February 18, 2011

To: Federal Trade Commission
Subject Category: A Preliminary FTC Staff Report on "Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers"

#361; File No. P095416

PrivacyActivism supports the Federal Trade Commission's efforts in giving consumers the choice about whether or not they wish to be tracked online. Most Net users are unaware of online tracking and data collection, so we support the need for a Do Not Track option.

An important first step is the acceptance of the need for transparency by data collectors and brokers about their data collection practices.

Companies should increase the transparency of their data practices

Improved privacy notices

• What is the feasibility of standardizing the format and terminology for describing data practices across industries, particularly given ongoing changes in technology?

There are numerous strategies that have been employed to help consumers understand the privacy choices available to them. The Cloze Test[1] and the Flesch-Kincaid Reading Ease readability tests have been used to gauge readability for financial and medical privacy notices. The model notices provided by the FTC to banking institutions complying with the GLB Act show how research can improve notices given to consumers. We believe strategies that improve the readability of complex material should be utilized for explaining privacy to consumers, especially for technically complex privacy issues.

We believe standard terminology and simplified formats are beneficial to consumers trying to understand how their privacy choices. However, it is likely not feasible to replicate model privacy notices for all online situations. Rather, the FTC should focus on providing businesses with guidance about how to create an understandable notice. The focus should be on:

1. Data collectors should ensure the most important data is available at the top of the policy. Policies affecting how a consumer's information may be shared with affiliates, other companies or the government should always be listed very close to the beginning of the policy.
2. Data collectors should provide consumers with information about how they can review, edit or delete information that has been collected on them.
3. Data collectors should provide consumers with a simple way to be notified if

[1] *Privacy Policies: Cloze Test Reveals Readability Concerns* Ronnie Fanguy, Betty Kleen and Lori Soule. Issues in Information Systems. Volume V, No 1, 2004. *www.iacis.org/iis/2004_iis/PDFfiles/FanguyKleenSoule.pdf*

privacy policies change and should be encouraged to notify consumers before changes take effect. For example, the Electronic Frontier Foundation's project, TOSBack, a website that tracks changes in the terms of service for numerous consumer-facing websites such as Google, Netflix, Facebook and PayPal. Consumers can stay up-to-date on changes to the terms of service of these companies by subscribing to an RSS feed or visiting the TOSBack website. EFF keeps minimal information about visits to their site, however, a recent day saw approximately 5,500 hits to the TOSBack site, not including images. It's a popular site and a direct reflection of strong consumer interest in staying aware of changes made to privacy policies.

4. Privacy policies should use short sentences and simple words.
5. Companies should be strongly encouraged to list the FTC Complaint Assistant in their privacy policies. Too often, consumers who are frustrated by the data practices of a website do not know where to submit complaints[2]. Instead of submitting complaints to the Federal Trade Commission, consumers often attempt to complain to the company that violated their privacy expectations in the first place. As a result, the FTC does not receive adequate data about the privacy concerns of consumers. The privacy policy is one place to address this issue.

Recommendation: PrivacyActivism recommends that the FTC create interactive online technology that will allow websites to generate customized privacy policies on the FTC website by answering questions about their data collection and retention practices. The OECD Privacy Statement Generator[3] provides an example for how such an interactive privacy policy generator could work, ensuring that key data elements are included and organized simply. While we do not consider the OECD Privacy Statement Generator to be a model for *content*, we do believe the business-side functionality can be a good starting point. If the FTC were to develop such a system, it should include ample room for customized text and avoid over-simplification. Charts, such as those used in the OECD version, will most likely be too simple. This will nonetheless be an opportunity to help ensure appropriate information is included, the most important information is close to the top and a link to the FTC's Complaint Assistant is added.

• How can companies present these notices effectively in the offline world or on mobile and similar devices?

For mobile devices, a consumer should be given a list of the data elements a site or application will be collecting at the moment of collection. The data elements should be subdivided into those elements which are required for the transaction to occur and those which are supplemental to the transaction. Applications and websites should be encouraged to provide the consumers with granular control over what data elements a website accesses beyond those necessary to fulfill a transaction. For example, a mobile

[2] *Know Privacy*, Joshua Gomez, Travis Pinnick and Askan Soltani. 10-10-2009. UC Berkeley Scool of Information Report 2009-037 http://escholarship.org/uc/item/9ss1m46b#page-1

[3] OECD Privacy Statement Generator is available at www.oecd.org/sti/privacygenerator

search engine may request location data from a consumer to improve search results but may not necessitate that information to fulfill the request. Considering the sensitivity of real-time location data, many consumers may choose to withhold that data if given the choice. Consumers should have the ability to set clear privacy preferences and then only be prompted when applications or devices request permission beyond those choices. Mobile applications and devices should also consider usability aspects. The permissions granted by the consumer should extend throughout the length of a transaction. For example, if a mobile device is providing directions and must access GPS data dozens of times during the trip, a consumer should only need to provide authorization one time. Otherwise, it will be prohibitive for the consumer to use these controls.

In the offline world, privacy notices should be made available at the moment of data collection whenever possible. As in the online world, data that is necessary for a transaction to take place should be separated from data that is requested from a consumer but not strictly necessary. Companies should be strongly encouraged to provide consumers with the ability to withhold data elements that are supplemental to the transaction.

• Should companies increase their use of machine-readable policies to allow consumers to more easily compare privacy practices across companies?

Where feasible, companies should be encouraged to increase their use of machine-readable policies. However, it is important that nuances and details of information are not lost when data is conveyed in machine-readable format.

• Should companies be able to charge a reasonable cost for certain types of access?

Companies should provide consumers with access to their data but should not assess a fee for that access. A company should be able to assess a fee for any physical copy that a consumer requests. This is in alignment with the consumer rights associated with medical records under the Health Insurance Portability and Accountability Act (HIPAA), whereby a consumer may inspect her medical record at no charge and a covered entity may only charge reasonable fees for copying and postage[4]. Costs associated with administration and labor would not be permissible. We believe that the consumer's rights to record inspection in the offline world can inform regulators and businesses about how to structure online world access to consumer records. We believe that, as in the medical context, a consumer's rights to accessing her records would be unduly prohibited if companies were to add fees.

• Should companies inform consumers of the identity of those with whom the company has shared data about the consumer, as well as the source of the data?

We believe that consumers should be made aware of the identity of corporations and,

[4] Patient's Guide to HIPAA: Part 2, Sec 21 "How Much Will It Cost?" World Privacy Forum. http://worldprivacyforum.org/hipaa/HipaaGuide21.html

where legally permissible, government agencies who access their data. However, we urge restraint as regards the identity of individual consumers who access data. In many instances, the rights of an online browser or purchaser of data should be weighed against the rights of the consumer the data describes. In the social networking context, users may have an expectation that they can browse public profiles anonymously. While it would be beneficial to provide consumers with an estimation of how many people accessed their profiles or pages, it would be inappropriate to disclose the identities of all visitors to a particular page without visitors' consent.

Furthermore, we believe that providing users with access to the source of data compiled about them is vital to helping consumers understand how data profiles are created and how to influence them. By providing consumers with information about the original source of data, consumers can combat misinformation or work to stop sensitive information from perpetuating by going directly to the original source. Failure to provide source information to consumers leaves consumers constantly struggling to remove false data that repopulates every time the data set is refreshed.

• Where companies do provide access, how should access apply to information maintained about teens? Should parents be able to access such data?

No. Teenagers require the option of privacy against their parents.

• Should access to data differ for consumer-facing and non-consumer-facing entities?

Yes. Consumers require extra protection against organizations they have no relationship with. We believe that access to consumer data by non-consumer-facing entities should be encouraged in the following ways:

1. The FTC should investigate this issue through workshops and investigation, and provide best practices for industries in this arena
2. We believe industry groups should implement a self-regulatory program akin to the IAB Self Regulatory Program for Online Behavioral Advertising. This program should provide consumers with a secure mechanism for accessing and/or deleting their records from a single point of control, and where feasible should also provide information about the source of data.
3. Legislation will likely be necessary to empower the FTC to regulate non-consumer-facing entities.

Any approach would need to be implemented with significant security precautions in order to prevent unauthorized access to the data!

In addition to access, we believe non-consumer-facing entities should maintain strict data retention limits.

• For non-consumer-facing companies, how can consumers best discover which

entities possess information about them and how to seek access to their data?

At this time, there is no method by which consumers can discover all of the entities that are collecting data about them, particularly non-consumer-facing companies. In Congressional testimony, Pam Dixon of the World Privacy Forum stated, "Consumers don't have the ability to see or understand the information that is being collected about them, and they don't have the tools to see how that information is impacting the opportunities that are being offered – or denied – to them."5

As Dixon explained, these non-credit, unregulated reporting agencies are seemingly beyond the purview of the FTC's authority regarding Fair Credit Reporting Act, even though these databases may include information which in other contexts would be within the jurisdiction of the FCRA. Not only are consumers unable to access and edit the information in these databases, they are unable to even know these databases exist. The most comprehensive list currently available to consumers is the Privacy Rights Clearinghouse's *Online Data Vendors: How Consumers Can Opt Out of Directory Services and Other Information Brokers*[6]. However, this list is far from complete and is weighted toward consumer-facing data brokers (those data brokers consumers can access themselves). There is no comprehensive list available for all data brokers, particularly those which sell and trade data between businesses.

Given this issue, we believe the FTC should hold workshops dedicated toward defining data brokers and identifying the threats to consumer privacy posed by such companies. We would support the FTC investigating whether such business practices might be considered unfair and deceptive, though we also believe legislation will ultimate be necessary to empower the FTC to successfully regulate this industry. We believe the privacy principles promoted in the FCRA provide a foundation for how such legislation could be structured.

• Is it feasible for industry to develop a standardized means for providing consumer access to data maintained by non-consumer-facing entities?

While this is currently an open research method as to the best mechanism for doing so, we believe that is feasible to develop a standardized means for providing consumer access to databases regardless of whether or not they are maintained by non-consumer-facing entities.

• Should consumers receive notice when data about them has been used to deny

---

5 *The Modern Permanent Record and Consumer Impacts from the Offline and Online Collection of Consumer Information*, of Pam Dixon, Executive Director, World Privacy Forum,Testimony Before the Subcommittee on Communications, Technology, and the Internet, and the Subcommittee on Commerce, Trade, and Consumer Protection of the House Committee on Energy and Commerce. *www.worldprivacyforum.org/pdf/TestimonyofPamDixonfs.pdf*

6 *Online Data Vendors: How Consumers Can Opt Out of Directory Services and Other Information Brokers, Privacy Rights Clearinghouse* http://www.privacyrights.org/online-information-brokers-list

them benefits? How should such notice be provided? What are the costs and benefits of providing such notice?

Yes, if a consumer is denied a service or benefit due to information gathered about them, consumers should have the right to know what data was used as well **as the source of the data**. Furthermore, we believe that consumers should have a right to know when data is being used to measure whether they will receive a benefit, regardless of whether or not the benefit is denied. In California, Civil Code §1786 provides consumers with the right to access an employment background check even 1) when they are not denied the position and 2) when the background check is not conducted by a third party. These additional protections ensure consumers can track down inaccurate information even if a potential employer cites another reason for rejecting the applicant or conducts the background check in-house. We believe similar protections are necessary in other circumstances in which a company utilizes data about a consumer to deny them other benefits. If a consumer is being formally evaluated for a benefit based on data elements collected on him or her, he or she should be informed of the database from which the data is derived, regardless of whether he or she is rejected the benefit. This would apply to job applications, credit applications, membership benefits and insurance applicants, among other things. The consumer report should be made available at no additional cost to the consumer.

• **What types of changes do companies make to their policies and practices and what types of changes do they regard as material?**

Websites can and do make substantive changes to their privacy policies and practices frequently, often in ways that may harm consumers or violate a consumer's expectation of privacy. Some elements that are routinely altered include but are not limited to:

- What information is required from a consumer to access a site or service
- What information is requested from a consumer to access a site or service
- What information is shared with other companies, applications, developers or affiliates, as well as which companies and affiliates
- Internal data security practices
- What information is made accessible to others (either through a URL or a search) and to whom (other registered site users v. general public, etc)
- How and when data is expunged
- Whether and when consumers can access, correct or remove data
- How information that is organized (for example, information reorganized in particular ways may make otherwise information that was hard to find more accessible, as with Facebook's recent page

• What is the appropriate level of transparency and consent for prospective changes to data-handling practices?

Companies undertaking a significant change in data-handling procedures should ensure:

1. Adequate prior notice is provided to consumers before change affects their

data.

2. Robust data portability policies should allow users to access and download their data so that they can migrate to a competing service, especially if the change in policy does not suit their privacy expectations.
3. Consumer outreach and education should be geared toward helping consumers understand how changes in policies will affect their data. Multimedia presentations should be encouraged to reach out to users, especially those with limited reading proficiency.
4. Wherever possible, users should be prompted to actively accept changes, so that it is clear that users are aware that changes are occurring.

- **What choice mechanisms regarding the collection and use of consumer information should companies that do not directly interact with consumers provide?**

• Is it feasible for data brokers to provide a standardized consumer choice mechanism and what would be the benefits of such a mechanism?

Such a standardized consumer choice mechanism would be an enormous boon to consumers. Currently, consumers struggle to identify all of the data brokers that collect their personal information, assess which of these companies provide a method of restricting the data they serve, communicate to each of these companies individually about one's data preferences and then periodically review whether sensitive information has been repopulated and whether new data brokers have entered the field. Consumers shoulder the entire burden for attempting to limit this data proliferation while having no meaningful choice about how their data is collected and used.

The data broker industry is currently largely unregulated. However, industry figures such as Intelius and Acxiom have proven that it is feasible to provide users with opt-out mechanisms to restrict the flow of certain types of sensitive consumer data. There are three challenges remaining: 1) many data brokers still do not provide an opt-out mechanism; 2) a consumer should be able to opt-out of having certain data elements restricted all at once, without contacting dozens or hundreds of companies; 3) enforcement will be necessary to ensure that data brokers respect the wishes of consumers to restrict their personal information. Enforcement will also necessitate a specific definition of what constitutes a data broker.

This issue necessitates further study as to the optimal methods of addressing each of these challenges. However, it is both feasible and desirable to empower users with a standardized consumer choice mechanism for data brokers.