
TO	IAB	DATE	December 7, 2010
FROM	Venable LLP	EMAIL	singis@venable.com
		PHONE	202.344.4613
RE	Summary of December 2010 FTC Preliminary Staff Report on Privacy		

The Staff (“Staff”) of the Federal Trade Commission (“FTC” or “Commission”) issued its much anticipated privacy report on December 1, 2010. The report, titled, “Protecting Consumer Privacy in an Era of Rapid Change”, sets forth the Staff’s proposed framework for how companies could address consumer privacy.¹ In the report, Staff expresses support for a universal choice mechanism with respect to online behavioral advertising, sometimes referred to as “Do Not Track”. The report suggests that this mechanism could be achieved either legislatively or through industry self-regulation. Comments on the report are due January 31, 2011. The Commission intends to issue a final report in 2011.

The report identifies the FTC’s growing concern with the rapid pace of technological change and new business models that depend upon capturing consumer data. The report does not specifically recommend legislation, but rather suggests a framework for privacy practices for businesses and policymakers.

I. SCOPE (pp. 42-43)

The Staff’s proposed framework would apply broadly to “all commercial entities” that collect or use consumer data that can be reasonably linked to a specific consumer, computer or other device. The proposed framework is intended to apply to both entities that collect data directly from consumers, as well as entities that do not have direct consumer-facing relationships. In addition, the Staff proposes applying the framework to any data that can be “reasonably” linked to a specific consumer, or a specific computer or other device, regardless of the content of the data, and thus would apply beyond personally identifiable information (“PII”) to include information such as an IP address.

II. CONSUMER CHOICE (p. 52)

The Staff proposes a new regime regarding consumer choice. Traditionally, the debate around choice has focused on whether the default choice is “opt-in” or “opt-out” for consumers. The regime proposed in the report focuses instead on the timing and placement of the choice. The framework would not require choice for uses of the data that are “commonly accepted practices” described below. All other practices would require consumer choice. The Staff still indicates that companies should provide notice of these practices in their privacy policies in order to promote transparency and accountability. For situations where a company provides

¹ FTC Report, available at <http://ftc.gov/os/2010/12/101201privacyreport.pdf>.

information to a service provider where the service provider is acting at the direction of a company for the enumerated purpose and there is no further use of the data, such a practice would not require choice.

A. Commonly Accepted Practices (pp. 53-54)

The Staff proposes a narrow set of practices to be included in this category where the provision of choice would not be required. These include:

- **Product and Service Fulfillment.** This includes collection and use of information for payment and shipping.
- **Internal Operation.** This includes information collected in customer satisfaction surveys. This would also include collection of information by websites about visits and click through rates to improve site navigation.
- **Fraud Prevention.**
- **Legal Compliance and Public Purpose.** This includes the providing of information with law enforcement in response to subpoenas. This would also include a business reports to a consumer's delinquent account to a credit bureau.
- **First Party Marketing.** This category includes the recommending by a company or website of products and services based upon their prior purchases.
- **Online Contextual Advertising.** The delivery of advertisements based upon a consumer's current visit to a web page or a single search query.

B. Affiliates (p. 55)

The report defines the commonly accepted practice of first party marketing to only include the collection of data from a consumer with whom the company interacts directly. Collection of data by business affiliates would not be considered first party marketing unless the affiliate relationship was made clear to consumers through common branding or a similar practice.

C. Providing Choice (pp. 57-58)

The Staff indicates that companies would be required to give consumers the ability to make "informed and meaningful" choices for all other commercial data collection and uses beyond commonly accepted practices. For such practices, the report indicates the choice mechanism should be offered at the point when the consumer is providing data.

The report identifies information collected at retail that is sold to a third party for marketing purposes as a practice that is not commonly accepted.

Similarly, Staff has indicated that **deep packet inspection** (pp. 55-56, 61) is not a commonly accepted practice. The primary rationale provided is that it is “unlikely that consumers would anticipate ISP monitoring of all of their online activity in order to created detailed profiles of them for marketing purposes” (p. 56).

The Staff indicates that deep packet inspection likely requires a heightened level of consent. It provides two reasons for this assertion: (1) the scope of the information collected about consumers—“the extensive mining of consumer information”; and (2) the limited number of broadband ISP providers and the inability of consumers to discontinue broadband service.

The Staff provides several examples of how choice should be provided.

- **Online Retailer.** Clear and conspicuous choice should be provided on the page where consumer types in information.
- **Social Media.**
 - If consumer information will be conveyed to 3rd party application provider then notice and choice should be provided at the time the consumer is deciding to use the application and at a minimum before consumer information is obtained.
 - If sharing occurs automatically through a default, then disclosure should be clear and conspicuous at the time the consumer becomes a member of the service, and not through the privacy policy of the service.
- **Mobile.** All companies that are involved in the collection and sharing of information on mobile devices—including the carrier, operating system vendors, applications, and advertisers—should provide meaningful choice mechanisms.

D. Sensitive data (pp. 56, 61)

Staff questions in the first party marketing context, which is a commonly accepted practice, whether consumers should be given a choice before sensitive data is used. Staff indicates that affirmative express consent should be required for the collection of sensitive information for online behavioral advertising and for information about children, financial and medical information, and precise geolocation data.

Staff also highlights the issue of teens and whether there are enhanced consent procedures that are important for teens. Staff indicates that teens may “not always think clearly

about the consequences of their actions” and asks whether additional protections should be explored for social media services.

For all of the above enumerated contexts, the Staff indicates that consumer choice should be “durable” and not subject to repeated additional requests from the particular merchant when the consumer elects not to have information collected, used, or stored.

E. Do Not Track List (pp. 63-69)

The Staff is calling for what it is calling a “do-not-track” list in the context of online behavioral advertising. While some papers and statements of the Staff were critical that self-regulation has not kept up with technology, the proposal for do-not-track is a misnomer and appears to mirror the consumer choice mechanism being deployed by the cross industry self-regulatory mechanism. The Chairman of the FTC, Jon Leibowitz in a press conference calling for the do-not-track list indicated that if the self-regulatory program delivers with its program that it is what the FTC is calling for.

Specifically, the report calls for a uniform and comprehensive consumer choice mechanism through the use of a “setting similar to a persistent cookie on a consumer’s browser and conveying that setting to sites that the browser visits, to signal whether or not the consumer wants to be tracked or receive targeted advertisements.” The Staff indicated that such a mechanism should be different than the “do not call” program and should not require a “registry” of unique identifiers and rather should use browser based persistent cookies. The Staff asked for comment on whether a universal choice mechanisms should include an option that enables consumers to control the types of data that they are willing to have collected about them. This presumably includes a listing of the categories of interest or market segments about a particular consumer browser.

III. INCREASED TRANSPARENCY (pp. 69-77)

The Staff proposes increasing consumer transparency, and calls for a number of measures that it believes will increase transparency of data collection and use practices to consumers. These include providing consumer choice mechanisms as discussed above, improving consumers’ ability to compare data practices across company, and providing consumers with access to their data.

A. Streamlined and Standardized Privacy Notices (pp. 70-72)

The report sets forth the view of the Staff that current privacy notices are opaque, lack uniformity, are cumbersome to navigate, and “bury” important disclosures. To alleviate this problem, the Staff proposes that privacy notices provide clear, comparable, and concise descriptions of a company’s overall data practices. It advocates for companies to standardize the format of their privacy notices and the terminology used, and to undertake consumer testing to

ensure that privacy notices are being comprehended by consumers. The Staff also highlights the need for companies that provide services on small screen handheld devices to determine how best to ensure that consumers get pertinent information about data practices on mobile devices.

B. Reasonable Access (pp. 72-76)

The Staff focuses on what it terms “consumer profiles” by collecting consumer data, combining it with other consumer information, and selling it to third parties. It supports a “sliding scale approach” to providing consumers with access to such data, based on the cost and benefit of access in various situations. As described further below in the discussion of information brokers, the report indicates that using data for authentication or decision-making purposes dictates that consumers have access to the actual data along with the ability to correct or delete any erroneous data. Data not used for decision-making purposes, such as marketing data, would only require disclosure of the general categories of data, and the provision of the ability for consumers to have their name removed from marketing lists.

C. Prominent Disclosure of and Affirmative Express Consent to Material Change (pp. 76-77)

The Staff asserts that it is well-settled FTC case law and policy that companies must provide prominent disclosures and obtain opt-in consent before using consumer data in a materially different manner than claimed when the data was collected, posted, or otherwise obtained. The report reiterates the importance of disclosure of material change and affirmative consumer consent, and proposes that this standard be applied in both the online and offline contexts. The report uses as an example a retailer who decides to begin sharing consumer data with third parties, stating that such retailer must prominently disclose the change in policy and obtain affirmative express consent for the use of any previously collected data.

V. PRIVACY BY DESIGN AND DATA SECURITY (pp. 44-52)

The report promotes “privacy by design” and encourages companies to incorporate privacy and data security protection into their business practices, product design and development. The report cites four types of substantive protection the Staff believes to be of critical importance to consumer privacy:

- **Physical, technical and administrative safeguards to protect consumer information.** The level of security required should depend on the sensitivity of the data, the size and nature of a company’s business, and the types of risk the company faces.
- **Data collection should be limited to what is necessary for legitimate business needs.** For example, the report states that if an advertising network is tracking consumers’ online activities to serve targeted ads, it should not also use key loggers to capture all of the data that a consumer inputs.

- **Limited data retention periods.** Data should be promptly and securely disposed of, once the specific business need for which it was collected has been satisfied. The FTC is especially concerned about the retention of location information, which may, aggregated over time, reveal patterns that expose sensitive or confidential information.
- **Ensure accuracy of data collected.** The report indicates that accuracy is especially important for data that could be used to deny benefits to consumers.

The report also indicates that companies should develop and implement comprehensive privacy programs that designate specific personnel with responsibility for privacy and directs companies to assess the privacy impact of their products and practices.

VI. EDUCATION (pp. 78-79)

The report discusses the need for greater consumer education to increase consumer awareness and understanding of overall data collection and use practices. The Staff calls upon stakeholders to educate consumers on various data practices and their privacy implications to alleviate, what it perceived from the roundtables as consumers' lack of understanding of these issues.

* * *