KEEPING THE INTERNET
OPEN • INNOVATIVE • FREE

www.cdt.org

CENTER FOR DEMOCRACY
& TECHNOLOGY

1634 I Street, NW
Suite 1100
Washington, DC 20006

P +1-202-637-9800
F +1-202-637-0968
E info@cdt.org

COMMENTS OF THE CENTER FOR DEMOCRACY & TECHNOLOGY BEFORE THE FEDERAL TRADE COMMISSION IN THE MATTER OF PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: A PROPOSED FRAMEWORK FOR BUSINESSES AND POLICYMAKERS

FEBRUARY 18, 2011

The Center for Democracy & Technology appreciates the opportunity to respond to the questions posed in the Commission's draft privacy report. We believe the draft report provides a strong foundation for a privacy protection framework and we applaud the FTC's excellent work. We are especially pleased to see that the FTC has embraced the full range of the Fair Information Practice Principles and recommended that those principles be applied to all companies that collect, use, and maintain consumer information, both online and offline. Fundamentally, CDT believes that this framework can only be accomplished across the entire ecosystem through baseline privacy legislation, and we urge the FTC to endorse that approach as the appropriate means to implement a new privacy protection framework in its final report. We respectfully submit these comments in response to the Commission's questions.

RESPONSE TO QUESTIONS POSED BY THE FEDERAL TRADE COMMISSION

Scope

- *Are there practical considerations that support excluding certain types of companies or businesses from the framework — for example, businesses that collect, maintain, or use a limited amount of non-sensitive consumer data?*

While the Fair Information Practice Principles are relevant to all entities, CDT supports a narrow exception to any regulatory framework for companies that store or otherwise process non-sensitive information about a relatively small number of individuals. However, companies exempted from the coverage of federal privacy regulation or legislation should nonetheless be encouraged to evaluate the privacy implications of their services and incorporate privacy by design before reaching the regulatory

threshold.[1] And, of course, companies regardless of size remain subject to basic privacy and security obligations under the FTC's unfair and deceptive jurisdiction.

The privacy bills proposed by Congressmen Boucher and Rush in the last Congress both contained exceptions to coverage for businesses that collect data relating to fewer than 15,000 people during a calendar year.[2] However, CDT recommended modifications to both exceptions. The language in the Boucher bill only applied to entities that collect data directly from a consumer and thus seemingly excepted non-consumer facing entities such as data brokers. Such an exception is far too broad. On the other hand, the language in Congressman Rush's BEST PRACTICES bill stated that the exception for small businesses did not apply to entities that "use covered information to study, monitor, or analyze the behavior of individuals as the person's primary business."[3] CDT expressed concern that this exception to the exception could be interpreted to extend coverage of the bill to investigative reporters and other news outlets, and we recommended that it be clarified to exempt news outlets to address First Amendment concerns.[4]

Japan's 2003 Personal Information Protection Act provides one example of how to draw a line that would promote privacy without erecting impediments to small business development. The Japanese law exempts low-risk entities that handle the individual records of fewer than 5,000 people during a six-month period; however, small entities that handle highly sensitive data are covered by the law.[5]

- *Is it feasible for the framework to apply to data that can be "reasonably linked to a specific consumer, computer, or other device"?*

Yes, CDT agrees that it is both feasible and desirable for the privacy framework to apply to any data that can be "reasonably linked to a specific customer, computer or device."

CDT strongly supports that the framework addresses both online and offline data. While much of the recent debate and news in Washington has focused on online data, consumers' privacy interests are equally affected when offline data is collected and used in unexpected ways. Moreover, while the online behavioral advertising industry has taken some steps toward meaningful self-regulation over the past several years,[6] comparable efforts to self-regulate by data brokers and other offline (and online) entities

[1] For more on Privacy by Design, *see* Comments of the Center for Democracy & Technology, FTC Consumer Roundtable, December 21, 2009 *available at* http://www.cdt.org/privacy/20091105_ftc_priv_comments.pdf.
[2] *See* Addendum to Testimony of Leslie Harris, President and Chief Executive Officer of the Center for Democracy and Technology, before the House Committee on Energy and Commerce, Subcommittee on Commerce, Trade, and Consumer Protection on "The BEST PRACTICES Act of 2010 and Other Federal Privacy Legislation" (July 22, 2010) *available at* http://cdt.org/files/pdfs/Privacy bills comparison chart_CDT_0.pdf.
[3] *Id.*
[4] *Id.*
[5] *See* Martha L. Arias, *Japan's Privacy Law* (March 29, 2010*), available at* http://www.ibls.com/internet_law_news_portal_view.aspx?s=latestnews&id=2242.
[6] *See* The Self-Regulatory Program for Behavioral Advertising Website, http://www.aboutads.info/ (last visited Feb. 18, 2010).

have either failed to develop or have foundered from lack of support.[7]

CDT also applauds the decision to move away from the outdated concept of "personally identifiable information." We believe the concept of "PII" has lost validity for two reasons. First, we strongly disagree with the notion that there are no privacy implications for consumers when profiles and tracking are linked to a pseudonymous device ID number rather than to a real-name identifier. Polls indicate that a majority of consumers object to having their activities tracked and used by third parties regardless of whether the tracking entity uses or even knows the consumer's name.[8] For that reason, we support the FTC's suggestion that the privacy framework should apply not only to any information tied to a person (identified by name or not) but also to information tied to a specific computer or device, including those such as a home computer that may be used by more than one person.

Second, changes in technology have rendered the term "personally identifiable information" a moving target. It is now well documented that non-personally identifiable information can be re-identified and used in ways that affect individuals.[9] Thus, CDT supports the FTC's application of the framework to data that can be "reasonably linked to a specific consumer, computer, or other device." A test of reasonableness is especially appropriate given the highly context-dependent of data "linkability."[10] We also appreciate, however, that companies deserve some clarity as to what is reasonably linkable and what is not. Companies that make reasonable, good faith efforts to de-link data from a consumer's identity (whether real-name or pseudonymous) or the identity of her device should not be penalized if new predictive or statistical models arise that render their efforts technically insufficient. Indeed, the threat of unfair penalization risks disincentivizing good faith efforts to de-identify data.

Accordingly, CDT urges the FTC to develop appropriate guidance and best practices concerning when data can and cannot be considered "reasonably linked" to a specific consumer, computer, or other device. (Development of such guidance should not,

---

[7] Comments of Chris Hoofnagle before the Department of Commerce, Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework, January 28, 2011 *available at* http://www.ntia.doc.gov/comments/101214614-0614-01/attachments/hoofnagle_doc_comments.pdf.

[8] *See, e.g.,* Edward C. Baig, *Internet users say, Don't track me*, USA TODAY, December 14, 2010, http://www.usatoday.com/money/advertising/2010-12-14-donottrackpoll14_ST_N.htm; Scott Cleland, *Americans want online privacy –per new Zogby poll*, The Precursor Blog, June 8, 2010, http://www.precursorblog.com/content/americans-want-online-privacy-new-zogby-poll.

[9] *See, e.g.,* Michael Barbar and Tom Zeller Jr., "A Face Is Exposed for AOL Searcher No. 4417749," New York Times, August 9, 2006, http://www.nytimes.com/2006/08/09/technology/09aol.html?_r=1&sq=aol%20data&st=Search&adxnnl=1&scp=2&adxnnlx=1262034171-J0pzIkEl93sbpKmhZ7NiCA, and Erica Newland, "Netflix Needs to Put 'Privacy Risks' in Their Queue," September 30, 2009, http://www.cdt.org/blogs/erica-newland/netflix-needs-put-privacy-risks-their-queue.

[10] For example, data sets that are released to the public, by virtue of being accessible to expert mathematicians, are far easier to link to individuals.[10] Hence, data that may not be "reasonably linked" to a specific consumer, computer, or other device when kept as proprietary information may need to be further obfuscated or aggregated prior to public release. *See, e.g.*, Erica Newland, Center for Democracy & Technology, PolicyBeta Blog, *Netflix Needs to Put "Privacy Risks" in Their Queue* (Sept. 30, 2009), http://blog.cdt.org/2009/09/30/netflix-needs-to-put-privacy-risks-in-their-queue/ (last visited Nov. 10, 2009); Michael Barbaro & Tom Zeller, Jr., *A Face is Exposed for AOL Searcher No. 4417749*, N.Y. TIMES, Aug. 9, 2006, *available at* http://www.nytimes.com/2006/08/09/technology/09aol.html (AOL incident highlights the difficulties in making data truly anonymous).

however, hold up adoption of the framework.)

- *How should the framework apply to data that, while not currently considered "linkable," may become so in the future?*

Once a company recognizes that data it had previously thought to be non-linkable is actually linkable to the identity of a person, computer, or device, that data should be deemed to be encompassed by the framework, and appropriate action should be taken.

However, CDT believes that applying the framework to data that is not currently considered "linkable," but *may* be so in the future, will effectively apply the framework to all non-aggregate data. This would disincentivize companies from attempting to de-identify their data: de-identification would render the data potentially less valuable while not reducing the compliance burden. Instead, we would limit the framework's application to data that a company *reasonably and objectively believes* will be linkable to the identity of a person (whether real name or pseudonymous) or device, recognizing that companies should not be expected to be prescient about future technologies and will not be able to reasonably foresee all innovations that may make certain data sets more linkable to individuals than was previously possible.

However, companies should be required to detail in their privacy policies which data they will hold in a linkable form and which data they will hold in a non-linkable form. If previously-collected non-linkable data were to be combined with other data such that this non-linkable data becomes linkable, then this would require affirmative consent from the affected consumers (as a material change in how previously collected data is being used).

Companies should promote consumer privacy throughout their organizations and at every stage of the development of their products and services

Incorporate substantive privacy protections

- *Are there substantive protections, in addition to those set forth in Section V(B)(1) of the report, that companies should provide and how should the costs and benefits of such protections be balanced?*

CDT is very pleased that the preliminary staff report included all of the FIPs principles as recommended by CDT. However, the FIPs are presented in a disjointed and possibly confusing way: Data Security, Collection Limit and Retention Limit (Data Minimization), and Accuracy are in V(B)(1), while Individual Participation is in V(C), Transparency, Purpose Specification, and Use Limitation are in V(D), and Accountability and Auditing are in V(B)(2). We believe that the clarity of the framework would be greatly improved if all of the FIPs were set forth in a comprehensive fashion in one section and in a more logical fashion, placing Purpose Specification ahead of the limits on data collection, retention and use, all of which flow from the purpose specification.

In particular, we note that Use Limitation, which is a core substantive protection, is somewhat buried in Section V(D). Whereas collection limitation refers to the principle whereby "companies should collect only the information needed to fulfill a specific,

legitimate business need," Use Limitation refers to the principle whereby collected information should only be *used* to fulfill these previously-specified specific, legitimate business needs. By specifically calling out Use Limitation as a substantive protection, the FTC's privacy framework should make clear that the adoption of a data use practice not specifically described in a purpose specification (see discussion *infra*, pp. 5-6) will be considered a deceptive or unfair practice by the FTC.[11]

Since the substantive protections outlined in Section V(B)(1), as well as the use limitation protection, hinge on the implementation of the Purpose Specification FIP, CDT suggests that the FTC more clearly articulate the purpose specification requirement.[12]

- *Should the concept of "specific business purpose" or "need" be defined further and, if so, how?*

CDT urges the Commission to link the concept of "specific business purpose" or "need" more strongly to the Purpose Specification FIP, requiring clear and specific disclosure of businesses' actual use of consumer data. The FTC should provide further examples of what constitutes a "specific business purpose" or "need."

CDT supports the FTC's requirement that "companies should collect only the information needed to fulfill a specific, legitimate business need." However, companies should additionally be required to *state* the "specific, legitimate business need" for which they are collecting data in a privacy policy and also through just-in-time notices. *See infra*, pp. 23-24. Requiring companies to make affirmative statements about how they will use data will make purpose specifications enforceable and more transparent to consumers.

However, purpose specifications only promote privacy insofar as they are girded by substantive parameters. As the Department of Commerce stated in its recent Green Paper: "An entity that clearly states that it intends to do anything and everything with the data it collects . . . may not be providing adequate protection for consumer privacy."[13] CDT emphatically agrees. Purpose specifications should take the form of narrowly scoped, clear, affirmative, and binding statements describing the purpose of data collection and how it relates to a "specific business purpose" or "need."

For example, the FTC should clarify that "product improvement" is not a "specific business purpose." Companies should explain how the data they are collecting is being used to improve specific products. The just-in-time notice and consent mechanism that Google shows users of its personalized voice search tool for Android phones is an example of purpose specification done right. Consumers are shown a full-screen notice with a large header that reads "Personalized recognition." Below the header, the notice reads: "To improve speech recognition quality, Google will associate your recordings with your Google Account per the Mobile privacy policy." The notice links to the privacy policy and users can choose "yes" or "no."

---

[11] CDT believes that they may constitute a deceptive or unfair practice under the current privacy framework as well.

[12] Comments of the Center for Democracy & Technology before the Department of Commerce, Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework, 10-13 *available at* http://www.ntia.doc.gov/comments/101214614-0614-01/attachments/CDT%20privacy%20comments.pdf.

[13] *Id.*

The FTC's privacy framework should make clear that the adoption of a data collection or use practice not specifically described in a purpose specification will be considered a deceptive or unfair practice by the FTC.[14] CDT further believes that in any new privacy framework, a failure to clearly state specific purposes for using personal information should be illegal and subject to enforcement. The inclusion of language that is excessively broad or generalized should similarly be forbidden and subject to enforcement.[15]

- *Is there a way to prescribe a reasonable retention period?*

- *Should the retention period depend upon the type or the sensitivity of the data at issue? For example, does the value of information used for behavioral advertising decrease so quickly that retention periods for such data can be quite short?*

CDT does not recommend specific, cross-industry time limits for data retention in law or FTC guidance. Such mandates could inadvertently freeze today's practices and discourage future innovation. CDT supports the standard articulated in the FTC privacy report: "companies should implement reasonable and appropriate data retention periods, retaining consumer data for only as long as they have a specific and legitimate business need to do so." Companies should be required to specify to consumer their retention periods for data, as well as their "specific and legitimate business needs."

Flexible approaches to data retention should not, however, give *carte blanche* to companies to maintain consumer data after it has outlived its reasonable usefulness. Under the current law, companies clearly do not have adequate incentives to put reasonable and appropriate data retention policies in place.[16] For this reason, CDT believes it may be appropriate for the Commission, after further inquiry, to recommend or prescribe industry-specific limits on how long data can be retained. (As with other implementation details, the development of any such specific requirements could proceed incrementally *after* the basic framework is adopted.) Alternatively, in sector-specific privacy standards such as those suggested in the Department of Commerce Green Paper[17] and in the BEST PRACTICES bill introduced by Congressman Rush,[18] self-regulatory groups should, with consultation with regulators and civil society, develop industry-specific "codes of conduct" that would include limitations on how long data can be retained within that sector. Such limitations would then be subject to FTC approval and enforcement.

---

[14] CDT believes that they may constitute a deceptive practice under the current privacy framework as well.
[15] For example, the overview of the Buy.com privacy policy reads: "Except as limited below, we reserve the right to use or disclose your personally identifiable information for business reasons in whatever manner desired." A statement such as this should constitute a deceptive practice. *See* Buy.com Privacy Policy, July 30, 2009, *available at* http://www.buy.com/corp/privacy_policy_complete.asp (last visited Jan. 27, 2011).
[16] "Information is now cheaper to save than to destroy, meaning data hangs around for a long time — and may later be given a new purpose that may or may not be consistent with consumer expectations…" *See* Remarks of David C. Vladeck, Director, FTC Bureau of Consumer Protection, at the International Association of Privacy Professionals Privacy Academy, September 29, 2010 *available at* http://www.ftc.gov/speeches/vladeck/100929conprivacy.pdf.
[17] Department of Commerce (Internet Policy Task Force), *Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework* (Dec. 16, 2010) *available at* http://www.ntia.doc.gov/reports/2010/IPTF_Privacy_GreenPaper_12162010.pdf.
[18] BEST PRACTICES Act, H.R. 611, 112th Cong. (2011).

- *How should the substantive principles set forth in Section V(B)(1) of the report apply to companies with legacy data systems?*

CDT appreciates that it may be challenging for companies to apply new substantive requirements to legacy data systems. However, we caution against any permanent exception to compliance requirements — in FTC guidance or in a consumer privacy law — for legacy systems. Such an exception would incentivize companies to *avoid* updating their data systems so that they could be exempted from providing substantive privacy protections for consumers.

Accordingly, CDT recommends that FTC guidance or a consumer privacy law may include a reasonable grace period during which companies can update their systems, but not provide an unlimited exception for companies with legacy data systems. For instance, Mozilla has announced that it will allow consumers to set persistent "Do Not Track" preferences for online tracking by sending "Do Not Track" HTTP headers in the next release of its web browser Firefox.[19] It may not be reasonable to expect that all third-party tracking networks will have the infrastructure in place to honor such a header immediately upon release. After consultation with stakeholders, it may be appropriate for the FTC to declare that networks have a certain amount of time to program their systems to respect such a header, after which failure to adhere to the header may be deemed a deceptive or unfair practice.

Maintain comprehensive data management procedures

- *How can the full range of stakeholders be given an incentive to develop and deploy privacy-enhancing technologies?*

CDT has long argued and continues to believe that companies need baseline privacy legislation to generate the necessary incentives for the adoption of privacy-enhancing technologies and other forms of privacy by design.[20] It will be difficult if not impossible to incentivize many industry players to deploy privacy enhancing technologies unless legislation establishes a common floor of privacy protection.

However, there may be specific mechanisms within such a legal framework for encouraging adoption of privacy-enhancing technologies. For example, under privacy frameworks such as those suggested in the Department of Commerce Green Paper and in the BEST PRACTICES legislation, industry-specific "codes of conduct" could include descriptions of how signatory companies will deploy privacy-enhancing technologies. Such descriptions could be taken into consideration as the Commission determines whether or not to approve the code and the Commission could make it clear that it would be more likely to approve codes outlining how member companies will adopt these technologies.

[19] Julia Angwin, *Web Tool On Firefox To Deter Tracking*, THE WALL STREET JOURNAL, January 24, 2011, http://online.wsj.com/article/SB10001424052748704213404576100441609997236.html.
[20] *See, e.g.,* Statement of Leslie Harris, President and Chief Executive Officer of the Center for Democracy and Technology, Before the Senate Commerce, Science & Transportation Committee, "Privacy Implications of Online Advertising" (July 9, 2008) *available at* http://www.cdt.org/files/pdfs/20080709harri.pdf.

Companies should simplify consumer choice

Commonly accepted practices

- *Is the list of proposed "commonly accepted practices" set forth in Section V(C)(1) of the report too broad or too narrow?*

CDT supports the FTC's proposal that companies should not need to provide choice before collecting and using data for "commonly accepted practices," such as billing and shipping, provided that the other Fair Information Practice Principles (including transparency, purpose specification, data minimization, and security) still apply to such data.

However, we have reservations about the scope and possible overbreadth of the "Internal Operations" category of behaviors. The "Internal Operations" category is described in the draft report entirely by two examples: one related to what might be called "product improvement" and one that describes website analytics. The concept of product improvement is potentially very broad and could be used to justify the collection and storage of large amounts of consumer data without any choice on the part of consumers. For example, consider a mobile map and global positioning app that routinely collects precise geolocation data about individuals as they use the app to navigate around town. Under a "product improvement" exception, the app maker could reasonably maintain detailed records of its users' everyday movements in order to gain greater insight into how its customers use their products, even after the data is no longer necessary for the specific session in which the customer was using the service. While some users might be fine with the collection and use of their location data for such product improvement, others may reasonably deem the privacy costs too steep. Given the special sensitivity of location information, we think that consumers should be asked for opt-in permission for all uses beyond provision of the service itself. More generally, consumers should have some control over whether they will serve as the subjects of experimentation by the companies whose services they use.

Similarly, analytics programs, including third-party analytics programs, could potentially be used to amass detailed profiles tied to persons or devices about individual usage of web services that a consumer may reasonably object to. Many analytics programs already allow consumers to opt out of being tracked for analytics purposes.[21] Moreover, analysis that aggregates usage for reporting purposes is already exempted from the scope of the framework, so this exemption would only apply to personalized tracking. *See supra*, pp. 2-4.

CDT suggests that the FTC redefine "Internal Operations" to be more consistent with language in the BEST PRACTICES bill, which defines one subset of "operational purpose" (thus outside the bill's choice requirements) as "basic business functions such

[21] *See, e.g.,* Google Analytics Opt-out Browser Add-on (BETA), http://tools.google.com/dlpage/gaoptout, (last visited Feb. 17, 2011).

as accounting, inventory and supply chain management, quality assurance, and internal auditing."[22]

CDT also has reservations about expanding the scope of "commonly accepted practices" to first-party marketing. *See infra*, pp. 9-11.

- *Are there practices that should be considered "commonly accepted" in some business contexts but not others?*

Although core "commonly accepted practices" will not and should not dramatically change across industries, it is quite possible that there will be distinctions at the margins.

For example, many modern websites regularly incorporate third-party content, including third-party advertising, into their sites. These third parties necessarily obtain and use the user's IP address (and potentially other information) simply in order to deliver such content to the user's browser. The FTC's definition of "commonly accepted practices" could include third-party web advertising and content delivery so long as those third parties were not using the information for tracking or other non-commonly accepted practices. In our draft scoping proposal of the definition of "Do Not Track," CDT carves out from the scope of a "Do Not Track" request an exception for non-tracking third-party content and advertising delivery. *See infra*, pp. 17-18. However, industries that do not rely on the sharing of unique identifiers to deliver content would not need to take advantage of such an exception.

The question of defining "commonly accepted practices" is part of the broader question of developing, for many elements of the framework, implementing rules suitable to unique features of certain sectors. Any privacy protection framework should allow and encourage different industries to innovate, and thus should provide flexibility. For that reason, CDT has recommended giving FTC discretionary rulemaking authority as part of any privacy legislation in order to fine tune the application of the FIPs to a wide range of companies.[23] CDT has also endorsed a coregulatory approach that allows industry associations to suggest industry-specific codes of conduct that would be deemed compliance with a privacy framework, subject to FTC approval and enforcement.[24] Such coregulatory codes may help define "commonly accepted practices."

- *What types of first-party marketing should be considered "commonly accepted practices"?*

CDT is skeptical about whether first-party marketing is appropriately deemed a "commonly accepted practice" such that consumers have no choice whatsoever about that use of their personal information for that purpose. We certainly recognize the distinction in principle between first- and third-party marketing. In our draft definition of the scope of what "Do Not Track" should mean for web browsers, CDT suggested that first-party marketing is appropriately outside the scope of "Do Not Track." In our

[22] BEST PRACTICES Act, *supra* note 18.
[23] *See* Addendum to Testimony of Leslie Harris, *supra* note 4; *see also* Comments of the Center for Democracy & Technology before the Department of Commerce, *supra* note 12.
[24] *Id.*

assessment, global choices such as "Do Not Track" are more appropriate to the third party context where a consumer may not always know what companies may be tracking them. On the other hand, consumers generally know what first parties they are interacting with, and thus have a greater ability to manage that relationship and information sharing themselves without relying on a global "Do Not Track" instruction.

However, that does not mean that the collection and use of personal information for marketing purposes should be completely without choice by the consumer. This brings us to an ambiguity in the FTC's presentation of the "commonly accepted practices" concept: While some commonly accepted practices, such as billing, should be subject to neither opt-in nor opt-out, others, such as marketing and product improvement, should at the very least be subject to opt-out. CDT believes it is appropriate to offer consumers the ability to opt out of first-party marketing on a company-by-company basis. We previously endorsed the approach in the BEST PRACTICES bill[25] that allows consumers to opt out of first-party marketing usage of their data, but also allows those first parties to refuse to do business with consumers who withhold their information for such purposes.[26]

- *Even if first-party marketing in general may be a commonly-accepted practice, should consumers be given a choice before sensitive data is used for such marketing?*

Regardless of the rules established for first-party marketing based on non-sensitive information, CDT firmly believes that companies should only use sensitive consumer information for marketing after receiving the consumer's affirmative consent after clear and conspicuous disclosure from the company. This position is consistent with what the FTC previously advocated in 2009 Self-Regulatory Principles for Online Behavioral Advertising, which stated that "companies should only collect sensitive data for behavioral advertising after they obtain affirmative express consent from the consumer to receive the advertising."[27]

The fact that opt-in permission is deemed necessary for even first parties to market based on sensitive information argues against the proposal to not give consumers any choices at all regarding other first-party marketing by deeming it a "commonly accepted practice." Obviously, the line between what is sensitive and what is not sensitive will be hazy at times; under the FTC's suggested formulation, types of data on one side of the line will require opt-in permission for marketing while similar data just on the other side of the line will require no permission at all. CDT proposes that consumers should have some control over non-sensitive first-party marketing through the ability to opt out of such usage of their information. Under CAN-SPAM, consumers have the right to opt out of first-party marketing entirely.[28] We merely propose to allow consumers to opt out of the usage of data shared for other purposes in first-party marketing.

[25] The BEST PRACTICES ACT, *supra* note 18.
[26] *See* Addendum to Testimony of Leslie Harris, *supra* note 4.
[27] Federal Trade Commission Staff Report: Self Regulatory Principles for Online Behavioral Advertising, at 42, *available at* http://www.ftc.gov/os/2009/02/P085400behavadreport.pdf.
[28] *See* The CAN-SPAM Act of 2003, Pub. L. No. 108-187, 117 Stat. 2699 (2003) (codified at 15 U.S.C. §§ 7701-7713 and 18 U.S.C. § 1037)

- *Should first-party marketing be limited to the context in which the data is collected from the consumer?*

While consumer expectations about the use of shared data for first-party marketing purposes may change as the correlation between the sharing and the eventual marketing becomes more attenuated, CDT believes that consumers should have some choice over all first-party marketing use of their data for targeted ad delivery, regardless of context or mode of delivery.

- *Should marketing to consumers by common-branded affiliates be considered first-party marketing?*

CDT supports the FTC's use of common branding as the determining factor in defining the contours of first parties. The determination of the scope of a party should depend upon association with a common brand or identity that is meaningful to the ordinary consumer, not artificial corporate structures or disingenuous labeling. It is reasonable to allow different corporate entities to share information on a first-party basis so long as those entities clearly operate in the eyes of the consumer under the same name or identity, such that a consumer would not be surprised by the data exchange.[29]

On the other hand, CDT strongly cautions against an overly broad definition of first-party to allow first-party sharing and marketing by all companies under common control. Broad affiliate sharing of commonly controlled entities has been widely criticized under the Gramm-Leach-Bliley rules for financial privacy,[30] and would not offer adequate protections in a broader baseline context. Modern media conglomerates often own and operate a wide range of separately branded domains that an ordinary consumer would not expect to be sharing user data with each other. Sharing of consumer data for marketing across such non-commonly branded domains should not be considered "first-party" marketing.

Practices that require meaningful choice

General

- *What is the most appropriate way to obtain consent for practices that do not fall within the "commonly accepted" category?*

CDT believes consent should always be obtained in a clear, concise, and time-appropriate manner tailored to the functional and aesthetic context of the service. Meaningful consent presupposes understanding by the consumer, which focuses on relevance and readability. However, we emphasize here, as the Commission found, that notice has its limits. The privacy challenges posed by 21st-century technology and business practices require implementation of the substantive privacy protections represented by the full set of FIPs.

[29] Pub. L. 108-187, S. 877 (2003) (codified as 15 U.S.C. § 7701 *et seq.*).
[30] *See* Gramm-Leach-Bliley Act, Pub. L. No. 106-102, § 507, 113 Stat. 1338 (1999) (codified as 15 U.S.C. § 6807).

Consent should always be obtained in a clear, concise, and time-appropriate manner. This means notices should be easy for the average person to understand, presented in a few short sentences, placed in a sensible location, and displayed at a time relevant to the consent.[31] Obtaining meaningful consent must be carefully implemented across both functional and aesthetic contexts. There is no "one size fits all" solution. Appropriate consent mechanisms must be designed with particular products and services in mind.

Some companies have made meaningful disclosures and provided clear explanations about consumer data usage outside of privacy policies. For example, the location-based service Loopt has done a good job of presenting basic information to consumers through the cell phone screen during the sign-up process. There have been some innovations in the applications space, as both Facebook and various mobile operating systems have implemented permissions models that clearly show, in digestible form, the data to be transferred to the third-party application at the initial permission request (though disclosure about the purposes for which those permissions are requested is typically lacking).

A key to effective choice is the disclosure of both the purposes of data collection and whether that data will then be transferred to other parties. Without meaningful disclosure of purpose specification, transparency as to data collection is of limited utility.

As these various examples have illustrated, consent should be obtained through carefully designed and appropriately implemented notices. However, it bears repeating that notice in the online context suffers from multiple and well-understood problems.[32] Notice and consent are crucial — and can be improved — but they are simply not enough on their own. They must be implemented as part of a mandatory baseline privacy framework that incorporates all of the Fair Information Practice Principles.

- *Should the method of consent be different for different contexts?*

Yes. Consent practices should be carefully tailored to different contexts. As with other Fair Information Practices such as data minimization that may apply differently to different industries, *see supra*, p. 6, coregulatory industry programs subject to regulatory review and enforcement may develop methods of consent that provide for appropriate innovation and certainty in a variety of contexts.

In the mobile space, for example, challenges facing meaningful consent are heightened. Small screens reduce opportunity for meaningful notice, and apps often collect UDIDs or other unique identifiers from mobile phones.[33] These factors intensify privacy concerns and are compounded by a relatively new and evolving mobile data ecosystem that is not well understood by consumers, platforms or application developers. Both platforms and application providers must strive to provide enhanced notice, but fully effective gains for

[31] *See generally* Complaint, In the Matter of Sears Holdings Management Corporation, No. C-4264 (Aug. 31, 2009), *available at* http://www.ftc.gov/os/caselist/0823099/090604searscmpt.pdf.
[32] *See, e.g.,* Howard Latin, *"Good" Warnings, Bad Products, and Cognitive Limitations*, 41 U.C.L.A. L. REV. 1193, 1221 (1994) (noting research findings that "the effectiveness of a warning is very dependent on the particular format selected, but exhaustive disclosure is incompatible with clear and vivid message formats").
[33] *See* Jennifer Valentino-DeVries, *Unique Phone ID Numbers Explained*, Digits Blog, December 19, 2010, http://blogs.wsj.com/digits/2010/12/19/unique-phone-id-numbers-explained/.

consumer privacy will require attention to the other elements of the FIPs on the part of platforms and app developers. CDT is currently conducting a project aimed at developing privacy guidelines for platform and application developers; our goal is to release final recommendations, after dialogue among all stakeholders, by the end of this year.

As suggested by the Commission, companies bear the responsibility to obtain a user's affirmative consent before using previously collected data in materially new ways. One approach is to present users with a "forced choice" that compels meaningful participation. For example, when the music listening site Pandora wanted to share users' music stations through Facebook, it prompted all users on its webpage to affirmatively choose whether they wanted their profile to be "public" or "private." Users had to choose one or the other — they couldn't just close the box to return to the default of public sharing. The box also contained links to give users the chance to learn more about how sharing works. The strength of this method is it prevents unwitting bypass of important decisions.[34]

- *Under what circumstances (if any) is it appropriate to offer choice as a "take it or leave it" proposition, whereby a consumer's use of a website, product, or service constitutes consent to the company's information practices?*

CDT believes that a primary goal of any privacy framework should be to allow consumers to make informed choices about how they share their information. By and large, where there is competition and where the transaction does not involve essential services, we do not object to companies offering "take it or leave it" value propositions to consumers, provided that the terms of the bargain are clearly and conspicuously disclosed and meaningful consent is obtained. Many online services operate under such a model today. In a robust marketplace where numerous sites and services are competing for users' business, we welcome innovative monetization models so long as terms are transparent and fairly presented. We would have reservations, however, about presenting consumers with "take it or leave it" propositions for essential services or in situations where there are few or no alternatives. Without a true market to adequately price privacy costs (or to allow consumers multiple options as to how they spend either their dollars or data), fiats to consumers to share data for secondary purposes may be inappropriate.

- *What types of disclosures and consent mechanisms would be most effective to inform consumers about the trade-offs they make when they share their data in exchange for services?*

As discussed *supra*, pp. 12-13, consent practices must be thoughtfully tailored to different contexts. "Take it or leave it" services typically provider fewer, if any, options to consumers to modify or interact with data practices. Accordingly, it is especially important that notices and disclosures implement the Purpose Specification FIP in a robust and clear fashion. A thorough and clear disclosure of purpose specification would give consumers a better sense of the bargain they're entering into when they choose to use a "take it or leave it" service.

[34] *See* Justin Brookman, *Closing Pandora's Box*, CDT Blog, August 4, 2010, http://www.cdt.org/blogs/justin-brookman/closing-pandora%E2%80%99s-box.

- *How should the scope of sensitive information and sensitive users be defined and what is the most effective means of achieving affirmative consent in these contexts?*

CDT supports enhanced protections for sensitive information, especially precise location information and information relating to health or medical history.[35] For defining "health information," the definitions in the regulations under the Health Insurance Portability and Accountability Act (HIPAA) might prove a useful model. As discussed *supra*, pp. 11-13, consent must be obtained in a clear, concise, and time-appropriate manner. Enhanced consent measures may be needed for some classes of sensitive data.

Although we support requiring opt-in consent for health information, we also want to make clear that adequately protecting health data requires more than merely applying greater consent rights. As stated clearly in the FTC Report, and as CDT has consistently argued, overemphasis on notice and consent results in weak privacy protection in practice. Protection of health information both on-line and off-line requires a comprehensive approach based on the full complement of fair information practices. We also urge the FTC to work closely with the Department of Health and Human Services to achieve a more coherent and consistent approach to protecting health data regardless of which entity is accessing, using or disclosing it, and regardless of the application of the HIPAA privacy and security rules.

- *What additional consumer protection measures, such as enhanced consent or heightened restrictions, are appropriate for the use of deep packet inspection?*

Just as with all other uses of technology for collecting data about individuals, uses of DPI require the protection of the full set of FIPs. Because Internet service providers (ISPs) serve as the gateway to the rest of the Internet, they have the potential to conduct profound and comprehensive surveillance of their users.[36] When DPI (or any other technology) is used to this full potential, those employing it should be held to the highest standards. Enhanced requirements in the form of robust, meaningful notice; informed and affirmative consent; strict collection, use, and disclosure limitations; strong security measures; and rigorous accountability and redress procedures would all certainly be warranted in this case.

However, DPI can serve a range of purposes (and be deployed in more or less invasive ways), each of which involves a different set of privacy risks and benefits to the network and users. For example, DPI used for troubleshooting or proactive security measures (such as spam or malware detection) provides a clear benefit to users and may warrant detailed but carefully-implemented inspection for the sake of obtaining this benefit. On

[35] *See* Addendum to Testimony of Leslie Harris, *supra* note 4.

[36] *See generally* Statement of Leslie Harris, President and Chief Executive Officer of the Center for Democracy and Technology, Before the House Committee on Energy and Commerce, Subcommittee on Communications, Technology and the Internet, "The Privacy Implications of Deep Packet Inspection" (April 23, 2009) *available at* http://www.cdt.org/privacy/20090423_dpi_testimony.pdf.

the other hand, the use of DPI for behavioral advertising or content filtering should trigger much higher scrutiny and more protective measures.[37]

- *What (if any) special issues does the collection or the use of information about teens raise?*

CDT is extremely skeptical that enhanced consent procedures for teens, regardless of their form or implementation,[38] could ever be effectively implemented because it is essentially impossible to determine the age of an Internet user. Moreover, a requirement for a website or online service to categorize it users based on age and to employ different consent procedures or treat minors' data differently from that of adults will lead to significant privacy and constitutional issues. Finally, such measures are unlikely to be effective in protecting teens' privacy or promoting more meaningful consent.

It is well established that online age verification is impossible to perform with any degree of certainty.[39] When a user's browser sends a request to a website or online service, the information it sends relates to characteristics of the user's browser and computer — no information about the user's age or date of birth is transmitted. Websites and online services could try to obtain age information by affirmatively asking for it or for some sort of proxy (such as a credit card number), but even when sites implement some form of age verification procedure, they cannot guarantee that the information provided by users allows them to accurately sort users into "adult" or "minor" categories.

In response to this uncertainty, many operators would likely simply bar teens from accessing their sites and services, mirroring the general industry response to COPPA of prohibiting access to children under 13. This will significantly reduce the online content — content that is fully legal and constitutionally protected for them — that is available to teens, in violation of their First Amendment rights.[40]

---

[37] Such uses may be difficult or impossible to implement in a privacy-protective way under certain circumstances.

[38] It is unclear what the Commission refers to when it raises the possibility of "enhanced consent procedures" for teens. Elsewhere, the Commission discusses affirmative express consent (or "opt-in" consent) as a form of enhanced consent; other commenters will likely recommend some form of verified parental consent for younger teens, similar to the requirements of the Children's Online Privacy Protection Act (COPPA) for minors age 12 and under. CDT has discussed in depth the legal and technical problems raised by suggestions to expand the COPPA Rule to cover some subset of teens in our comments in the Commission's COPPA Rule Review proceeding. *See generally* Supplemental Comments of the Center for Democracy & Technology, Before the Federal Trade Commission, In the Matter of Implementation of the Children Online Privacy Protection Rule (July 12, 2010) *available at* http://www.cdt.org/files/pdfs/CDT_Supplemental_Comments.pdf; Comments of the Center for Democracy & Technology, the Progress & Freedom Foundation, and the Electronic Frontier Foundation, Before the Federal Trade Commission, In the Matter of Implementation of the Children's Online Privacy Protection Rule (June 30, 2010) *available at* http://cdt.org/files/pdfs/CDT-PFF-EFF_Joint_Comments.pdf.

[39] Courts have concluded that age verification services do not "actually reliably establish or verify the age of Internet users. Nor is there evidence of such services or products that can effectively prevent access to Web pages by a minor." *ACLU v. Gonzales*, 478 F. Supp. 2d 775, 800 (E.D. Pa. 2007), *aff'd*, ACLU v. Mukasey, 534 F.3d 181 (3d Cir. 2008); *see also Mukasey*, 534 F.3d at 196. Credit cards, debit accounts, adult access codes, and adult personal identification numbers do not in fact verify age." *Gonzales*, 478 F. Supp. 2d at 811.

[40] Older minors have a right to receive information just as adults do. *See, e.g., In re* Gault, 387 U.S. 1, 13 (1967) ("Neither the Fourteenth Amendment nor the Bill of Rights is for adults alone."); Erznoznik v. City of Jacksonville, 422 U.S. 205, 214 ("In most circumstances, the values protected by the First Amendment are no less applicable when government seeks to control the flow of information to minors."). Minors' right to access information has been recognized as a necessary component of their intellectual development, vital to

Further, requiring users of all ages to disclose personal information in order to access material online would be an impermissible burden on free speech. Users will be deterred from accessing sensitive or controversial — but constitutionally protected — material if they must provide personal information to do so;[41] this requirement would also burden users' right to speak and access information anonymously.[42] Website operators' free speech right to communicate constitutionally protected material to their audiences would also be burdened if operators were required to implement costly age verification systems (that, again, would not be effective).[43] Sites would likely have to charge fees for content they otherwise would have provided for free and would lose users who are reluctant to provide personal information or pay for content that they might obtain freely elsewhere.[44]

As the Commission has noted, individual sites and social networking services may choose to offer an extra level of protection to users who self-identify as teens. This type of decision falls well within the bounds of sites' ability to set their own terms of service (though sites should still be required to provide a minimum level of protection for, access to, and notice about what data is being collected or shared). But if this type of differential treatment of user data is compelled by a legal mandate, rather than a voluntary action, that mandate will face difficult constitutional challenges.

- *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?*

CDT does not believe that it is possible for non-consumer facing third parties to meaningfully offer "choice" to consumers. Instead, it falls upon the companies that originally obtained the relevant data from consumers to meet the Transparency and Purpose Specification FIPs when they collect the data in the first place. As discussed, *infra*, pp. 26-27, under a comprehensive privacy protection framework, first parties should disclose to consumers the identity of all third parties to which they transmit user data. In order to fulfill the Individual Participation Fair Information Practice Principle, data brokers should offer access to consumers to profiles and correction; only if data brokers refuse to offer access and correction is deletion at will appropriate. Moreover, data

---

their ability to fully exercise the rights of speech, press, and political freedom as adults. *See* Bd. Of Educ. V. Pico, 457 U.S. 853, 867 (1982) ("The right to receive ideas is a necessary predicate to the recipient's meaningful exercise of his own rights of speech, press, and political freedom."). Minors' access to constitutionally protected material can only be restricted "in relatively narrow and well-defined circumstances." *Erznoznik*, 422 U.S. at 212-213.

[41] *ACLU v. Ashcroft*, 322 F.3d 240, 259 (3d. Cir. 2003), ***aff'd*** 542 U.S. 656 (2004).

[42] *See, e.g.*, ACLU v. Mukasey, 534 F. 3d 181, 197 (3d Cir. 2008) (discussing the difference between online and offline methods of restricting minors' access to material that is constitutionally protected as to adults: "Blinder racks do not require adults to pay for speech that otherwise would be accessible for free, they do not require adults to relinquish their anonymity to access protected speech, and they do not create a potentially permanent electronic record. Blinder racks simply do not involve the privacy and security concerns that" age verification procedures raise.).

[43] *Mukasey*, 534 F.3d at 197.

[44] *Gonzales*, 478 F. Supp. 2d at 804-806, 812-13; for a full discussion, see CDT Supplemental Comments pg. 4-5.

brokers should be required to abide by the other Fair Information Practice Principles, including data quality, data minimization, and security.

Special choice for online behavioral advertising: Do Not Track

- *How should a universal choice mechanism be designed for consumers to control online behavioral advertising?*

CDT has long supported the development of "Do Not Track" mechanisms for consumers to make a universal, persistent choice not to be tracked as they surf the web.[45] If third-party tracking is permitted on an opt-out, as opposed to opt-in basis, there must be a mechanism for consumers to exercise their choice across all third-parties. Otherwise consumers are faced with the unreasonable task of tracking down each and every third-party tracker and opting out of each one. With some websites hosting as many as 234 separate third-party trackers, this task quickly becomes impossible.[46] And tracking controls should be persistent, meaning that a consumer's choices should not be wiped out each time she engages in normal behavior such as clearing her computer of cookies (a practice that currently deletes many opt-out cookies).

For the moment, CDT is not endorsing a particular "Do Not Track" mechanism, as different browsers have recently released different tools designed to accomplish the fundamental goals of "Do Not Track."[47] Microsoft's "Tracking Protection Lists" has the advantage of completely blocking disclosure of data to third-party tracking domains, but it relies on others to generate and maintain lists of tracking domains. Mozilla's "Do Not Track" header is simple and universal, but relies on tracking companies to recognize and adhere to the header's instructions. Google Chrome's "Keep My Opt Outs" provides a persistent means to opt out of more than 50 ad networks' behavioral advertising, but does nothing for other companies' tracking (or for those networks' collection of tracking data). There are advantages and disadvantages to all these approaches, and they may be complementary.

A key question with any "Do Not Track" approach is to define "tracking." Consumers and third parties alike need a clear definition of what the choice covers. Without a clear definition of the scope of "Do Not Track" across all platforms, it will be challenging for companies to align their business models with consumer expectations and potentially legal requirements.

---

[45] *See* Alissa Cooper, *Do Not Track. No, Seriously.*, CDT Blog, November 8, 2007, http://cdt.org/blogs/alissa-cooper/do-not-track-no-seriously.

[46] What They Know, Introduction Page, THE WALL STREET JOURNAL, http://blogs.wsj.com/wtk/ (last visited Feb. 17, 2011).

[47] *See* Aaron Brauer-Rieke, *"Do Not Track" In Your Browser? Microsoft Introduces New Tracking Protection*, CDT Blog, December 8, 2010, http://cdt.org/blogs/aaron-brauer-rieke/do-not-track-your-browser-microsoft-introduces-new-tracking-protection; Aaron Brauer-Rieke, *"Do Not Track" Gains Momentum as Mozilla Announces New Tracking Tool*, CDT Blog, January 24, 2011, http://cdt.org/blogs/aaron-brauer-rieke/"do-not-track"-gains-momentum-mozilla-announces-new-tracking-tool.

To answer this question and support ”Do Not Track” efforts, CDT recently released a draft paper proposing a definition of “Do Not Track” in the context of web browsing.[48] We have provisionally defined “tracking” as:

> **Tracking is the collection and correlation of data about the Internet activities of a particular user, computer, or device, over time and across non-commonly branded websites, for any purpose other than fraud prevention or compliance with law enforcement requests.**

Based on this definition, we define certain activities as tracking, such as third-party behavioral advertising, but exclude some others, such as certain third-party ad delivery and reporting, identity authentication, and analytics. CDT does not believe that “Do Not Track” can be applied so bluntly as to prohibit all collection of consumer data by third parties; such an approach would hinder legitimate, non-tracking activities such as fraud prevention and third-party contextual ad delivery and analytics services that do not merge data across domains. Though a prohibition on *collection* of data would be simpler and easier to police, we believe that, in at least some scenarios, “Do Not Track” mechanisms would also be effective if they only prevented the tracking *use* of data by third-parties. However, parties that collect uniquely identifiable data for non-“tracking” purposes should be required to make an affirmative accountable statement in a privacy policy or elsewhere expressly disclaiming use of such data for tracking.[49]

CDT will be convening stakeholders over the coming weeks to refine this scoping document. We hope that the FTC will welcome and encourage our effort to develop a common understanding of “Do Not Track.” To that end, we are attaching our draft document as an appendix to this filing.

CDT stresses that widespread industry support is crucial to the success of any self-regulatory approach to “Do Not Track.” Unless domains delivering third party content make it clear whether they are or are not tracking, the compilers of “Tracking Protection Lists” may feel compelled to list and block all domains delivering third-party content without assurances that those domains are not tracking, resulting in a poor web experience on sites that heavily incorporate third-party content. On the other hand, if trackers do not set up their infrastructure to respect Mozilla’s “Do Not Track” headers, consumers may be lulled into a false sense that their preferences are being honored. Similarly, without full industry participation, Google Chrome’s “Keep My Opt Outs” approach will always be an incomplete solution. Thus, “Do Not Track” is a crucial test for industry claims that self-regulation can work. It is worth noting that, at least as far as CDT is aware, no ad networks have yet stated that they will set up non-tracking domains to serve ads for browsers that use Microsoft’s “Tracking Protection Lists” or honor Mozilla’s “Do Not Track” header. As such, it may be necessary for the FTC to interpret Section 5 to require adherence to “Do Not Track” requests or for Congress to adopt legislation to compel compliance.

---

[48] Press Release, Center for Democracy & Technology, CDT Releases Draft Definition of 'Do Not Track', January 231, 2011 *available at* http://cdt.org/pr_statement/cdt-releases-draft-definition-do-not-track.

[49] Such an approach requiring an affirmative has also been advocated by Privacy Choice, who is one of four entities to have released a “Tracking Protection List” for Microsoft’s approach “Do Not Track.” *See* Jim Brock, *IE9 tracking protection: Two suggestions*, PrivacyChoice Blog , February 17, 2011, http://blog.privacychoice.org/2011/02/17/ie9-tracking-protection-two-suggestions/.

- *How can such a mechanism be offered to consumers and publicized?*
- *How can such a mechanism be designed to be clear, easy-to-find, usable, and understandable to consumers?*

Any browser "Do Not Track" setting should be prominently located in the privacy settings such that an ordinary consumer could easy find and operate the setting. The setting should provide a concise description to consumers of the setting and provide a link to a more detailed (though still readily comprehensible) explanation. Upon installation of the browser (or upon a consumer's first engaging with a pre-installed browser), the consumer should be taken to a "privacy settings" page (as part of the initial set-up wizard) that prominently offers to consumers the option to set their preferences to "Do Not Track." Browsers makers that wish to compete on privacy and give consumers strong privacy defaults may consider "Do Not Track" as a default setting or may present a "forced choice" that requires consumers to choose between "Do Not Track" or "Allow Behavioral Advertising" (or similar language) as part of the initial set-up.

- *What are the potential costs and benefits of offering a standardized uniform choice mechanism to control online behavioral advertising?*

Not only do the potential benefits of offering a standardized uniform choice mechanism to control online behavioral tracking well outweigh the costs, considering among other factors clarity and certainty, but a standardized uniform choice mechanism (or a set of complementary mechanisms for expressing universal and persistent choice) is the *only* way to effectively give consumers the ability to control online behavioral tracking. As noted above, in an "opt-out" environment, consumers cannot possibly be expected to navigate the third-party tracking ecosystem and affirmatively opt out of tracking from each and every ad network or domain. Even companies whose entire business model is predicated on finding tracking domains do an incomplete job of identifying all trackers at any given point in time.[50] Of the four entities that have published "tracking protection lists" to allow consumers to take advantage of Microsoft's "Do Not Track" approach, one list contained 94 separate tracking domains, one contained 463, and one listed 2,189 separate tracking domains.[51] Whereas consumers may previously have had the global option to deleting all HTTP cookies on a regular basis, as a proxy for "Do Not Track," ad networks are increasingly using others means to track consumers, including flash local storage,[52] static IP addresses,[53] and browser fingerprints.[54] Even if browsers were to

[50] Jim Brock, *Are privacy add-ons effective? Surprising results from our testing*, PrivacyChoice Blog, November 17, 2011, http://blog.privacychoice.org/2010/11/17/are-privacy-add-ons-effective-surprising-results-from-our-testing/.

[51] Ed Bott, *Privacy protection and IE9: who can you trust?*, Ed Bott's Microsoft Report, February 14, 2011, *available at* http://www.zdnet.com/blog/bott/privacy-protection-and-ie9-who-can-you-trust/3014. The fourth list created by TrustE does not block any domains; instead if affirmatively white lists nearly 4000 domains as "not tracking." TrustE has said that it will add domains to its blocking list that it demonstrates are not in compliance with the Digital Advertising Alliance's self-regulatory program after 30 days' notice.

[52] Ashkan Soltani, et. al., *Flash Cookies and Privacy* (Aug. 10, 2009) *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1446862.

[53] Wendy Davis, ClearSight Launches Targeting Platform Tying IP Addresses To Offline Data, ONLINE MEDIA DAILY, June 28, 2010, http://www.mediapost.com/publications/?fa=Articles.showArticle&art_aid=131044.

[54] *See* Panopticlick, Electronic Frontier Foundation, http://panopticlick.eff.org/ (last visited Feb. 18, 2011).

develop new and separate controls for each of these tracking mechanisms (they haven't), consumers cannot reasonably be expected to learn about and take advantage of each new privacy setting.[55] Moreover, many ad networks (that most consumers have never heard of) do not currently offer any means to consumers to opt out of their tracking. In short, there is no other tracking control mechanism under consideration today that offers benefits as clear as the "Do Not Track." implementations being developed by the major browser makers.

- *How many consumers would likely choose to avoid receiving targeted advertising?*
- *What is the likely impact if large numbers of consumers elect to opt out? How would it affect online publishers and advertisers, and how would it affect consumers?*

"Do Not Track" does not mean "do not deliver advertisements." Even if large numbers of consumers affirmatively chose to set their browsers to "Do Not Track," ad networks would still deliver ads to those consumers, and the effect on the overall online advertising market and the online services supported by advertising would be minor. For most of the history of online advertising, advertising based on behavioral tracking only constituted a mere sliver of overall revenue.[56] Even today, researchers have estimated that behavioral advertising accounts for only 4% of the overall ad market.[57] Context-based advertising remains the dominant model and would continue to be such under "Do Not Track." Moreover, most formulations of "Do Not Track," including CDT's draft definition, do not prohibit first party tracking, so ads could be still be targeted based on a consumer's usage of one particular site.[58] Also, "Do Not Track" would not prohibit third-party behavioral tracking — it would only switch the default from "opt-out" to "opt-in." Marketers could still make value propositions to consumers to request that they allow tracking in exchange for improved content or lower prices. In terms of potential impact on advertising and the services it supports, the advertising industry should be more concerned that by denying consumers tools to disassociate advertising from detailed behavioral profiles, they may drive consumers to adopt more blunt tools that block advertising altogether.

The goal of "Do Not Track" should be to allow consumers to make decisions about whether to be tracked more easily than they can today. If consumers would rather pay for online services with money instead of with their privacy, policymakers should respect

[55] In December of last year, CDT released a report evaluating the privacy controls of each of the five major web browsers: Chrome, Firefox, Internet Explorer, Opera, and Safari. Center for Democracy & Technology, *CDT Browser Report 2010 - Browser Privacy Features: A Work in Progress*, December 7, 2010, http://www.cdt.org/browserreport2010. The report showed that each of the browsers had introduced new privacy controls, but that the range and diversity of controls needed to truly protect one's privacy was too complicated for most users. We concluded that consumers needed simple, universal controls such as "Do Not Track" in order to meaningfully lock down their privacy.

[56] Jonathan Mayer, *Do Not Track Is No Threat to Ad-Supported Businesses*, The Center for Internet and Society Blog, January 20, 2011, http://cyberlaw.stanford.edu/node/6592.

[57] David Hallerman, *Is Behavioral Targeting Outmoded?*, The eMarketer Blog, March 12, 2010, http://www.emarketer.com/blog/index.php/behavorial-targeting-outmoded/.

[58] CDT believes, however, that consumers should be permitted to opt out of first-party tracking and targeting on at least a site-by-site or company-by-company basis. *See supra*, pp. 9-11.

that decision and let consumers and business place values on services and privacy in a newly transparent marketplace. Concerns about consumers taking advantage of "Do Not Track" tools should not lead to paternalistic decisions to deny consumers control of their information by making the decision for them that they must endure surreptitious tracking in order to receive web content.

- *In addition to providing the option to opt out of receiving ads completely, should a universal choice mechanism for online behavioral advertising include an option that allows consumers more granular control over the types of advertising they want to receive and the type of data they are willing to have collected about them?*

CDT strongly supports the development of granular controls and permissions that would allow consumers to make detailed and precise decisions about how they are marketed to online, and we believe "Do Not Track" is flexible enough to allow the development of such controls. "Do Not Track" does not have to operate as a blanket prohibition on all tracking. Instead, "Do Not Track" should be envisioned as effectively switching the default for tracking from "opt-out" to "opt-in" — companies should still be free to solicit consumers' consent to tracking in exchange for consideration.[59] Thus, while "Do Not Track" should be seen by marketers as an default instruction not to track consumers, there should be nothing to prevent those marketers from then making their pitch to consumers as to why they should consent to be tracked by that particular company. For example, under the Microsoft "Tracking Protection List" approach, a company could request to be added to a "white list" to allow tracking from a particular domain. Under the Mozilla "Do Not Track" header approach, a company could solicit a consumer's affirmative permission to ignore a "Do Not Track" instruction. Some websites already tell consumers that they cannot access the site if they have "Ad Block" or other another ad-blocking extension installed in a browser. The market can develop value propositions to offer to consumers to allow tracking, such as lower prices or expanded content. However, the Federal Trade Commission should be clear that requests for permission to track should be made clearly and prominently to consumers and not buried in opaque terms of service agreements where consumers are unlikely to notice the requests.[60] This would effectively nullify the purpose of "Do Not Track," reinstating today's status quo. However, as noted earlier, it may be appropriate to provide for an exception to tracking for essential services for which there is no meaningful marketplace or competition. *See supra*, p. 13.

- *Should the concept of a universal choice mechanism be extended beyond online behavioral advertising and include, for example, behavioral advertising for mobile applications?*

Yes. In a privacy framework based primarily on "opt-out" permissions for information sharing, the Federal Trade Commission should push for the development of "Do Not

[59] *See supra* note 48.

[60] *See* Complaint, In the Matter of Sears Holdings Management Corporation, No. C-4264 (Aug. 31, 2009), *available at* http://www.ftc.gov/os/caselist/0823099/090604searscmpt.pdf.

Track" and comparable global choice mechanisms in areas beyond web-based behavioral tracking.

Mobile platforms might be the next logical step. Certainly, there can be no compelling argument that a person who visits the New York Times through a mobile browser should have less privacy protections than a person who interacts with the New York Times through a mobile app. Currently, mobile users have significantly fewer privacy controls for mobile applications than they do for traditional web browsing, even when accessing the same kinds of content. Mobile platforms typically allow developers to pass along permanent unique identifiers to third-party tracking networks with no transparency to the user and no choice about whether to share that information.[61] Most mobile ad networks do not allow consumers to access their profiles and do not give consumers the ability to opt out of tracking.[62] Furthermore, considerably more extensive and more sensitive information may be at stake when consumers interact through mobile apps. On the web, information shared with a site (and its third-party tracking partners) is typically limited to the particular URLs that a consumer passively browses. Consumers may be asked for more personal information, but typically they have to manually enter the information themselves and so have a keen awareness of what they are sharing. In contrast, in the mobile context, applications at the time of installment may ask for blanket permissions to access broad categories of sensitive information, such as real-time location, contacts, and access to a device's hard drive. Consumers are often not fully informed to what end such permissions are being sought, and they do not always later receive "just in time" notice when that information is accessed or transferred by the application.

The FTC final report should encourage mobile platform makers such as Apple, Google, Microsoft, and Intel to develop operating system level "Do Not Track" options to allow consumers to make global and persistent choices not to be tracked when they use a mobile device. As with web browsers, this should simply switch the defaults from opt-out to opt-in for tracking, and developers and marketers should be free to make value propositions to consumers to obtain consent for tracking (just as many developers today offer free versions of apps that are supported by more extensive advertising than paid versions).

- *If the private sector does not implement an effective uniform choice mechanism voluntarily, should the FTC recommend legislation requiring such a mechanism?*

CDT is hopeful that industry initiatives can develop that offer effective and universal "Do Not Track" options for consumers. However, as noted above, no ad networks have currently stated their intention to adhere to and design their systems to support "Do Not Track" technologies. The FTC should actively encourage industry to develop workable solutions within a reasonable time frame.

The FTC should also consider making a declarative statement that failing to adhere to "Do Not Track" instructions without receiving a consumer's clear, affirmative permission

[61] *See, e.g.,* Jennifer Valentino-DeVries, *Unique Phone ID Numbers Explained*, Digits Blog, December 19, 2010, http://blogs.wsj.com/digits/2010/12/19/unique-phone-id-numbers-explained/.

[62] *See* Jennifer Valentino-DeVries, *What Can You Do? Not Much*, THE WALL STREET JOURNAL, December 18, 2010, http://online.wsj.com/article/SB10001424052748703929404576022140902538236.html.

to track would constitute a deceptive or unfair business practice under the FTC's existing Section 5 authority. Section 5 was designed to be flexible and to apply to a wide range of business practices. The FTC has applied Section 5 aggressively in the security context to require companies to implement reasonable technological safeguards for consumer data.[63] The FTC should consider issuing a statement as it did regarding astroturfing in its Endorsement Guidelines to declare that the Commission would deem certain activities to be unfair and deceptive.[64] Even absent such a statement, we believe it may be appropriate for the FTC to bring targeted enforcement actions against companies that clearly evade consumer's "Do Not Track" choices.

CDT has reservations about dedicated "Do Not Track" legislation for two reasons. First, we would oppose any legislation that prescribes particular technologies to address privacy issues; such mandates, locked into law, may make sense when written, but may fail to address how data is shared in the future and may even freeze technological innovation. More importantly, we firmly believe that baseline privacy legislation that addresses *all* privacy issues is of paramount importance, and a "Do Not Track" bill should not be used as a proxy or replacement for an omnibus bill. There are very important privacy issues associated with cloud computing, social networking, and off-line data sharing that would not be addressed by "Do Not Track." We encourage the FTC to endorse a baseline law that addresses the full range of privacy concerns, both online and off.

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?*

CDT believes standardizing notice formats is an important area for innovation. However, we note that past voluntary efforts in this regard have largely been unsuccessful. Furthermore, it is important to ensure that complicated and diverse data practices are not so oversimplified in standardization as to reduce transparency and consumer choice. In particular, the Purpose Specification FIP should be implemented with detailed descriptions so that consumers have easy access to that information.

So far, voluntary self-regulatory efforts by industry have not resulted in improved transparency for consumers.[65] Voluntary efforts to standardize privacy policies in a

[63] *See, e.g.,* Agreement Containing Settlement Order, *In the Matter of BJ's Wholesale Club, Inc.*, No. 042 3160 (F.T.C. 2005) available at http://www.ftc.gov/os/caselist/0423160/092305comp0423160.pdf; Agreement Containing Consent Order, *In the Matter of DSW, Inc.* No. 052 3096 (F.T.C. 2005), available at http://www.ftc.gov/os/caselist/0523096/051201agree0523096.pdf.

[64] Guides Concerning Use of Endorsements and Testimonials in Advertising, 16 C.F.R. § 255.0 (2009) available at http://www.ftc.gov/os/2009/10/091005revisedendorsementguides.pdf; Press Release, Federal Trade Commission, Public Relations Firm to Settle FTC Charges that It Advertised Clients' Gaming Apps Through Misleading Online Endorsements (Aug. 26, 2010) available at http://www.ftc.gov/opa/2010/08/reverb.shtm.

[65] *See generally, e.g.,* CyLab Usable Privacy and Security (CUPS) Laboratory Website, http://cups.cs.cmu.edu/ (last visited Jan. 27, 2010).

machine-readable format have failed.[66] Industry coalition efforts dating back to the Online Privacy Alliance have yet to generate consensus for and develop consistent and understandable disclosures about consumer data collection and usage.[67]

More recently, the Digital Advertising Alliance has announced promising plans to introduce common iconography into online ads and to make available information about the sources of information behind those ads.[68] Even though it is limited only to online behavioral advertising, this self-regulatory effort has still not been publicly deployed on any wide scale after years of development, and not all the details about what information will be made available to consumers are known. CDT is unaware of any comparable self-regulatory effort to improve transparency in any other industry.

This history suggests it is not feasible to standardize data practices across industries without regulatory support. The issue of transparency, like others related to privacy, can be effectively dealt with only by a combination of baseline legislated requirements, coregulatory industry standards, and FTC backstop enforcement and rulemaking.

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

What constitutes meaningful transparency obviously differs considerably from context to context. Even if the FTC were to devise standards today for online and mobile behavioral advertising, those standards would not readily apply to emerging industries with their own catalog of privacy issues, such as the digital signage industry. Similarly, there is no one model that could consistently apply to all offline data transactions. For this reason, CDT has supported a coregulatory model that encourages specific industry sectors, with consultation from regulators and civil society, to devise and propose industry appropriate safe harbor compliance programs for FTC approval and enforcement. *See, e.g., supra*, p. 6

Secondly, *all* companies should be required to comply with the Purpose Specification FIP and publish detailed and comprehensive privacy policies apart from just-in-time notices that meaningfully describe what the company is actually doing with consumer data and with whom and for what purpose that data is being shared. Although such privacy policies are unlikely to be read by the average consumer, they still will serve a valuable function in educating consumer advocates, regulators, and the press about the details of those companies' data usage.[69]

---

[66] *See* Ari Schwartz, *Looking Back at P3P: Lessons for the Future* (Nov. 2009), *available at* http://www.cdt.org/files/pdfs/P3P_Retro_Final_0.pdf.

[67] *See* Dennis D. Hirsch, *The Law and Policy of Online Privacy: Regulation, Self-Regulation, or Co-Regulation?*, 34 SEATTLE U. L. REV. 439 (2011).

[68] *See* The Self-Regulatory Program for Behavioral Advertising Website, http:www/aboutads.info/ (last visited Jan. 27, 2010).

[69] *See* David Sarno, *Apple collecting, sharing iPhone users' precise locations*, LOS ANGELES TIMES (June 21, 2010) available at http://latimesblogs.latimes.com/technology/2010/06/apple-location-privacy-iphone-ipad.html.

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

As discussed *supra* pp. 23-24, CDT believes machine-readable policies have promise, but we are skeptical that they will be successful without regulatory support.

Reasonable access to consumer data

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

CDT believes that companies should be able to charge a reasonable cost for certain types of access, provided the costs are commensurate with the real and fair cost incurred in providing the access. Cost might arise in providing access mechanisms for distributed, non-consumer facing entities. However, many online services should be able to provide access at no cost.

- *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?*

CDT believes that it is reasonable to require that companies inform consumers of the identity of those with whom it has shared data about the consumer. Similarly, companies should also inform consumers about the sources of any data collected about them from a third party.

The question raises broader concerns about data stewardship. For many companies, being able to tell consumers where data about them is coming from and where it is going would require those companies to exercise much better control over their own data sources and flows — control that should be in the best interests of the companies themselves, who really should know where data about their customers is coming from and where it is going. At the moment, however, the current privacy framework does not provide adequate incentives to companies to monitor their use and transfers of consumer data. Last year, for example, a Wall Street Journal story detailed how several mainstream websites included a surprising number of third-party invisible "web bugs" on their sites that allowed a wide range of targeting companies to place unique tracking cookies on users' computers. Congressmen Ed Markey and Joe Barton issued letters to many of these companies asking, *inter alia*, whether the companies knew to which third parties they were transferring consumer information. Many answered "no."[70] It is impossible to fully empower consumers to make meaningful choices about the uses of their data if the companies themselves do not understand their own data practices. The concept that consumers benefit from the collection and use of data about them and will choose or allow certain data practices in exchange for valuable services is meaningless if companies cannot tell consumers where their data is coming from and where it is

[70] Press Release, Office of Congressman Ed Markey, Markey, Barton Release Responses From Web Sites on Their Tracking of Consumer Behavior, October 8, 2010 *available at* http://markey.house.gov/index.php?option=content&task=view&id=4103&Itemid=125.

going.

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

While teen should have access to data that a company maintains about them, websites and online services should not be required to provide parents[71] with access to the same data. Teens have a First Amendment right to speak and to access information without prior parental consent or parental review.[72] Courts have held that requiring a parent's consent or supervision of a minor when that minor is exercising his First Amendment rights is "a curtailment of those rights."[73] The importance of teens' independent access to information is highlighted in the area of medical care, where older minors have a clear right to obtain treatment without their parents' permission or even knowledge.[74] Just as users would be discouraged from accessing sensitive or controversial speech if they must provide personal information to do so, teens' access to relevant, constitutionally protected information would be chilled if they faced the prospect of parental monitoring and review of data about their Internet activity.

None of this prevents parents from talking to their teenage children and looking at this data together. It may be entirely appropriate for the parent of a 13-year-old to ask the child for the username and password to his social network profile, in order to review both the information the network collects about the child and the content the child has posted himself. But this is a decision best made by families for themselves. Mandatory parental access to data about teens' Internet use would be an unconstitutional burden on teens' speech.

[71] As a purely practical matter, the problems of inaccuracy that plague age and identity verification online would only be amplified if sites were also asked to establish familial relationships among users; allowing certain users of a website or online service access to other users' data creates room for significant safety and privacy harms. Determining which adult users of a site were truly the parent or legal guardian of a teen user, and therefore entitled to access the teen's data, would be a complex and likely very expensive undertaking.

[72] Tinker v. Des Moines Independent Community School District, 393 U.S. 503, 511 (1969) ("Students in school, as well as out of school, are 'persons' under our Constitution. They are possessed of fundamental rights which the State must respect.")

[73] Am. Amusement Mach. Ass'n v. Kendrick, 244 F.3d 572, 579 (7th Cir. 2001).

[74] Minors' rights to access information pertinent to their sexual and reproductive health have been well established in the "mature minors" line of cases, which hold that mature minors have the right to obtain abortions without parental consent under certain circumstances. *See* Bellotti v. Baird, 443 U.S. 622, 640-643 (1979) (plurality opinion); Planned Parenthood v. Casey, 505 U.S. 833, 899 (1992); Lambert v. Wicklund, 520 U.S. 292 (1997). In these cases, the defining characteristic of a mature minor is her ability to make critical decisions in an informed manner. *See* Bellotti at 634. Minors also have a recognized right to receive information about contraception. *See* Bolger v. Youngs Drug Prods. Corp. 463 U.S. 60, 75 n.30 (1983).

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

No. Precisely because non-consumer facing entities cannot directly provide consumers with choice about collection and usage, those companies should have at least as strong an obligation to provide access mechanisms as their consumer-facing counterparts.

- *For non-consumer-facing companies, how can consumers best discover which entities possess information about them and how to seek access to their data?*

As discussed *supra*, p. 16, non-consumer facing entities should be discoverable through the entities that have provided them with data. A centralized, standardized access mechanism is likely to be undesirable due to significant security concerns (e.g., one set of credentials would provide access to a large swath of consumer data). Links provided by first-party entities disclosing with whom they share consumer information may be the most efficient method to inform consumers about non-consumer facing companies.

- *Should consumers receive notice when data about them has been used to deny them benefits? How should such notice be provided? What are the costs and benefits of providing such notice?*

CDT believes that the Fair Credit Reporting Act already requires that companies must give notice in the event of adverse actions, and we encourage the Commission to continue to bring targeted enforcement actions against companies that fail to adhere to that law's provisions. However, the law should not be interpreted as applying to a number of everyday, commonly accepted online practices that arguably involve "denying benefits" based on data. For example, a first-party online retailer might offer certain promotions or coupons to certain customers based on purchase history or demographic information provided by the consumer. Here, it is unlikely anyone would expect to receive a notice whenever they were not included in a particular promotion. Furthermore, it would probably be cumbersome to the retailer and annoying to the consumer to require notice. Here, well-implemented transparency and purpose specifications are likely sufficient.

However, where an entity leverages third-party data sources to deny a consumer a benefit such that a consumer might be surprised or unaware such data could be considered, there is a clearer need for notice. For example, most consumers would not expect that data aggregated by an ad network or social network would be leveraged to make eligibility or other important decisions about them in other contexts. Here, a notice requirement makes sense.

Unfortunately, while existing law provides for relatively robust protections for records that are deemed to be subject to FCRA, some data brokers in recent years have increasingly interpreted the scope of their databases as outside of FCRA's protections. CDT believes that this narrow reading of the FCRA is incorrect, and we have urged the FTC to give a broader interpretation to the Act.[75] An ideal privacy protection framework would utilize a

[75] Center for Democracy & Technology, *Protecting Privacy in Online Identity: A Closer Look at the Fair Credit Reporting Act*, March 1, 2010, http://cdt.org/blogs/jonathan-dunn/protecting-privacy-online-identity-closer-look-fair-credit-reporting-act.

more nuanced sliding scale of notification requirements based on a number of factors, including consumer expectations, relative importance of the "benefit" at issue, and likelihood for errors in the underlying database. In the meantime, we recommend that the FTC continue to bring targeted FCRA enforcement cases to reestablish the parameters of the law's applications.[76]

Material Changes

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

CDT supports the approach put forward in the BEST PRACTICES bill which would require companies to post new privacy policies that include material changes regarding the collection, use, or disclosure of personal information at least 30 days in advance before collecting information pursuant to the new policy.[77] Although the average consumer would perhaps not read the new policy in any detail, the advance notice would allow advocates and the media to review, assess, and publicize the changes to those policies, which would allow users to make informed decisions about whether to continue using those companies' services.[78]

[76] Sean Brooks, *CDT Files FTC Complaint Against Spokeo*, Inc., June 30, 2010, http://www.cdt.org/blogs/sean-brooks/cdt-files-ftc-complaint-against-spokeo-inc.

[77] *See* BEST PRACTICES Act, *supra* note 18.

[78] *See Apple collecting, sharing iPhone users' precise locations*, *supra* note 69.