Mellon University), available at http://repository.cmu.edu/cgi/viewcontent.cgi?article=1008&context=dissertations (noting that consumers lack basic knowledge regarding the use and storage of their personal information online); Joseph Turow, Americans & Online Privacy: The System is Broken, ANNEBERG PUB. POLY CTR., 4 (June 2003), http://www.annenbergpublicpolicycenter.org/Downloads/Information_And_Society/20030701_America_and_Online_Privacy/20030701_online_privacy_report.pdf (pointing out that while it may be useless to attempt to educate consumers about online protection due to the speed at which the techniques for bypassing protections are changing, consumers are in favor of laws allowing easy access to information gathered about them online).

253. This position may also involve an argument from coercion. See Scott R. Peppet, Unraveling Privacy: The Personal Prospectus & the Threat of a Full Disclosure Future, NW. U. L. REV. (forthcoming 2011), available at http://ssrn.com/abstract=1678634 (arguing that while some consumers may benefit from positive information disclosures, other consumers may feel coerced into disclosing private information to avoid any negative connotations as to why they choose not to do so).

254. For more information on the notion of a “nudge” function for regulation as well as the concept of “choice architecture” as basis for modifying behavior, see RICHARD H. THALER & CASS R. SUNSTEIN, NUDGE: IMPROVING DECISIONS ABOUT HEALTH, WEALTH AND HAPPINESS 252 (2009); see also DAN ARIELY, PREDICTABLY IRRATIONAL 239-40 (2009) (summarizing development of “behavioral economics” theory); Benjamin Wallace-Wells, Cass Sunstein Wants to Nudge Us, N.Y. TIMES, May 16, 2010, at MM38,
tionality smacks of paternalism. Still others suggest that use of a "precautionary principle" requires that, when faced with uncertainty as to harm, a "better safe than sorry" approach should obtain. Ultimately, the question of market failure is relative, as

http://www.nytimes.com/2010/05/16/magazine/16Sunstein-t.html (noting Cass Sunstein's behavioral economics theory may be used to move people toward more rational behavior). Thus, for example, some suggest that the problem of obesity in society represents "emergence of a sub-optimal choice environment," which can be corrected through modification of food marketing techniques. Paul Anand & Alistair Gray, Obesity as Market Failure: Could a "Deliberative Economy" Overcome the Problems of Paternalism?, 62 KYKLOS 182, 190 (2009); Kelly D. Brownell, et al., Personal Responsibility and Obesity: A Constructive Approach to a Controversial Issue, HEALTH AFFAIRS, March 2010, at 379, available at http://www.yaleruddcenter.org/resources/upload/docs/what/food-obesity/Person alResponsibility_HA_3.10.pdf (stating that personal responsibility can be supported through programs of improved school nutrition, menu labeling, and alteration of food industry marketing practices). Others see forms of regulation to cure obesity as pure paternalism. William Saletan, The Growing Ambitions of the Food Police, SLATE (Sept. 29, 2009, 11:23 AM), http://www.slate.com/id/2229194/; see Adam Ozimek, They Came First for the Sugar, Then They Came for the Salt... , MODEL BEHAVIOR (Apr. 22, 2010), http://modeledbehavior.com/2010/04/22/they-came-first-for-the-sugar-then-they-came-for-the-salt... -ctd/ (posting a letter that humorously hints at the potential for soft paternalism to lead to increasing regulation); see generally Mario J. Rizzo & Douglas Glen Whitman, Little Brother is Watching You: New Paternalism on the Slippery Slopes, 51 ARIZ. L. REV. 685, 685 (2009) (arguing that moderate paternalism is not sustainable and will inevitably expand).

255. Indeed, some suggest that paternalistic policies themselves tend to accrete, largely because of the irrational framing of public policy, through a series of seemingly moderate steps. Glen Whitman, The Rise of the New Paternalism, CATO UNBOUND (Apr. 5, 2010), http://www.cato-unbound.org/2010/04/05/glen-whitman/the-rise-of-the-new-paternalism/; but see Matthew Thomas & Luke Buckmaster, Paternalism in Social Policy—When Is It Justifiable?, PARLIAMENT OF AUSTRALIA, 1 (Dec. 15, 2010), http://www.aph.gov.au/library/pubs/rp/2010-11/11rp08.pdf (suggesting that paternalistic policies are "ubiquitous" in society, and "the main issue is not whether or not paternalism itself is justifiable, but rather the conditions under which particular policies may be said to be justifiable.").

virtually every market is imperfect to some degree.\textsuperscript{257} }

cautious principle may be "thousands of years old" and is "widely embraced throughout the world"). Some have termed the precautionary principle "senseless," in that it may become "paralyzing—forbidding inaction, stringent regulation, and everything in between." Cass R. Sunstein, \textit{Beyond the Precautionary Principle}, 151 U. PA. L. REV. 1003, 1003 (2003); see also Cass R. Sunstein, \textit{The Precautionary Principle as a Basis for Decision Making}, 2 THE ECONOMISTS' VOICE, no. 2, 2005 at 1, 1, available at http://www.bepress.com/cgi/viewcontent.cgi?context=http%3A%2F%2Fwww.bepress.com%2Fev&article=1079&date=&mt=MTMwODE1MDgwMQ%3D%3D&access_ok_form=Continue (pointing out that it is not always clear what to do if one wants to be safe rather than sorry because risks "can arise from action as well as from inaction;" there is no "principled way" to make policy decisions without balancing "relevant costs" of a policy). Still others suggest, in the context of privacy-protecting regulations, that "techno-panic" (fear of impending disaster from technology developments) should not determine policy. See Adam Thierer \& Berin Szoka, \textit{What Unites Advocates of Speech Controls \& Privacy Regulation?}, THE PROGRESS \& FREEDOM FOUND., 7-8 (Nov. 2009), http://www.pff.org/issues-pubs/pops/2009/pop16.19-unites-speech-and-privacy-reg-advocates.pdf (noting that a risk exists that once regulatory efforts begin "the 'crisis' cycle never ends"); see also Nat Ives \& Rich Thomaselli, \textit{Marketing Takes a Beating Inside the Beltway}, ADVER. EDUC. FOUND. (July 27, 2009), http://www.aef.com/industry/news/data/2009/9035 (suggesting that concerns about the state of the economy have made marketing "an unpopular and easy target ripe for regulation"); Jonathan H. Marks, \textit{9/11 + 3/11 + 7/7 = ? What Counts in Counterterrorism}, 37 COLUM. HUM. RTS. L. REV. 559, 559 (2006) (explaining that "emotional responses" can produce "systematic biases" that affect policy); Kenneth Brown, \textit{The Internet Privacy Debate}, INTL. J. OF COMM'N. L. \& POL'Y, 1, 9, (2000-2001), http://www.ijclp.net/files/ijclp_web_doc_11-6-2001.pdf (noting that "[a]ll new technology must go through its cycle of public debate over consumer safeguards," and suggesting that privacy debate should be deliberative, "not [fueled by] panic"). At a minimum, because regulation is not cost-free, and because freedom of commerce is a fundamental part of civil society, "[r]egulation of private transactions, even in the name of consumer protection," requires (if at all possible) some form of cost-benefit justification. Alvin C. Harrell, \textit{Basic Choices in the Law of Auto Finance: Contract Versus Regulation}, 7 CHAPMAN L. REV. 107, 109 (2004). "The hesitancy of the common law to broadly prohibit or prescribe in detail the terms of common transactions apparently stems partly from a recognition that regulation is inherently alien to freedom of contract and therefore carries a very high and commonly misunderstood social price." \textit{Id.} at 110. Even proponents of the precautionary principle recognize as much. See Kysar, \textit{supra} at 9 ("[N]o regulator would adhere to the [precautionary principle] without paying some attention to foregone benefits, new information, and changed circumstances."); John S. Applegate, \textit{The Taming of the Precautionary Principle}, 27 WM. \& MARY ENVTL. L. \& POLY REV. 13, 17 (2002) (noting that the precautionary principle is not absolute and that regulatory responses may be altered appropriately as more knowledge about a potential risk becomes available). Ultimately, the political question of whether to enact strengthened privacy laws may come down to how the issue is "framed" (privacy protection versus free content, for example). See Jonathan Remy Nash, \textit{Framing Effects and Regulatory Choice}, 82 NOTRE DAME L. REV. 313, 314 (2006) ("Framing effects may render [regulatory] instruments subject to criticism.").

\textsuperscript{257} Paul L. Joskow, \textit{Market Imperfections Versus Regulatory Imperfections}, ALFRED P. SLOAN FOUND. \& MIT, 6 (June 20, 2010), http://econ-
Second, assuming some demonstrated market failure and a recognized need for some form of intervention, the question becomes: What form of intervention is best?\textsuperscript{258} Interventions may take many forms:\textsuperscript{259} disclosure of information to the market, such as in compliance with the Sarbanes-Oxley Act; restriction of activities such as prohibitions on insider trading in securities; mandates such as requirements to offer health insurance to workers; or ownership restrictions such as the Glass-Steagall prohibition against commercial banks owning investment banks.\textsuperscript{260} As the FTC’s 2010 Report noted, the principal regulatory aims have been to ensure that consumers have “notice” of the privacy practices of online firms, and at least the possibility to “opt-out” out of interactions with the firm if those practices are unacceptable.\textsuperscript{261} Such limited information-distribution aims could, in theory, be addressed entirely by market self-regulation and self-certification of good practices or could be backed by government authority such as the FTC’s prosecution of claims for unfair or deceptive competition when firms fail to follow their own privacy policies.\textsuperscript{262}

\textsuperscript{258} See \textit{STEPHEN BREYER}, \textit{REGULATION AND ITS REFORM} 191 (1982) (using a “mis-match thesis,” to uncover areas for necessary regulatory reform and seeking “to match the tool to the problem at hand”).


\textsuperscript{260} \textit{Government Markets, supra, note 250, at 13-51.}

\textsuperscript{261} \textit{FTC 2010 REPORT, supra note 92, at 19-24; see generally discussion supra Parts III-V, VII (describing early and more recent FTC regulatory efforts aimed at OBA).}

\textsuperscript{262} See Kenneth A. Bamberger \& Deidre K. Mulligan, \textit{Privacy on the Books}
Such self-regulation, moreover, could be extended beyond the borders of the United States to respond to regulatory concerns in other countries.\textsuperscript{263} Governments may also co-regulate in this vein, by offering incentives, such as “safe harbor” protection, to firms that engage in accepted best practices.\textsuperscript{264} The advantages of these


\textsuperscript{264} See Ira S. Rubinstein, \textit{Privacy and Regulatory Innovation: Moving Beyond Voluntary Codes} (NELLCO Legal Scholarship Repository, Working Paper No. 3-1-2010), available at www.lsr.nellco.org/nyu (“[C]o-regulation, including privacy safe harbors, is an effective and flexible policy instrument that, if properly designed, offers several advantages as compared to the false dichotomy of voluntary industry guidelines versus prescriptive government regulation.”); Ira Rubinstein, \textit{Guest Blog on Privacy Safe Harbors}, FUTURE OF PRIVACY FORUM, www.futureofprivacy.org (last visited Oct. 2, 2011) (noting “some success” with COPPA safe harbor programs (the “best example” of a safe harbor program), limited by “very low rate of industry participation,” and “lack of regulatory flexibility” in approving self-regulatory programs pursuant
approaches generally center on flexibility as technology changes, and on the ability to draw on the expertise and insights of many participants in the market. Yet self-regulation, even with a government backstop, may provide inadequate incentives to ensure wide-scale industry participation, especially for new entrants and rogue operators.

The form of preferred intervention also has to do with the degree of specificity of the intervention. The government may pursue a “sectoral” approach, as the United States has largely done, or a more “comprehensive” system as in Europe and other areas. The sectoral approach essentially addresses “one problem at a time,” but risks being overtaken by new technology, new business practices, and new problems in the market. Here, for example, Con-


265. See INTERIM REPORT STUDY ON CO-REGULATORY MEASURES IN THE MEDIA SECTOR, HANS-BREDOW INST. (May 19, 2005), www.hans-bredow-institut.de (last visited Oct. 2, 2011) (traditional “command-and-control” regulation “ignores the interests of the objects (companies) it regulates” and is “doomed to failure in increasingly complex, rapidly changing societies;” because “knowledge [is] held by different actors, a model of “co-operation” is “essential”).


268. See id. (citing Fair Credit Reporting Act, Video Privacy Protection Act and Cable Television Consumer Protection and Competition Act as “sectoral” approaches); Chris Jay Hoofnagle, New Challenges to Data Protection Study - Country Report: United States, SSRN (Jan. 20, 2010), available at http://ssrn.com/abstract=1639161 (noting that “[t]he hallmark of the US federal approach to privacy is sectoral regulation,” and that the approach is “largely driven by outrage at particular narrow practices”). One recent example of a proposed “sectoral” solution appeared in Indiana, where a prosecutor refused to proceed against an alleged voyeur who took “upskirt” photographs at a mall,
gress or regulators might mandate, or encourage in other ways, the implementation of some specific set of privacy-enhancing technologies. Conversely, the comprehensive system generally outlines certain "fair information practices" ("FIPS"), which some commentators suggest are required to "patch up the holes" that the U.S. sectoral approach necessarily produces. Yet, even a FIPS system requires interpretation and oversight by some enforcement agency and may produce variations in application of the rules. Specific FIPS-implementing regulations or statutes, because the voyeurism statute arguably did not cover the offense. See Prosecutors Split on IN Voyeurism Law, WANE.COM (Mar. 3, 2010), http://www.wane.com/dpp/news/wane-indianapolis-Shoe-camera-man-charged-with-voyeurism. In apparent reaction, the Indiana legislature began consideration of a bill to create a new crime entitled "invasion of privacy by photography." See Indiana Lawmakers to Consider Upskirt Ban, IND. INTELLECTUAL PROP. & TECH. BLOG (Jan. 9, 2011), www.indianaintelectualproperty.wordpress.com.
moreover, risk becoming obsolete as business practices and technologies change.\textsuperscript{272}

Absent a definitive statement of FIPS, a statute regarding privacy protection could outline privacy protection in very general terms, such as a requirement that only "necessary" gathering of personal information take place in internet transactions.\textsuperscript{273} Such an approach might be combined with a requirement that the agency engage in a cost-benefit analysis in implementing the statute, to ensure that any regulations address the diverse range of values that may be reflected in agency implementation of the statute.\textsuperscript{274} Agency rulemaking, however, is slow.\textsuperscript{275} Such a broad delegation of authority to the agency,\textsuperscript{276} moreover, may be challenged on consti-

\textsuperscript{ments: Research Challenges and Future Directions, 19 INTERNET RESEARCH 194 (2009) (noting challenges to application of fair information principles in "ubiquitous" computing environment).}

\textsuperscript{272.} See Fernando R. Laguarda, Preserving Innovation in a Consumer-Focused Advertising Marketplace, ITIF (Sept. 27, 2010), http://www.itif.org/files/2010-preserving-innovation.pdf (noting the need to avoid "freeze[ing] in place" business models and that "[s]ensible rules will not inhibit innovation").

\textsuperscript{273.} See Jerry Kang, Information Privacy in Cyberspace Transactions, 50 STAN. L. REV. 1193, 1194 (1998) (suggesting "default" rule, to be modified only where parties "expressly agree otherwise").

\textsuperscript{274.} See Cass R. Sunstein, Congress, Constitutional Moments, and the Cost-Benefit State, 48 STAN. L. REV. 247, 248 (1996) (arguing that executive branch should oversee regulatory implementation with Congress providing "broad policy direction"); Brian Z. Tamanaha, Instrumentalism In Legislation and Administration, in LAW AS A MEANS TO AN END, 190, 190 (2006) (citing Louis L. Jaffe, Law Making by Private Groups, 51 HARVARD L. REV. 201, 252 (1937)) ("[O]ur entire economy is honeycombed with violent and bitter intra and inter group conflict," these interests "in one way or another, [will] be effective, be it in the legislative or in the administrative process.").

\textsuperscript{275.} Jonathan Sallet, "New Products at Every Stage"—The Application of Common-Law Reasoning in an Age of Innovation, REFORMING THE FCC, http://fcc-reform.org/ftccref/sallet-20090105.pdf (last visited June 17, 2011) ("Rules take time to create and often as much or more time to modify.").

\textsuperscript{276.} Broadly-stated statutory directions are a frequent element of regulatory regimes. See Cass R. Sunstein, Is Tobacco a Drug? Administrative Agencies as Common Law Courts, 47 DUKE L.J. 1013, 1014 (1998) (suggesting that, as a result of broadly worded statutes, "administrative agencies have become America's common law courts," such that “[t]he task of adapting the law to new circumstances, of both value and of fact, is largely an administrative responsibility."); see also Michael Herz, Purposivism and Institutional Competence in Statutory Interpretation, 2009 MICH. ST. L. REV. 89, 92 (suggesting that agencies are in best position, due to technical competence, to interpret statutes, and that democratic values are not undermined by the process of agency interpretation); Cass R. Sunstein, Beyond Marbury: The Executive's Power to Say What the Law is, 115 YALE L.J. 2580, 2582 (2006) (discussing Chevron, U.S.A., Inc. v. NRDC, 467 U.S. 837 (1984) and its implications for agency authority to interpret statutes). Nevertheless, the "New Deal" model, where "Congress' role was largely one of identifying a problem and asking the agency to deal with it," has been modified to some degree in the modern era, where statutes often contain "relatively clear guidelines for administrators to follow." Cass R. Sunstein, Changing Conceptions of Administration, 1987
Regulating Online Behavioral Advertising

277. See Jonathan Macey, Executive Branch Usurpation of Power: Corporations and Capital Markets 115 YALE L.J. 2416, 2419 (2006) ("The emergence of the executive branch as the fulcrum of power within the administrative state represents a deviation from the traditional balance of powers among the three branches of government. Only a concerted effort by the federal judiciary can rein in agencies that improperly usurp the authority of the legislative branch through the enforcement process."); David Schoenbrod, Delegation and Democracy: A Reply to My Critics, 20 CARDOZO L. REV. 731, 732 (1999) (suggesting that Congress evades responsibility by delegating to administrative agencies, and that "democracy suffers" as a result); but see Carl McGowan, Reflections on Rulemaking Review, 53 TUL. L. REV. 681, 687 (1979) (suggesting that the fundamental role of courts is to assure "procedural efficiency and fair play [by agencies], and conformity to statutorily mandated policies").


281. See Paul M. Schwartz, Internet Privacy and the State, 32 CONN. L. REV. 815, 816 (2000) ("[T]he State's important role in shaping both a privacy mar-
of the "right," moreover, affects certainty of application, and conversely, the adaptability of the standard.\textsuperscript{282} Thus, some observers propose incorporation of civil liability into a system of co-regulation, where a government "safe harbor" would protect companies that engage in approved self-regulatory behavior from both government enforcement proceedings and private actions for damages.\textsuperscript{283} Others suggest that private enforcement mechanisms are simply inadequate to the task of affecting "optimal" institutional change.\textsuperscript{284}

Finally, whatever the means of intervention in the American federalist system, an additional question arises as to whether the federal government should occupy all or simply some of the field of regulation.\textsuperscript{285} In the modern regulatory structure, co-extensive enforcement by both federal and state regulators is generally preferred as a means to enhance the resources for consumer protec-

ket and privacy norms," by identifying information privacy as "a constitutive value that helps both to form the society in which we live in and to shape our individual identities."); see also Paul M. Schwartz, Beyond Lessig's Code for Internet Privacy: Cyberspace Filters, Privacy-Control, and Fair Information Practices, 2000 WIS. L. REV. 743, 745 (2000) ("propertization" will "not necessarily promote privacy," due to the "problem of privacy market failure"). Others, however, suggest that a "dual regime" of government enforcement and private rights of action "is extremely unlikely to enhance social welfare or event consumer interests." Michael S. Greve, Consumer Law, Class Actions, and the Common Law, 7 CHAP. L. REV. 155, 156 (2004). Still others reject the notion that "government supposedly creates the market by defining and enforcing property and contract rights; [and] consequently, there is nothing particularly wrong with the government radically altering those rights . . . ." Timothy Sandefur, Does the State Create the Market—And Should it Pursue Efficiency?, 33 HARV. J.L. & PUB. POL'Y 779, 780-81 (2010) (arguing that markets "come first," but recognizing role of courts in enforcing rights).

\textsuperscript{282} See Vincy Fon & Francesco Parisi, On the Optimal Specificity of Legal Rules, 3 J. OF INSTITUTIONAL ECON. 147 (2007), available at http://journals.cambridge.org/action/displayFulltext?type=1&fid=1065020&jid=JOI&volumeId=3&issueId=02&aid=1065012 (contrasting "rules," such as speed limits, versus "standards," such as reasonableness, and suggesting that "optimal" degree of specificity must be determined by considering factors such as "legal obsolescence, volume of litigation, legal traditions and codification styles, judges' specialization, and complexity").

\textsuperscript{283} See Ira Rubinstein, On Privacy Safe Harbors, FUTURE OF PRIVACY FORUM (2010), http://www.futureofprivacy.org/ira-rubinstein-on-safe-harbors/ (suggesting "tiered" liability system, where firms that do not participate in safe harbor program could be subject to civil actions and liquidated damages and noting that "[s]afe harbors are a very powerful regulatory instrument.").

\textsuperscript{284} See Matthew C. Stephenson, Public Regulation of Private Enforcement: The Case for Expanding the Role of Administrative Agencies, 91 VA. L. REV. 93, 97 (2005) (suggesting that agencies should determine whether any private right of action applies because of "complex, contingent, and context-specific policy judgments" involved).

\textsuperscript{285} See generally JOSEPH FRANCIS ZIMMERMAN, CONGRESS: FACILITATOR OF STATE ACTION (State Univ. of NY Press, 2010) (providing overview of preemption issues in modern regulatory structure).
A further question, however, also presents itself: Should the states have the ability to engage in additional legislation to increase consumer protection in some regard? Arguably, lack of nationally uniform law may adversely affect business activity. Yet, states are widely regarded as "laboratories" for government innovation in regulatory methods. As a result, some theorists suggest a combined system where the federal government may nudge states toward experimentation without permitting wholly chaotic independent action.


290. See Jenna Bednar, Nudging Federalism Toward Productive Experi-
XII. Conclusion

As with many aspects of the regulation of technology, competent, logical discourse on privacy protection is often hard to find. The online advertising industry is substantial, and generally growing. The industry, moreover, is in the midst of a fundamental restructuring, in part as a result of the recession, but also due to changes in the essential economics of the market. The industry is also highly concentrated and could benefit from more entrants and more competition. Due to the value of information exchange


292. See John Deighton & John Quelch, Economic Value of the Advertising-Supported Internet Ecosystem, IAB. (June 10, 2009), http://www.iab.net/insights_research/industry_data_and_landscape/economicvalue (estimating value of internet advertising, not counting external social benefits, conservatively at up to $680 billion).

293. See Suzanne M. Kirchhoff, ADVERTISING INDUSTRY IN THE DIGITAL AGE, CONGRESSIONAL RESEARCH SERV. (Nov. 9, 2009), http://www.fas.org/sgp/crs/misc/R40908.pdf (suggesting that companies “must move beyond traditional advertising”); see also Edward Landry, Carol Ude & Christopher Vollmer, HD MARKETING 2010: SHARPENING THE CONVERSATION, BOOZE ALLEN HAMILTON (2009), http://www.boozallen.com/media/file/HD_Marketing_2010.pdf (noting “key trends” in online advertising, including: “marketing as conversation”); See generally DAVID MEERMAN SCOTT, REAL-TIME MARKETING AND PR: HOW TO INSTANTLY ENGAGE YOUR MARKET, CONNECT WITH CUSTOMERS, AND CREATE PRODUCTS THAT GROW YOUR BUSINESS NOW (2010) (highlighting new trends that include the ability to read buying signals as customers interact online); CHRISTOPHER VOLLMER, ALWAYS ON: ADVERTISING, MARKETING AND MEDIA IN AN ERA OF CONSUMER CONTROL 31-50 (2010) (marketing practices fragmenting to serve splintered audiences, requiring fine-grained insights and continuous innovation); Eric Clemons, Why Advertising is Failing on the Internet, TECHCRUNCH (Mar. 22, 2009), http://techcrunch.com/2009/03/22/why-advertising-is-failing-on-the-internet/ (arguing that internet marketing is "shattering" conventional advertising).

294. The online advertising industry is highly concentrated among a few
via the Internet, government actors should be cautious about placing restrictions on the OBA process.295

Ultimately, privacy regulation involves considering an array of options, which may range from market self-regulation to full-scale “command and control” by one or more agencies for one or more purposes. Creating an optimal privacy protection regime requires a clear understanding of the size and character of the problem to be addressed, the nature of the marketplace, including the inevitable imperfections that appear in the market, and the advantages and disadvantages of each form of regulation. Moreover, government regulators, both federal and state, must recognize the fast-paced changes in technology, business practices, and consumer preferences that inhere in our information-based economy, and they must plan for the probability that any regulatory approach adopted today may become obsolete and even harmful sometime in the future. Finally, government regulators must acknowledge that no single form of regulation is necessarily “best” in the view of all. Regulation involves subjective value choices and balancing of many interests. Input from all affected stakeholders, coupled with a willingness to experiment and abandon approaches that do not work under the circumstances, will ensure that the government may come closer to “getting it right.” The continuing struggle to develop effective and efficient means to regulate OBA suggests that the need for caution is well understood.296

295. See J. Howard Beales III & Timothy J. Murvis, Choice or Consequences: Protecting Privacy in Commercial Information, 75 U. CHI. L. REV. 109, 135 (2008) (noting arguments made by former FTC officials that use of broad “fair information practices” is not justified and that regulation should focus on “misuse” of “sensitive” information).

296. The length of the debate also shows how slowly social movements sometimes develop. See Laura Huey, A Social Movement for Privacy/Against Surveillance?, 42 CASE W. RES. J. INT’L L. 699, 699 (2010) (“[A]s a whole the issue of surveillance has yet to spawn a larger social movement.”); Benjamin R.