

## Privacy & Security ADVISORY

December 6, 2010

### FTC Issues Privacy Report; House Energy & Commerce Committee Holds Privacy Hearing on FTC's Do-Not-Track Proposal

On Thursday, December 2, 2010, the House Energy & Commerce Committee held its last privacy hearing of the year to examine the feasibility of "Do-Not-Track" legislation authorizing the Federal Trade Commission ("FTC") to establish a mechanism (similar to the popular Do-Not-Call registry) for Internet users to globally opt-out of receiving targeted online advertising based on their Internet behavior (i.e., known in the industry as "online behavioral advertising"). The House hearing was held less than 24 hours after the FTC released a long-awaited report and proposed guidelines for businesses on consumer data practices, including the Do-Not-Track proposal, entitled *Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers* (the "Privacy Report").<sup>1</sup> This advisory provides a brief summary of both the Privacy Report and the House hearing on the Do-Not-Track proposal.

#### FTC Privacy Report

The Privacy Report, released by the FTC following a year-long series of public roundtables on businesses' privacy practices that began in December 2009, proposes a new framework for businesses and policymakers that the FTC believes will better protect consumer privacy in the rapidly developing information marketplace. The report's stated purpose is to "inform policymakers, including Congress, as they develop solutions, policies and potential laws governing privacy, and guide and motivate industry as it develops more robust and effective best practices and self-regulatory guidelines." In this sense, as a policy proposal, the report is similar in form (but not scope or substance) to the FTC's report on online behavioral advertising released in February 2009.<sup>2</sup> However, the statements of key policymakers made in the wake of the report's release indicate that it may soon serve as the blueprint for federal legislation to be introduced in the new Congress beginning in January 2011.

#### A. Reaction of Key Federal Legislators to Release of Privacy Report

The guidelines proposed by the FTC in the Privacy Report are based on the Commission's finding that industry efforts to address consumer privacy concerns through self-regulation "have been too slow, and up to now have failed to provide adequate and meaningful protection." In his remarks on the Privacy Report, FTC Chairman Jon Leibowitz observed, "A legislative solution will surely be needed if industry does not step up to the plate."<sup>3</sup> Senate Commerce Committee Chairman Jay Rockefeller (D-WV) reacted to the report's release with a similar sentiment, stating that "Americans need greater control over how their information is collected

<sup>1</sup> The Privacy Report is available online at <http://www.ftc.gov/os/2010/12/101201privacyreport.pdf>.

<sup>2</sup> *FTC Staff Report: Self-Regulatory Principles for Online Behavioral Advertising: Tracking, Targeting, and Technology*, February 12, 2009, available at: <http://www.ftc.gov/os/2009/02/P085400behavadreport.pdf>.

<sup>3</sup> The complete remarks of the Chairman are available at: <http://www.ftc.gov/speeches/leibowitz/101201privacyreportremarks.pdf>.

This advisory is published by Alston & Bird LLP to provide a summary of significant developments to our clients and friends. It is intended to be informational and does not constitute legal advice regarding any specific situation. This material may also be considered attorney advertising under court rules of certain jurisdictions.

and used, and the FTC needs the authority to take action against companies who fail to provide consumers with basic privacy protections.”<sup>4</sup>

In perhaps the most significant statement made by any federal legislator following the Privacy Report’s release, Senator John Kerry (D-MA), Chairman of the Senate Commerce Committee’s Subcommittee on Communications, Technology and the Internet, confirmed that he has been drafting comprehensive privacy legislation that many anticipate to be introduced early next year, and that it would likely embody some of the FTC’s policy recommendations. In his release, Senator Kerry stated, “The Federal Trade Commission’s report should be a wakeup call for every Internet user in this country. The report confirms that many companies – both online and offline – don’t do enough to protect consumer privacy....The report presents a thoughtful prescription for common practices that all firms should adopt and provides an important confirmation of the conclusions I’ve reached over the past few months while drafting privacy legislation.”<sup>5</sup>

## B. Summary of Privacy Report’s Proposed Framework

In its statement released at the time of the Privacy Report’s publication, the FTC confirmed its commitment to ensuring that the burden for protecting consumer information is placed on businesses rather than on the consumers themselves. In particular, the FTC noted that businesses’ privacy policies “have become too long, legalistic disclosures that consumers usually don’t read and don’t understand if they do,” and that privacy policies therefore “force consumers to bear too much burden in protecting their privacy.”<sup>6</sup> The proposed framework, according to the Privacy Report, is designed to serve as a “forward-looking policy vehicle for approaching privacy in light of new practices and business models” and “to establish certain common assumptions and bedrock protections on which both consumers and businesses can rely as they engage in commerce.”<sup>7</sup>

### 1. Scope of Framework

The Privacy Report proposes a framework that would apply broadly to all commercial entities – both online and offline – that “collect, maintain, share, or otherwise use consumer data that can be reasonably linked to a specific consumer, computer, or other device.”<sup>8</sup>

The scope of the FTC’s framework is worded very broadly and is formulated to capture nearly all commercial businesses that collect, process or use data about consumers (or their computers or devices) in the course of their business operations. It is significant in at least two key respects that reflect the culmination of emerging trends in FTC policy formulation and enforcement practices that we explored in greater depth in our September 2010 Privacy and Security Advisory.<sup>9</sup>

---

<sup>4</sup> Senator Rockefeller’s full statement is available at: <http://commerce.senate.gov/public/index.cfm?p=PressRoom>.

<sup>5</sup> Senator Kerry’s full statement is available at: <http://kerry.senate.gov/press/release/?id=223b8aac-0364-4824-abad-274600dffe1c>.

<sup>6</sup> The complete FTC statement is available at: <http://www.ftc.gov/opa/2010/12/privacyreport.shtm>.

<sup>7</sup> Privacy Report, pp. 39-40.

<sup>8</sup> Privacy Report, p. 42.

<sup>9</sup> Privacy and Security Advisory: *The Impact of Emerging Consumer Privacy Standards on the Collection and Use of Customer Data*, September 21, 2010, available at: <http://www.alston.com/files/Publication/88ed912a-1e66-4c3b-a2bf-f29273d57d61/Presentation/PublicationAttachment/211582be-05bc-4d70-bd8d-5462e26401b3/10-507%20Special%20Privacy%20Law%20Update%20-%20Customer%20Data.pdf>.

First, it is notable that the FTC proposes the scope of this framework to extend to consumer data collected both online and offline, especially after the Commission spent more than a decade focusing almost exclusively on online businesses' privacy practices. This trend toward examining offline privacy practices with the same scrutiny as online practices has been building over the past several years, particularly in light of the FTC's enforcement of data security standards where offline data breaches have been the subject of FTC enforcement actions. A second way in which the scope has been expanded beyond recent domestic privacy laws is by applying the framework to data that can be linked to a particular "computer or other device." Most privacy laws and regulations have, to date, been narrowly focused on personally identifiable information, or data that can be used to identify a particular consumer. With this framework, the FTC is proposing that privacy interests exist and must be protected even with respect to identifiable devices, not individuals, despite the fact that computers or devices may be used by multiple users.

Together, these elements combine to establish a marked expansion of the scope of the privacy concerns the FTC is pursuing, and also reflect the FTC's desire to expand its role as a policymaking body beyond its core responsibility as an enforcement agency. More specifically, the Commission is making clear that it does not see itself as merely serving as the principle enforcement authority over the FTC Act and other consumer protection laws, but that it should serve as the primary policymaking body in the federal government regarding the business collection, disclosure and use of a broader class of "consumer data" collected via any means.<sup>10</sup>

## **2. Three Major Elements of Framework**

The Privacy Report makes the following three conceptual recommendations for ensuring that covered commercial entities better protect consumer privacy:

### **a. "Privacy By Design"**

The Privacy Report recommends that businesses integrate privacy protections into their products, services and operations at "every stage of their development." For example, the FTC recommends that businesses do this by adopting the following guidelines:

- instituting measures to secure consumer data;
- only collecting and retaining consumer data if there is a legitimate business need;
- establishing procedures to promote the accuracy of consumer data;
- assigning personnel to oversee data management procedures;
  
- training employees about data privacy protections; and
- conducting privacy reviews for new products and services.

### **b. Simplified Consumer Choice**

---

<sup>10</sup> The FTC has acknowledged in the past that its enforcement authority in the privacy area is limited to areas such as deceptive statements under the FTC Act and under other specialized statutes such as the Children's Online Privacy Protection Act. See, e.g., *Privacy Online: Fair Information Practices in the Electronic Marketplace*, FTC Report to Congress, at 33-34, available at: <http://www.ftc.gov/reports/privacy2000/privacy2000.pdf>.

The second bedrock principle recommended by the Privacy Report is that companies should “simplify consumer choice.” It proposes a bifurcated framework depending on whether a business practice is “commonly accepted” or not.

For commonly accepted practices, the FTC acknowledges that businesses need not provide choice before collecting and using consumers’ data where a consumer’s consent to do so can clearly be inferred from the context of the transaction. The FTC cites as one example the provision of a consumer’s address solely to deliver a product the consumer ordered online. For business practices that are not commonly accepted, the FTC believes that consumers should be able to make “informed and meaningful choices” at the time “when – and in the context in which – the consumer is making a decision about his or her data.” As highlighted in its statement released with the Privacy Report, the FTC explains that the basis for this recommendation is to counter existing business practices that leave consumers insufficiently informed at the time they must make a choice, particularly when consumer choice options are presented to consumers “after having to read long, complicated disclosures that they often cannot find.”

The most significant “simplified” method of choice proposed in the Privacy Report is the FTC’s recommendation that consumers be provided a “Do-Not-Track” option that, once selected, would prohibit businesses from collecting information about a consumer’s online searching and browsing activity for the purposes of delivering targeted advertisements to them and for other purposes. The Privacy Report’s suggested mechanism for allowing consumers to utilize the Do-Not-Track option is the placement of a persistent setting, similar to a cookie, on the consumer’s Internet browser that would signal the consumer’s choices about being tracked and receiving targeted advertisements.

This proposed Do-Not-Track list has been under consideration by the FTC since it was first mentioned at the Commission’s policy forum on online behavioral advertising in late 2007, but the Privacy Report marks the first time that the FTC has formally proposed a Do-Not-Track mechanism in a report. As noted in the summary of the House privacy hearing below, this proposal is controversial and opposed by industry.

### **c. Transparency**

The Privacy Report recommends a third set of measures to improve the transparency of business practices regarding the collection, storage and use of consumer information, including:

- clearer, shorter and standardized privacy notices in a form that allows consumers to compare the information practices of competing businesses;
- consumer access rights to the data that businesses maintain about them, particularly for non-consumer facing entities such as data brokers (a concept that could introduce significant new costs for businesses where applied);
- prominent disclosures and obtaining consumers’ opt-in consents before using consumer data in a manner that is materially different than claimed at the time of its collection; and
- participation in consumer educational efforts to explain business data privacy practices.

## House Hearing on the Feasibility of Do-Not-Track Legislation

The Commerce, Trade and Consumer Protection Subcommittee of the House Energy and Commerce Committee held a hearing on Thursday morning, December 2, on the feasibility of the FTC's Do-Not-Track proposal. The hearing revealed a clear divide between the federal government and consumer interest groups on the one hand, and businesses on the other, as to the best means for protecting consumer privacy. Former Energy & Commerce Committee Chairman John Dingell (D-MI) echoed his support for the FTC's conclusions by suggesting that industry's efforts to protect consumer privacy through self-regulatory efforts have been insufficient. Other members said that more can and should be done by businesses to protect consumer privacy interests. Subcommittee Ranking Member Ed Whitfield (R-KY), however, raised the potentially negative economic effects that a government-mandated and operated Do-Not-Track mechanism may have on Internet content, e-commerce and the recovering economy. He recommended that, before the FTC's recommendation is pursued in legislation, economic impact studies should be conducted to assess how such a proposal may affect online businesses and the information economy.

Testifying on behalf of the Obama Administration and the FTC were, respectively, Daniel J. Weitzner, Associate Administrator for the Office of Policy Analysis and Development at the National Telecommunications and Information Administration, and David Vladek, Director of the Bureau of Consumer Protection at the Commission. Mr. Weitzner and Mr. Vladek agreed that current industry efforts to address consumer privacy concerns have been insufficient, and that consumer choice and increased control over their personal information are critical to sound Internet policy. They also observed that a Do-Not-Track mechanism could be created in a way that does not diminish Internet content. The two government witnesses differed in some respects under questioning from the Subcommittee's members. While Mr. Vladek focused his remarks on explaining the FTC's findings on privacy practices and certain elements of the Privacy Report, including the Do-Not-Track proposal and the Commission's ability to enforce it, Mr. Weitzner expressed broader concerns about the need for the U.S. to renew its leadership role in the global privacy debate by developing a privacy framework that is focused on enhancing trust and encouraging innovation.

The second panel of witnesses consisted of representatives from industry, consumer groups and academia. Of note, Susan Grant, Director of Consumer Protection at the Consumer Federation of America, which is an association of nearly 300 consumer organizations, expressed concern about the increasing rate at which businesses are "spying" on consumers online. Ms. Grant said that while Do-Not-Track legislation would not entirely eliminate her interest group's concerns, it would ameliorate them, and she looked forward to working with Congress on the legislation. Her enthusiastic support for the FTC's proposal was challenged by the industry witnesses. Joan Gillman, Executive Vice President and President of Media Sales at Time Warner Cable, suggested that, before rushing to implement a Do-Not-Track mechanism that may negatively affect consumers' online experience and harm the online economy, the policy debate should focus on industry-led efforts to implement self-regulation and best practice guidelines that are more capable of quickly evolving to adapt to the fast-changing online environment.

A webcast of the hearing, a witness list and complete copies of all witness testimony for this hearing are available on the House Committee's webpage at the following location: [Hearing on Do-Not-Track Legislation: Is Now The Right Time?](#)

## Conclusion

The value of consumer data as a corporate asset, and the ability of businesses to leverage their data stores, will be significantly impacted should the FTC's privacy framework be adopted in something close to its current form. The framework set out in the Privacy Report would introduce significant challenges for many services, product lines and, in some cases, entire businesses that have been built on existing concepts of consumer privacy and legally permissible ways to use consumer data in the U.S.

The FTC announced that it will be accepting public comments on the Privacy Report through January 31, 2011, and for the reasons highlighted above, it is anticipated that many businesses and industry trade associations will file comments with the Commission addressing the proposed framework and the controversial elements of its new privacy guidelines for commercial entities collecting and using customer data.

Businesses should monitor the FTC and Congress closely in the coming months, particularly after the new Congress is seated in January, to determine how the FTC's recommendations in the Privacy Report might be implemented into law. Additionally, businesses with significant customer data assets should consider engaging in the FTC public comment process on the Privacy Report as well as in the Congressional debate, in both cases to help shape any statute or future regulation on consumer privacy that may be based on the proposed framework in the report. As noted above, businesses may wish to participate to ensure that implementation of the Privacy Report's recommendations do not lead to increases in their regulatory compliance costs, the disruption of their legitimate business practices and the contraction of the information marketplace.

Alston & Bird's [Privacy and Security Practice](#) has been recognized as one of the leading practices in the nation by [Chambers USA: America's Leading Lawyers for Business](#) every year since Chambers & Partners began listing law firms in this area.

If you would like to receive future *Privacy & Security Advisories* electronically, please forward your contact information including e-mail address to [Privacy.Post@alston.com](mailto:Privacy.Post@alston.com). Be sure to put "**subscribe**" in the subject line.

If you have any questions or would like additional information please contact your Alston & Bird attorney or any of our [Privacy & Security](#) attorneys.

---

## This *Privacy & Security Advisory* was prepared by:

Edward Britan  
[edward.britan@alston.com](mailto:edward.britan@alston.com)  
202.239.3364

David C. Keating  
[david.keating@alston.com](mailto:david.keating@alston.com)  
404.881.7355

Paul G. Martino  
[paul.martino@alston.com](mailto:paul.martino@alston.com)  
202.239.3439

---

## Privacy & Security Attorneys and Policy Advisors

Andria E. Beeler-Norrholm  
[andria.beeler-norrholm@alston.com](mailto:andria.beeler-norrholm@alston.com)  
404.881.4933

John R. Hickman  
[john.hickman@alston.com](mailto:john.hickman@alston.com)  
404.881.7885

Naotaka Matsukata  
[nao.matsukata@alston.com](mailto:nao.matsukata@alston.com)  
202.239.5591

Edward Britan  
[edward.britan@alston.com](mailto:edward.britan@alston.com)  
202.239.3364

David C. Keating  
[david.keating@alston.com](mailto:david.keating@alston.com)  
404.881.7355

Todd McClelland  
[todd.mcclelland@alston.com](mailto:todd.mcclelland@alston.com)  
404.881.4789

Angela T. Burnette  
[angie.burnette@alston.com](mailto:angie.burnette@alston.com)  
404.881.7665

Scott Kitchens  
[scott.kitchens@alston.com](mailto:scott.kitchens@alston.com)  
404.881.4955

Gerald L. Mize, Jr.  
[gerald.mize@alston.com](mailto:gerald.mize@alston.com)  
404.881.7579

Jennifer L. Butler  
[jennifer.butler@alston.com](mailto:jennifer.butler@alston.com)  
202.239.3326

Kelly Culpepper Larkin  
[kelly.larkin@alston.com](mailto:kelly.larkin@alston.com)  
404.881.7916

Eric A. Shimp  
[eric.shimp@alston.com](mailto:eric.shimp@alston.com)  
202.239.3409

Clare H. Draper, IV  
[clare.draper@alston.com](mailto:clare.draper@alston.com)  
404.881.7191

Pamela Keeney Lina  
[pamela.lina@alston.com](mailto:pamela.lina@alston.com)  
404.881.4935

Dwight C. Smith, III  
[dwight.smith@alston.com](mailto:dwight.smith@alston.com)  
202.239.3325

Jonathan Gordon  
[jonathan.gordon@alston.com](mailto:jonathan.gordon@alston.com)  
213.576.1165

Robert C. Lower  
[bob.lower@alston.com](mailto:bob.lower@alston.com)  
404.881.7455

Paula M. Stannard  
[paula.stannard@alston.com](mailto:paula.stannard@alston.com)  
202.239.3626

William J. Helmstetter, III  
[bill.helmstetter@alston.com](mailto:bill.helmstetter@alston.com)  
404.881.7942

Paul G. Martino  
[paul.martino@alston.com](mailto:paul.martino@alston.com)  
202.239.3439

Katherine M. Wallace  
[katherine.wallace@alston.com](mailto:katherine.wallace@alston.com)  
404.881.4706

### ATLANTA

One Atlantic Center  
1201 West Peachtree Street  
Atlanta, GA 30309-3424  
404.881.7000

### CHARLOTTE

Bank of America Plaza  
Suite 4000  
101 South Tryon Street  
Charlotte, NC 28280-4000  
704.444.1000

### DALLAS

Chase Tower  
Suite 3601  
2200 Ross Avenue  
Dallas TX 75201  
214.922.3400

### LOS ANGELES

333 South Hope Street  
16th Floor  
Los Angeles, CA 90071-3004  
213.576.1000

### NEW YORK

90 Park Avenue  
New York, NY 10016-1387  
212.210.9400

### RESEARCH TRIANGLE

Suite 600  
3201 Beechleaf Court  
Raleigh, NC 27604-1062  
919.862.2200

### SILICON VALLEY

Two Palo Alto Square  
Suite 400  
3000 El Camino Real  
Palo Alto, CA 94306-2112  
650.838.2000

### VENTURA COUNTY

Suite 215  
2801 Townsgate Road  
Westlake Village, CA 91361  
805.497.9474

### WASHINGTON, D.C.

The Atlantic Building  
950 F Street, NW  
Washington, DC 20004-1404  
202.239.3300

[www.alston.com](http://www.alston.com)

© Alston & Bird LLP 2010