Comments from the Consumer Federation of America on the Preliminary FTC Staff Report "Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers"

February 18, 2011

The Consumer Federation of America (CFA), an association of some 300 nonprofit consumer organizations that that was established in 1968 to advance the consumer interest through research, advocacy, and education, is pleased to provide comments on the proposed privacy framework (herein referred to as the FTC staff report) recently issued by the Federal Trade Commission (FTC).[1] CFA applauds the FTC for its leadership in privacy issues and for including the perspectives of consumer and privacy organizations in the roundtables and other events that it has held to gather input about how to address the challenging privacy issues that confront consumers and businesses in the United States. While we do not agree with the proposition that consumers need not be entitled to choice for first-party marketing, we generally support the privacy framework described in the FTC staff report.

We are especially pleased that the FTC staff report calls for a universal "Do Not Track" mechanism for consumers who do not want their online activities to be tracked, an idea that CFA and other organizations first suggested in 2007. It is important to state at the onset, however, that an effective privacy framework, including a universal "Do Not Track" mechanism, cannot be achieved by voluntary industry measures alone. CFA urges the FTC to call for legislation in order to establish clear lines of conduct for industry and provide consumers with enforceable privacy rights.

Scope

Who should be covered in a privacy framework?

We agree that all commercial entities that collect or use consumer data that can be reasonably linked to a specific consumer, computer or other device should be covered by a privacy framework. While there are good reasons why there are special obligations on certain entities under current law, such as those that handle our medical information or communications, because of the sensitivity of that information,

[1] Preliminary FTC Staff Report, *Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers,* December 2010, www.ftc.gov/os/2010/12/101201privacyreport.pdf.

the lack of an overall privacy framework for businesses has resulted in a situation in which consumers' video rental records are better protected than the information about what they buy or read online.

We are hesitant to suggest that certain types or sizes of businesses or quantities of data should be excluded from baseline requirements for consumer privacy protection. Even small businesses or those that do not use consumer data themselves may share or sell it with others such as advertising networks or data brokers. Furthermore, the use of sensitive data, even in small quantities or by small companies, can raise significant concerns. Moreover, new methods for collecting consumer data [2] and new data uses are constantly emerging.

As the FTC staff report states, "consumers are generally unaware of the number of online and offline entities that collect their data, the breadth of the data collected, and the extent to which data is shared with third parties that are often entirely unknown to consumers."[3] Even when consumers are aware of the collection or use of their data, their options for control are limited by our current fragmented, and in some cases weak legal protections,[4] and by company policies that are often incomprehensible and one-sided.

An effective privacy framework must be sufficiently broad to avoid gaps that could leave consumers without meaningful privacy protection. Exceptions, if any, should be very narrowly tailored. It might be appropriate, for instance, to exempt businesses that collect small amounts of non-sensitive data for their own marketing purposes or that hold data for a very short period of time from certain obligations such as providing consumers with access to their data. Some privacy rights, however, are so fundamental that it would be inappropriate to exempt any businesses from them, e.g. clearly disclosing to consumers that their data is shared with third parties for marketing or other secondary uses.

What should be covered?

We agree that the old formulations for "personally identifiable information" such as name, address and phone number no longer work in an era in which bits of seemingly non-identifying information can be put together to identify individuals or to treat them a certain way without ever knowing their names.

---

[2] E.g. browser "fingerprinting," see Erik Larkin, *Browser Fingerprints: A Big Privacy Threat*, PCWorld, March 26, 2010, www.pcworld.com/article/192648/browser_fingerprints_a_big_privacy_threat.html.

[3] FTC staff report at 42.

[4] For example, the privacy protections in the Gramm-Leach Bliley Act, 15 USC §§ 6801-6809, give consumers only opt-out control of financial institutions sharing their personal information with third parties for marketing purposes and no choice for affiliate or joint marketing sharing. A bill recently filed in Congress, H.R. 653, would strengthen consumers' rights in regard to data-sharing by financial institutions.

Furthermore, supposedly anonymous data can in many cases be re-identified.[5] Certain types or uses of data may merit special protections, as we will discuss later in these comments, but a privacy framework should generally cover any consumer data that can be reasonably linked to a specific consumer, computer or other device. While in some cases it may not be possible to anticipate whether or when data might become reasonably linked to a specific consumer or device in the future, at the point at which it becomes clear that the data might be so linked, its collection and use should be governed by a privacy framework.

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

Should "specific business purpose" or "need" be defined?

We believe that companies should incorporate privacy and security protections into their business practices and consider both privacy and security at all stages of their business activities – not only in designing and developing products and services but in marketing and fulfillment. In doing so, companies should determine what consumer data they actually need for specific purposes, how long it needs to be retained, who should have access to the data and for what purposes, and how to monitor compliance with their internal policies and procedures.

When Google was mapping the placement of WiFi networks for its Street View service, it did not need to collect consumers' unencrypted email addresses, passwords and other personal data. The fact that Google did collect that data, and that such collection was avoidable, demonstrates a lack of the careful consideration for privacy concerns that should be routine.[6]

There are several reasons why the principle that companies should only collect consumer data that is needed for a specific business purpose is important in a privacy framework. First, despite companies' best efforts to safeguard data there is always some risk of a security breach. Another risk for consumers

[5] See Nate Anderson, *"Anonymized" data really isn't – and here's why not*, last updated September 8, 2009, http://arstechnica.com/tech-policy/news/2009/09/your-secrets-live-online-in-databases-of-ruin.ars; Arvind Naryanan and Vitaly Shmatikov, *Myths and Fallacies of "Personally Identifiable Information,"* Communications of the ACM, June 2010, Vol. 53, No. 6, http://www.cs.utexas.edu/~shmat/shmat_cacm10.pdf; Michael Barbaro 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=2&ex=1312776000&pagewanted=all.

[6] In a letter to Google Attorney Albert Gidari on October 27, 2010, FTC's Chief of the Consumer Protection Bureau, David Vladeck, said that the company's failure to discover that it had been collecting the payload data "indicates that Google's internal review processes – both prior to the initiation of the project to collect data about wireless points and after its launch – were not adequate…," see www.ftc.gov/os/closings/101027googleletter.pdf.

is that their data may be sought by law enforcement agencies, plaintiffs' lawyers or others. Consumer data should not be exposed to such risks needlessly. Furthermore, having collected consumer data, it may be tempting for companies to think about ways to use it that were not originally planned and that may not comport with consumers' expectations.

To avoid these problems and help companies and consumers understand their rights and obligations under a privacy framework, it would be helpful for the FTC to define "specific business purpose" and "need." Descriptions of data use such as "internal operations," "fraud prevention," and "legal compliance" are so vague that it is difficult for anyone to know exactly what they mean. Could "internal operations" include sharing consumer data with affiliates or a joint marketing venture with a third party? Could "fraud prevention" mean using or supplying consumer data to investigate whether consumers may have violated a third-party's intellectual property rights? Could "legal compliance" include cooperating with the government's request to compile information about people who seem to fit certain profiles? It is especially important to define these terms if, as suggested in the FTC staff report, it might be appropriate to exempt those uses from requirements for consumer choice.

How long should consumer data be retained?

We agree with the FTC that another important component of any privacy framework is the principle that consumer data should not be retained any longer than is needed for the specific business purpose for which it was collected or that is required by law. In the *Legislative Primer for Online Behavioral Tracking and Targeting* that CFA and several other consumer and privacy groups issued in September 2009, we suggested that online behavioral data should not be retained beyond three months.[7] We also proposed that if such data was only collected and used for a 24 hour period, no consent would need to be obtained from the consumer (with the exception of sensitive data, which we suggested should not be collected or used for behavioral targeting at all). After that period, affirmative consent would be needed for subsequent collection or use. Our rationale was that behavioral data is likely to become "out of date" and thus less useful over time, and that a narrow choice exemption would serve as an incentive for companies to hold consumer data for a very limited amount of time, especially if there is no operational need to retain it longer. It might be useful for the FTC to convene a public workshop that would bring stakeholders together to focus specifically on reasonable retention limits for certain types of data and uses.

[7] See www.consumerfed.org/elements/www.consumerfed.org/file/OnlinePrivacyLegPrimerSEPT09.pdf at 18.

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

Both carrots and sticks can be used to give companies incentives to develop and deploy privacy-enhancing technologies. One obvious "stick" is legislation, which sets out baseline requirements and prohibitions. When companies decide to differentiate themselves by going even further than the law requires it is usually good for their bottom lines – the "carrot" – as well as for consumers. For example, in response to the proliferation of state credit freeze laws, the major credit reporting agencies decided to offer consumers who live in states that do not have such laws the ability to freeze their credit reports for a nominal fee. This gives consumers who are concerned about identity theft more peace of mind, but reducing the potential for identity theft may also help to mitigate credit bureaus' costs in dealing with it.

"Do Not Track" is another example of how the carrot and stick approach could work well. If companies were required by law to honor consumers' "Do Not Track" requests, it would be in their best interests to ensure that "Do Not Track" mechanisms that work effectively. Otherwise, they might be accused of violating consumers' rights, when in fact the problems stemmed from "Do Not Track" mechanisms that did not function adequately. Just the threat that a universal "Do Not Track" mechanism may be required has spurred browser manufacturers to respond, as we will discuss later. But it also presents them with an opportunity to differentiate their companies in the marketplace and generate consumer goodwill.

We are opposed, however, to using broad "safe harbors" as incentives, under which the obligations of collectors and users of consumer data are significantly reduced or eliminated and legal immunity may be provided simply by virtue of their participation in a self-regulatory program. Not all companies will participate, and the degree to which companies are scrutinized before entering into such programs and monitored for compliance afterwards varies. A recent report[8] by the World Privacy Forum on the Safe Harbor agreement between the United States and the European Union concerning the cross-border flow of consumer data documents how a self-regulatory program can provide the illusion of privacy protection but be largely ineffective. Safe harbors may be appropriate in some circumstances, but only if they are very narrowly tailored and carefully monitored.

[8] See *The US Department of Commerce and International Privacy Activities: Indifference and Neglect*, World Privacy Forum, November 2010, www.worldprivacyforum.org/pdf/USDepartmentofCommerceReportfs.pdf.

Companies should simplify consumer choice

Is the list of "commonly accepted practices" for which no choice is needed too broad or narrow?

We agree with the FTC that consumers are over-burdened by lengthy and complex privacy policies, though privacy policies are still important to hold companies accountable for their actions. What consumers need are simple disclosures and meaningful choices. We also agree that choice may not be necessary in certain situations. The most obvious is when consumer data is necessary for product and service fulfillment. An explanation may still be needed – for example, when consumers who sign up for a credit monitoring service are asked for their Social Security numbers, the service provider should explain that this is needed to help identify the correct credit records – but no choice need be given.

"Internal operations," "fraud prevention," and "legal compliance and public purpose" are somewhat vague terms, however. It would be helpful for the FTC to provide more detailed guidance about what these terms mean. They should be defined as narrowly as possible to avoid becoming large loopholes.

Collecting and using consumer data for first-party marketing, however, seems to fall into a slightly different category than these other practices, which are either in direct response to a consumer's explicit request or purely operational in nature.

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

Consumers do not understand that first-party marketing may be based on information that has been gleaned from third parties because that information-sharing process is invisible to them. Research has shown that consumers do not understand the information-sharing practices commonly used in online marketing, or what privacy policies on companies' websites means in terms of sharing their data with third parties or obtaining their data from third parties.[9] Regardless of whether consumers' data has been obtained online or offline, the use of third-party data for marketing should not be considered a "commonly accepted practice" that would exempt the first party from providing choice. As we will explain later, however, we believe that first parties should provide choice no matter whether the data used for marketing is from their direct interaction with consumers or from third parties.

[9] See Joseph Turow, University of Pennsylvania Annenberg School for Communication, and Deirdre K. Mulligan and Chris Hoofnagle, Samuelson Law, Technology & Public Policy Clinic at UC-Berkeley Law School, *Consumers Fundamentally Misunderstand the Online Advertising Marketplace*, October 2007, http://groups.ischool.berkeley.edu/samuelsonclinic/files/annenberg_samuelson_advertising.pdf

For the reasons cited above, we agree with the FTC that first-party sharing of consumers' data with a third party other than a service provider acting on the first party's behalf should not be considered a "commonly accepted practice" because Deep packet inspection by consumers' Internet Service Providers (ISPs) for marketing purposes should also be outside the scope of "commonly accepted practices" because consumers would not anticipate that their ISPs would be monitoring their online activities for marketing purposes.

Similarly, when consumers place their data in "the cloud" – for instance, using cloud services to store and share documents, photographs, personal health records, and other personal data – they would not anticipate that the cloud service providers might access that data and use it to market to them. We discussed this issue at a retreat about consumer protection in cloud computing that CFA held in June 2010. In the report[10] that emerged from the retreat, we noted that "Consumers may conceive of a cloud service as akin to a storage locker – as a rental company that simply rents space that is physically locked by the consumer."[11] Secondary use by the cloud service provider is akin to the rental company breaking the lock and peeking at the contents. While our group, which included businesses as well as consumer and privacy advocates, academics, and representatives of government, agreed that there should be clear disclosure of secondary use and its purpose, we did not reach consensus about whether consumers should be able to say "No" to such use.

CFA strongly believes that consumers should have choice in that regard. One of the features used to promote cloud computing services is that they make it easier for consumers to data with others. But the choice of with whom that data may be shared should always be the consumer's.

Third-party sharing by cloud service providers should also clearly be outside of the scope of any exemption for choice. We understand that some cloud service providers factor internal or third-party use of such data into their business models, but providing choice will not necessarily break those business models. Not all consumers will object to their data being used for marketing, especially if the benefits – for instance, that the data use helps the company provide the service for free – are clearly explained.

---

[10] *Consumer Protection in Cloud Computing Services: Recommendations for Best Practices from a Consumer Federation of America Retreat on Cloud Computing*, November 30, 2010, www.consumerfed.org/pdfs/Cloud-report-2010.pdf

[11] *Id* at 16.

Collection of consumer data across websites, even if done by a single party and not shared with others, should also not be considered a "commonly accepted practice." For example, concerns have been raised about Facebook's "social plugins," which enable the social networking company to track members' visits to websites that install the plugins and compile detailed profiles about what they do on those sites.[12] Consumers would not expect to be tracked in that manner or that that information about their online activities could conceivably be used for marketing purposes, either by the social network itself or by others.

Under the CAN-SPAM Act and the Telemarketing and Consumer Fraud and Abuse Prevention Act[13] consumers have the right to tell companies that solicit them via email or telephone, respectively, not to do so again, even when there are established business relationships. These laws recognize the fundamental principle that consumers should have the right to control their privacy and that marketing intrudes on their privacy. When we talk to consumers about privacy and marketing, they often express frustration that there is not a similar law for solicitations by mail. On balance, we believe that the best and most consistent approach in a privacy framework would be to require that consumers have the ability to opt-out of first-party marketing.

We agree with the FTC, however, that choice should not be required for online contextual advertising. It does not raise the same privacy concerns since it does not involve the collection and retention of data about consumers' online activities over time.

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

Any use of sensitive data, for marketing purposes or other purposes, whether by first parties or third parties, raises serious concerns about how to protect consumers from unanticipated and potentially harmful consequences. In our legislative primer for online behavioral tracking and targeting we stated that sensitive data should not be used for behavioral targeting.[14] CFA believes that sensitive information should not be used for any purpose, online or offline, beyond that for which consumers have specifically provided it. Privacy legislation that has been proposed in Congress would require opt-in consent for

[12] See Justin Brookman, *Facebook Pressed to Tackle Lingering Privacy Concerns*, Center for Democracy & Technology, www.cdt.org/blogs/justin-brookman/facebook-pressed-tackle-lingering-privacy-concerns.
[13] 15 USC §§ 7701-7713 and 15 USC §§ 6101-6108, respectively.
[14] See www.consumerfed.org/elements/www.consumerfed.org/file/OnlinePrivacyLegPrimerSEPT09.pdf at 6.

collection, use and sharing of sensitive data beyond what is needed for the transaction and other operational purposes, with no exception for first-party marketing.[15]

The secondary use of sensitive data raises many valid concerns. For one thing, consumers may not anticipate that sensitive information such as their health conditions, finances, race, ethnicity, sexual preferences, and finances may be used for marketing or other purposes. They may find such use offensive, or be concerned that it could expose them to embarrassment in their households, schools, or workplaces. They may be concerned about the potential use of such information to deny them benefits or to steer them to higher-priced or less advantageous deals. They might be concerned about the security of their sensitive data or about potential access to it by the government or others. If their information is shared with affiliates, consumers may not fully comprehend the different business lines in which a company is engaged and how the information might be used.

If it is appropriate for sensitive information to be collected and used for marketing at all, consumers should be entitled to a heightened level of control, affirmative consent via an opt-in mechanism, even in the case of first-party marketing. The FTC should define sensitive information and set the parameters for its collection and use through a rulemaking procedure, working in cooperation with other agencies that may have jurisdiction over certain types of data such as that related to health and finances.

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

We agree that consumers might not anticipate receiving solicitations by mail or telephone from companies with which they have interacted online, or receiving emails from brick-and-mortar establishments where they have made purchases. Concerns about these practices can best be addressed by requiring choice for first-party marketing. Choice can be granular, allowing consumers to decide how they want to hear from companies about new offers, if at all.

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

We do not think that it is valid to assume that consumers are comfortable with their data being shared with commonly-branded affiliates for marketing purposes. Those affiliates may be in very different types of businesses; for example, General Electric sells appliances and other consumer products, but the

[15] The "Best Practices Act", H.R. 611, Section 104. (b). Note that opt-out choice is required under the bill for first-party marketing in Section 103 (a).

company also sells financial services under the GE name. With the advent of "smart" appliances that can record and transmit information about user behavior, it is not difficult to imagine how such data might be used by the company to market its financial services. Our view is that consumer choice should be required for sharing consumer data with all affiliates, whether commonly branded or not.

How should data "enhancement" be handled under a privacy framework?

As we noted earlier, since consumers would not anticipate that companies with which they have relationships may be marketing to them using data that has been gleaned from other sources, this should not be considered a "commonly accepted practice." If consumers must be given choice, it will prompt companies to explain this data practice, which is not well understood by consumers now. Data enhancement is not necessarily a bad thing, but as we have seen in online behavioral advertising, there can be surprising sources of data, such as one's friends list on social networking sites, and data can be used in ways that consumers may not anticipate.

Practices that require meaningful choice

How should consent be obtained for practices that do not fall within the "commonly accepted" category?

The best method of obtaining consent will vary in different contexts. We agree with the FTC that the choice must be presented at the time that consumers are providing the data – for example, at the cash register, or when consumers are typing in their information into online order forms, or when consumers are deciding whether to use applications. Choice mechanisms should not be located within long privacy policies that consumers are unlikely to read, nor should pre-checked boxes be used. Short, standardized notices should be used to explain companies' practices and consumers' choices.

We will be very interested in suggestions from businesses and industry associations about the best ways to obtain choice in different contexts, and in any studies that demonstrate how well various approaches work. A uniform graphic or icon might be very helpful in signaling to consumers that there is a privacy choice to be made. We are concerned, however, that a proliferation of different icons and graphics may create consumer confusion. Again, some standardization would be useful. We are convinced that if companies use the same creativity and resourcefulness in designing choice mechanisms as are used to design marketing campaigns, choice mechanisms will be more effective.

Under what circumstances, if any, is it appropriate to offer choice as a "take it or leave it" proposition?

Consumers' fundamental rights should not be allowed to be abrogated by "take it or leave it" propositions. As we noted earlier, consumers' data may be needed to provide the product or service that they have requested or for other uses that fall within a carefully defined category of commonly accepted practices. In those instances, "take it or leave it" is appropriate. But except for such narrow exemptions, a privacy framework should prohibit denying consumers access to goods or services, including the content of websites, simply because they have chosen to limit the collection or use of their personal data.

In the financial privacy bill that we referenced earlier,[16] financial institutions would be prohibited from denying goods or services to consumers who choose not to allow their data to be shared, unless that sharing is necessary to provide the products or services they have requested. The legislation allows financial institutions to offer incentives for data sharing – a discount, for example. As a matter of public policy, we believe that this is the correct approach. While there are many choices for consumers in the marketplace, some practices that we believe are unfair, such as mandatory binding arbitration clauses in credit card and cell phone contracts, have become so ubiquitous that consumers do not effectively have any real choice in that regard. We would not want to see similar kinds of clauses for data collection or use become the norm in consumer contracts or terms of service, especially considering how essential services such as search engines, social networking sites, and news portals have become in consumers' everyday lives.

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

Children and teenagers are a special class of consumers that merits special consideration. Since we are joining other groups in separate comments to the FTC about children and teenagers, we will not elaborate here on how issues related to them should be addressed.

Consumers should make informed privacy choices based on timely disclosures about the things they care about most: what data will be collected; how it will be used and by whom; how the data is secured; what the options are for consumer control; and who to contact if there are any questions or problems.

[16] H.R. 653 (2011)

In our cloud computing report, Appendix B provides a sample disclosure that addresses privacy and security, among other issues. It includes a notice about data sharing, what countries' laws apply and which regulators govern the service, basic security information, and the contact information for the service's privacy and security officer.[17]

In this example, because the data is not shared with third parties and is only used by the cloud service provider for technical operation of the service, there is no consent mechanism needed. If there were secondary data uses, we would expect that to be briefly explained and consumers' options in that regard to be outlined in plain language in the disclosure, with "Yes" and "No" buttons provided. Where there is a concrete benefit to the consumer for other types of data uses – for instance, in a free cloud computing service that is supported, at least in part, by the use or sharing of consumers' data for marketing purposes – that could also be explained in clear, straightforward terms (e.g. "Most of our revenue comes from the customer data sharing that we have described. This helps us offer our service at no charge."). We will be interested in the comments of marketing experts about the most effective ways to provide consent mechanisms. As we said earlier, one thing that should be clearly *prohibited* for any type of consent mechanism is the use of pre-checked boxes agreeing to data collection or use.

Special choice for online behavioral advertising: Do Not Track

Should the concept of a universal choice mechanism be extended beyond online behavioral advertising?

CFA and other consumer and privacy organizations first called for creating a "do-not-track" mechanism in joint comments to the Federal Trade Commission in 2007 in connection with an FTC Town Hall on "Ehavioral Advertising: Tracking, Targeting, and Technology."[18] We proposed it as one of several pro-active steps that the FTC should take in order to protect consumers as behavioral tracking becomes more ubiquitous.

In 2008, in response to the FTC's proposed principles for online behavioral advertising, CFA submitted comments with Consumers Union urging stronger action, including creating a "Do Not Track"

[17] See *Consumer Protection in Cloud Computing Services: Recommendations for Best Practices from a Consumer Federation of America Retreat on Cloud Computing*, November 30, 2010, www.consumerfed.org/pdfs/Cloud-report-2010.pdf at 25.

[18] www.consumerfed.org/elements/www.consumerfed.org/file/other/FTC_sign-on_letter_Ehavioral_Advertising.pdf, November 1, 2007

mechanism.[19] We argued that self-regulatory programs such as such as the National Advertising Initiative[20] fail to provide consumers with an effective means of opting out of online tracking because consumers are not aware of them, there is no requirement that companies participate in them, there is no oversight or transparency, and there is no enforcement. Furthermore, we noted that the opt-out mechanisms that these voluntary programs provide to consumers, which are based on cookies, did not work for some tracking methods and fail to provide persistent protection from unwanted tracking since cookies may be deleted for a variety of reasons.

We are pleased that the FTC staff report acknowledges the shortcomings of voluntary measures – the burden that opting out company-by-company places on consumers, the limitations of opt-out cookies, the fact that an effective opt-out mechanism has not been implemented on an industry-wide basis, the lack of clarity about whether existing mechanisms prevent consumers from being tracked or simply prevent them from receiving targeted advertising, and the fact that consumers are not likely to be aware of the technical limitations of existing mechanisms – and that it supports the concept of a universal "Do Not Track" mechanism.[21]

Online tracking can be used for purposes beyond advertising, however. It can be used to make assumptions about people in connection with employment, housing, insurance, and financial services; for purposes of lawsuits against individuals; and for government surveillance. It is already being used, for instance, by life insurers to predict people's longevity.[22] There are no limits to what types of information can be collected, how long it can be retained, with whom it can be shared, or how it can be used. As the Wall Street Journal characterized it in the beginning of its landmark series on privacy, "one of the fastest- growing businesses on the Internet is the business of spying on consumers."[23] A universal "Do Not Track" mechanism should enable consumers to avoid online tracking for any purpose, not just advertising. "Do Not Track" requests should be honored by any entities that are tracking consumers' online activities, no matter whether they are first parties, first-party affiliates, or third parties. First

[19] www.consumerfed.org/pdfs/CFA-CU-behavioralmarketingcomments.pdf, April 11, 2008
[20] See World Privacy Forum report, *National Advertising Initiative: Failing at Consumer Protection and at Self Regulation*, November 2007, www.worldprivacyforum.org/pdf/WPF_NAI_report_Nov2_2007fs.pdf.
[21] "Commission staff supports a more uniform and comprehensive consumer choice mechanism for online behavioral advertising, sometimes referred to as 'Do Not Track'." See www.ftc.gov/os/2010/12/101201privacyreport.pdf at 66.
[22] "Insurers Test Data Profiles to Identify Risky Clients," Wall Street Journal, November 19, 2010, http://online.wsj.com/article/SB10001424052748704648604575620750998072986.html.
[23] Julia Angwin, *The Web's New Gold Mine: Your Secrets*, The Wall Street Journal, July 30, 2010, http://online.wsj.com/article/SB10001424052748703940904575395073512989404.html.

parties should be required to notify other parties that may be engaged in tracking though the first parties' websites.

We also believe that a universal "Do Not Track" mechanism should be developed for mobile devices. There are technical issues that will have to be dealt with, but the fact is that mobile devices are increasing becoming computers with voice capabilities, and data about consumers' activities, including their physical locations, is being tracked and used.

Should a universal choice mechanism offer consumers granular control?

"Do Not Track," as we envision it, would not necessarily be an all-or-nothing proposition. It is simply a way for computer users to tell websites and other Internet entities not to track them, much like putting a "No Trespassing" sign on one's property. But on the Internet, the sign can be interactive, enabling consumers to selectively allow tracking if they wish. It is very important, however, to have a legal definition of tracking. It must encompass the collection or data as well as its use. The FTC should define the term and require clear disclosures about what is being tracked, by whom, and for what purposes. In order for consumers to make well-informed decisions about when to turn "Do Not Track" mechanisms on and off and how to respond to requests by specific entities to allow tracking, this information must be provided in a timely, easy-to-understand, standardized format.

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

The FTC has waited long enough for voluntary measures to give consumers effective control of online tracking, but voluntary efforts, starting with the failed NAI program, have fallen short. In July 2009 four trade associations announced voluntary principles for online tracking,[24] including providing "choice" mechanisms for consumers, but there are many limitations. No choice need be given for tracking by first parties or their affiliates, "sensitive" information is very narrowly defined, and the principles only apply to tracking for advertising purposes. While the proposal calls for creating a centralized choice mechanism, which has only recently become available, companies that subscribe to the principles do not have to use it; they can provide their own choice mechanisms instead if they wish. It is also envisioned that there may be multiple self-regulatory programs in connection with the principles. While it is too early to assess the effectiveness of the principles or the choice mechanisms offered under this

[24]See press release at www.iab.net/about_the_iab/recent_press_releases/press_release_archive/press_release/pr-070209.

initiative, we believe that this approach is likely to be very confusing for consumers and to suffer from the same drawbacks as the NAI program: participation is voluntary, with no real oversight or enforcement, and the choice mechanisms will not be universal or persistent.

When we first raised the "Do Not Track" idea in 2007, we envisioned a list of online trackers' domains that the FTC would maintain and that consumers could download to avoid tracking by those domains (we have never advocated a list of IP addresses of consumers who do not want to be tracked, which would be somewhat analogous to consumers putting their phone numbers on the federal "Do Not Call" registry, because of privacy and security concerns). Our thinking has evolved, however. We believe that a more effective solution would be a tool that would be included in web browsers and that would send information, called a "header," to the websites that consumers visit telling them that the consumers do not wish to be tracked. The browser-header would not physically prevent tracking – it would simply convey the request to the website that the consumer is visiting. Thus, for this method to work effectively there must be a requirement that websites honor the header requests and that they convey those requests to any third parties that collect behavioral data from their sites.

Recently Microsoft announced that the next version of its web browser would accommodate lists of the types that we first envisioned. The company is not proposing to create the lists; it would simply ensure that its browser can accommodate them. The FTC has not proposed that the government create or maintain such lists, either, so it appears that this would be left to the private sector. We think that "blacklists" and "whitelists" for online tracking might be useful, but more as a complement, not a substitute, for the browser-header approach that we advocate.

From a practical standpoint, there are many concerns about the list approach: How would consumers know which list is best among multiple lists that may be offered? Would inferior lists leave consumers exposed to unwanted tracking? How would the lists be kept updated? Would consumers have to pay to subscribe to lists and/or keep them updated? Furthermore, while one advantage of using a list of tracking domains is that it would actually block tracking from those domains, this can easily be defeated by using other tracking technology, such as "fingerprinting," from domains that are not on the list. The list approach is also less flexible than the browser-header approach, since it would block any information from being exchanged between consumers' computers and the domains on the list.

The browser-header approach would work better for consumers and be easier to implement from a technological standpoint. This is the approach being taken by Mozilla Firefox in its recent

announcement. Google also recently announced that it would facilitate consumers' do not requests through a new plug-in to its Chrome browser, but this would only block tracking by a group of specific advertisers.[25] As commentators have pointed out, requiring consumers to add extensions or download lists is burdensome; a do-not-track mechanism that is built into the browser is easier for consumers.[26]

Clearly, there is a groundswell of support for the concept of universal, easy-to-use, and persistent do-not-track mechanisms. We note that as the date of these comments, the FTC has received comments from more than 250 individual consumers in support of "Do Not Track." Congress is also becoming engaged on this issue. A hearing about whether "Do Not Track" is needed was held last December,[27] and legislation, "The Do Not Track Me Online Act," has now been introduced. The bill defines the types of consumer data that should be covered and the entities that should be subject to "Do Not Track" requirements, mandates the FTC to set standards for "Do Not Track" mechanisms, and requires companies to honor consumers' "Do Not Track" requests.[28]

While the FTC has not yet called for legislation, we urge it to do so as part of its final privacy framework. Voluntary measures, while encouraging, will not achieve the goal of providing consumers with "Do Not Track" options that are universal, easy-to-use and enforceable.

Companies should increase the transparency of their data practices

What is the feasibility for standardizing the format and terminology for describing data practices?

We believe that standardizing the format and terminology for describing data practices would help consumers make informed choices about the privacy of their data and help businesses explain their data practices more clearly. It might also provide an incentive for businesses to change their data practices to make them easier to describe. The aim should be to develop something similar to the standardized format and content of nutrition labels, with some flexibility as appropriate. The FTC should consult with experts and hold a public workshop to seek more input in this regard and should develop models and other guidance.

---

[25] See *Firefox, Google Chrome adding "Do Not Track" tools*, Associated Press, January 24, 2011, www.google.com/hostednews/ap/article/ALeqM5ixAo_1N_82L-2-r5l0VgIhKP5Tkg.

[26] See Cade Metz, *Google, MS, Mozilla: Three 'Do Not Tracks' to woo them all*, The Register, February 14, 2011, www.theregister.co.uk/2011/02/14/google_mozilla_and_microsoft_do_do_not_track/.

[27] See CFA testimony at http://www.consumerfed.org/pdfs/Do%20Not%20Track%20Testimony%20of%20Susan%20Grant.pdf.

[28] H.R. 654 (2011)

Should companies inform consumers about the identity of those with whom they have shared their data, and about other sources of their data?

Companies should disclosures the types and names of the businesses with which they share consumer data (except for commonly accepted practices such as fulfillment). While we do not believe that it is necessary for companies to send notices to consumers every time the names of those businesses change, up-to-date information about the businesses with which consumer data is shared should be available through the companies' websites and their customer service representatives. If companies collect consumer data from other sources, those sources should also be disclosed (again, with exceptions as noted above).

Consumers who want access to records showing with whom their data has been shared or where their data came from should have reasonable access to that information. This information would help consumers verify information about data sharing and data sources correct problems such as incorrect data or inappropriate sharing or use of data. The FTC should provide guidance as to what would constitute "reasonable" access.

While the FTC does not ask about access to consumer data by other entities such as by lawyers, private investigators, and government agencies, these are also important privacy concerns. One of the consensus recommendations in our cloud computing report is that, where not prohibited by law, users should receive notice of criminal and civil requests for information,[29] and the model disclosure says: "If possible, we will notify you if another party requests data or other information about your use of this service."[30]

How should non-consumer –facing companies be treated in this regard?

Because consumers have no direct relationship with data brokers, they do not know the identities of those companies or how to reach them. It would be helpful to require all data brokers to be listed in a registry maintained by the FTC or by industry that would provide a central source of contact information

[29] See *Consumer Protection in Cloud Computing Services: Recommendations for Best Practices from a Consumer Federation of America Retreat on Cloud Computing*, November 30, 2010, www.consumerfed.org/pdfs/Cloud-report-2010.pdf at 5.
[30] *Id* at 25.

and that would enable consumers to request access to their data easily. This would be similar to the central source for free annual credit reports.[31]

Should consumers be charged for access to information about sharing or sources of their data?

Access to one's personal data is an important right that should not be limited by unjustifiably high fees. The OECD Privacy Principles provide that individuals should be able to obtain data related to them from the data controller "at a charge, if any, that is not excessive."[32] Under the Federal Privacy Act, federal agencies can charge individuals for the cost of copying the data they request, but not for the time in researching their requests.[33] The Fair Credit Reporting Act (FCRA) gives individuals the right to request free copies of their credit reports from the nationwide credit reporting agencies once in every 12 month period, and in certain other circumstances.[34] Consumers have the right to purchase copies of their credit reports at any time for a fee that must be "reasonable" and which cannot exceed a cap set annually by the FTC.[35]

Thus, the principle is well-established that any charge for accessing and obtaining a copy of one's data must be minimal and reasonable. Fees that are disproportionate to the cost of actually providing the data should be prohibited because they would discourage consumers from requesting their data; worse still, they might provide an incentive for entities to collect more data than they actually need.

Information about the sources of data is also important to consumers, especially if it has been used to make an adverse decision concerning them, as we will elaborate on later in these comments. Companies should maintain audit trails about the sources of data not only to provide consumers with that information on request but to monitor the accuracy and reliability of data sources. The FTC should set reasonable standards for consumers' access to their data and to information about data sources.

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

When a consumer's data is used to determine whether to serve her an online advertisement for a pickup truck or a sedan, the consequences of getting it wrong are not serious enough to justify notifying her about how that decision was made. When a consumer's data is used to deny her eligibility for things

[31] See remarks of Pam Dixon, World Privacy Forum, during FTC Roundtable Series 1, December 7, 2009, http://www.ftc.gov/bcp/workshops/privacyroundtables/PrivacyRoundtable_Dec2009_Transcript.pdfb at 259.
[32] Organization for Economic Cooperation and Development, see http://oecdprivacy.org/#participation.
[33] See explanation at http://usgovinfo.about.com/library/weekly/aa121299a.htm.
[34] See explanation at http://www.ftc.gov/bcp/edu/pubs/consumer/credit/cre35.pdf.
[35] FCRA §612 (f) (1), FTC-prepared document at http://www.ftc.gov/os/statutes/fcradoc.pdf.

such as employment, housing, insurance, credit, or government benefits, however, the consequences *are* serious enough to mandate an explanation. This important principle is reflected in requirements under the FCRA to provide notice of adverse action when credit is denied based on information in a credit report or another source[36] or employment is denied based on credit report information.[37] Consumers are entitled to information about the source of the data and have the right to dispute any inaccurate information.

But with new sources of consumer data such as social networking sites and behavioral tracking over multiple websites, and data brokers collecting increasing amounts of consumer data from a myriad of sources, it is unclear what rights consumers have under the FCRA or other existing laws when the data is used to their detriment. Are employers required to disclose that they have rejected job applicants on the basis of information gleaned from social networking sites?[38] What if insurance benefits are denied on that basis?[39] Must consumers be notified if information about who their friends are or what they chat about on social networking sites is factored into determining their creditworthiness?[40] If adverse decisions are based on tracking consumers' online activities over multiple websites, are the data users required to provide notice and information about the sources of that information to consumers?

It is also important to point out that data about consumers can be used not only to deny them benefits but to determine the prices or contractual terms of the goods or services they are offered. Credit reports have long been used to make unsolicited offers of credit or insurance to consumers. Now some credit card issuers are using online behavioral data to determine which card offers to show to

---

[36] *Id* § 615 (a) and (b)
[37] *Id* §604 (b) (3)
[38] See Wei Du, *Job candidates getting tripped up by Facebook*, MSNBC, August 14, 2007, http://www.msnbc.msn.com/id/20202935/ns/business-personal_finance/, and Grant V. Ziegler, *How social networking is costing people jobs*, News Register, January 24, 2011, http://www.newsregisteronline.com/campus-life/how-social-networking-is-costing-people-jobs-1.1914347.
[39] See Jacqui Chan, *Creepy insurance company pulls coverage due to Facebook pics*, Ars Technica, November 22, 2009, http://arstechnica.com/web/news/2009/11/creepy-insurance-company-pulls-coverage-due-to-facebook-pics.ars; see also Leslie Scism and Mark Maremont, *Insurers Test Data Profiles to Identify Risky Clients*, Wall Street Journal, November 19, 2010, http://online.wsj.com/article/SB10001424052748704648604575620750998072986.html.
[40] See Lucas Conley, *How Rapleaf is Data-Mining Your Friends Lists to Predict Your Credit Risk*, fastcompany.com, November 16, 2009, http://www.fastcompany.com/blog/lucas-conley/advertising-branding-and-marketing/company-we-keep; see also Erica Sandburg, *Social networking: Your key to easy credit?*, CreditCards.com, January 13, 2010, http://www.creditcards.com/credit-card-news/social-networking-social-graphs-credit-1282.php.

consumers who visit their websites.[41] This practice raises a number of questions: Do consumers understand the basis on which the offers are being made to them? Do they realize that they may have other options that could be more advantageous to them? If inaccurate assumptions about consumers result in higher-priced offers, what recourse do consumers have to dispute the information? What is the potential for certain groups of consumers to be unfairly steered towards goods or services at higher prices or less favorable terms than other groups of consumers? Behavioral data is also being used to determine the price that consumers will see at online retailers' sites.[42] This appears to be perfectly legal, though it does not seem fair; when Amazon experimented with variable prices for DVDs based on behavioral tracking, it generated a firestorm of protest and the company quickly retreated.[43]

In the Legislative Primer for Online Behavioral Tracking and Targeting we state that the use of behavioral targeting for redlining activities – denying or increasing the cost of services such as banking, insurance, access to jobs, and access to healthcare, etc. based on information such as race, gender, sexual preference, ethnic origin, disability, income and other characteristics – should be illegal.[44] To the extent that consumer data, whether gleaned online or offline, is allowed to be used to deny benefits or determine the price or terms of an offer, that practice should be transparent and consumers should the ability to get information about the source of the data. Redlining should be prohibited and, as we noted before, "sensitive" data should not be collected or used for behavioral targeting.[45]

Material changes

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

We agree with the FTC that "if transparency and choice are to have any meaning, companies must honor the privacy promises they have made, even when they change their policies with respect to new

[41] See Emily Steel and Julia Angwin, *On the Web's cutting Edge, Anonymity in Name Only*, The Wall Street Journal, August 4, 2010, http://online.wsj.com/article/SB10001424052748703294904575385532109190198.html.
[42] See Annie Lowrey, *How online retailers stay a step ahead of comparison shoppers*, The Washington Post, December 12, 2010, http://www.washingtonpost.com/wp-dyn/content/article/2010/12/11/AR2010121100143.html.
[43] See Troy Wolverton, Now showing: random DVD prices on Amazon, CNET News, September 5, 2000, http://news.cnet.com/2100-1017-245326.html.
[44] See http://www.consumerfed.org/elements/www.consumerfed.org/file/OnlinePrivacyLegPrimerSEPT09.pdf at 6.
[45] *Id*

transactions."[46] The FTC asserts that it is well-settled that companies must obtain opt-in consent before using consumer data in a materially different way than originally claimed. In recent conversations with some businesses on this subject, however, we have found that there is still uncertainty about whether consent should be opt-in or opt-out. We believe that opt-in is the appropriate standard because consumers essentially entered into a contract that their data will be handled in a certain way when they provided it, and a material change to the company's data practices is a change to that contract that requires a new agreement. Another question that has arisen in our discussions is whether any consent, opt- in or opt-out, should be required if a business changes its data practices in a way that provides *more* privacy protection for consumers' data; for instance, if it originally shared such data with third parties and has decided to stop doing so. The issue of whether consumers should be able to cancel contractual obligations without penalty when data collected about their going forward is going to be treated in a materially different way should also be addressed. It would be helpful for the FTC to promulgate clear rules about consumers' rights regarding material changes in the handling of their data.

Consumer Education

How can individual businesses, industry associations, consumer groups, and government do a better job of informing consumers about privacy?

Education about how data practices work, what the potential benefits and pitfalls are, and what options and rights consumers have is crucial in order for consumers to make well-informed choices about the collection and use of their data. All stakeholders have a role to play in educating consumers.

We support the suggestion of the Information Commissioner of the United Kingdom[47] that education about privacy should be integrated into the school curriculum. Consumers need other objective sources of information about privacy as well. Nonprofit organizations are doing innovative work on privacy education. For instance, the American Civil Liberties Union of Northern California has created a special website about online privacy, at www.dotrights.org, with engaging tutorials on a variety of subjects. More funding is needed from foundations and other sources for these types of projects.

[46] FTC staff report at 77.
[47] http://www.ftc.gov/os/comments/privacyreportframework/index.shtm, comment #109 at 5.

What role should government and industry associations have in educating businesses?

Government agencies play a key role in educating consumers about privacy. The FTC has been a leader in this area, with microsites, publications, and other resources for education about children's privacy, identity theft, and general privacy and security issues.[48] State and local government agencies are also active in privacy education. California has an Office of Privacy Protection which provides educational information to both consumers and businesses,[49] and state attorneys general and city and county consumer offices also provide privacy education.[50] As with nonprofit organizations, however, government resources are severely strained, and education is often one of the first areas to be cut when budgets are downsized. Consumer education about privacy and other issues should be recognized as an important government priority.

The most important role that industry associations can play is educating their members. The Direct Marketing Association, for example, provides Guidelines for Ethical Business Practices[51] which cover a variety of privacy issues, and on the Mobile Marketing Association's website there are guidelines and best practices to educate businesses about mobile privacy and other issues.[52] The FTC and other government agencies also provide business education. Sufficient resources should be dedicated to business education about privacy, and government and industry associations should work together to maximize resources for that purpose.

Industry can also help support the efforts of nonprofit organizations to educate consumers about privacy issues. For instance, Capital One has provided funding for Consumer Action to create educational materials about identity theft[53] and other issues.

Other issues related to a privacy framework

One issue that the FTC staff report did not raise is whether it is appropriate for companies to charge consumers to prevent their personal data from being sold. CFA and other consumer and privacy

[48] See FTC consumer privacy portal at www.ftc.gov/bcp/menus/consumer/data.shtm.
[49] See www.privacyprotection.ca.gov/.
[50] See, for example, Hillsborough County Florida Consumer Protection Agency advice on phishing, www.hillsboroughcounty.org/consumerprotection/internet/phishing.cfm.
[51] www.dmaresponsibility.org/guidelines/
[52] http://mmaglobal.com/main
[53] See consumer publication about identity theft at www.consumer-action.org/english/articles/id_theft_account_fraud/

organizations were very disappointed that the recent FTC settlement with US Search, Inc. did not address this issue.[54] The implication was that it is OK to charge consumers who want to opt-out of their information being shared as long as you actually the data for those who pay. This is a troubling precedent. The FTC should squarely confront this issue and take the position that charging consumers for protecting their privacy violates acceptable public policy.

Another issue that the FTC should address more fully in its privacy framework is whether some types of data or some uses of data should simply be "off limits" for uses beyond that which consumers have specifically provided it. We believe that improved transparency and choice are not sufficient to protect consumers in some cases. The FTC should initiate a robust discussion in this regard.

CFA appreciates the opportunity to share our views on the FTC staff report and we look forward to continuing to work with the FTC on these challenging privacy issues.

Respectfully submitted,

Susan Grant, Director of Consumer Protection
Consumer Federation of America
1620 Eye Street NW, Suite 200
Washington, DC 20006
202-387-6121

[54] See joint letter to the FTC at http://www.consumerfed.org/pdfs/FTC_Comments_US_Search.pdf.