TECHNOLOGY POLICY INSTITUTE
Studying the Global Information Economy

February 16, 2011

Federal Trade Commission
600 Pennsylvania Ave. NW
Washington, DC 20580

Dear Sir/Madam:

I hereby submit the attached comments in response to the FTC's December 1, 2010 Notice of Inquiry, "Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers."

Respectfully,

Thomas M. Lenard
President and Senior Fellow
Technology Policy Institute

Before the
FEDERAL TRADE COMMISSION
WASHINGTON, DC 20580

In the Matter of:

Protecting Consumer Privacy in an Era of
Rapid Change: A Proposed Framework
for Businesses and Policymakers

COMMENTS OF

Thomas M. Lenard, Ph.D.
President & Senior Fellow
Technology Policy Institute
1401 Eye Street, NW
Suite 505
Washington, DC 20005
202-828-4405

I. Introduction and Summary

The Federal Trade Commission has issued a preliminary staff report proposing a new privacy framework for businesses and policymakers.[1] The new framework includes provisions intended to better inform consumers about how their information is being used, provide consumers with easier-to-understand choices including a "Do Not Track" option, and restrict how businesses collect, retain and use data.

The Staff Report's rationale for a new privacy framework is that "[a]lthough many…companies manage consumer information responsibly, some appear to treat it in an irresponsible or even reckless manner." "[M]any companies…do not adequately address consumer privacy interests," and therefore "[i]ndustry must do better."[2] However, the report provides virtually no data to support these assertions or shed light on whether the proposed framework would improve consumer welfare relative to the status quo or to alternative proposals. Before finalizing its report, the FTC staff should rigorously analyze its proposal and alternatives by:

- Collecting current data on the privacy and data management practices of major web sites. The most recent data referenced in the Staff Report are from 2000.
- Producing evidence showing whether current practices are harming consumers. Although the Staff Report rejects a harm-based approach, the proposed framework will only produce benefits to the extent it alleviates identified harms.
- Reviewing what is known about how consumers value privacy and undertaking additional studies as a basis for estimating the benefits of a new privacy framework.
- Estimating the costs of the proposed framework and alternatives, including direct pecuniary costs to firms from devoting more resources to privacy and the indirect costs of

[1] Protecting Consumer Privacy in an Era of Rapid Change – A Proposed Framework for Businesses and Policymakers, Preliminary FTC Staff Report, December 2010. (Hereafter FTC staff report).

[2] FTC Staff Report at i.

having less information available. The Staff Report does not acknowledge that its proposal would entail any costs.

- Producing sufficient evidence of a reasonable expectation that the benefits of its proposal are greater than the costs. Otherwise, the proposal should not be adopted.

Notwithstanding the lack of data, the staff is not asking for comments on its basic proposal, but rather only for "comments to help guide further development and refinement of the proposal."[3] A crucial first step is to determine whether the basic proposal has any empirical support.

Many types of regulatory proposals are routinely subject to this type of analysis under Executive Order 12866, issued by President Clinton, and preceding executive orders. The principles of E.O. 12866 were just recently reaffirmed by President Obama:

> As stated in that Executive Order [12866] and to the extent permitted by law, each agency must, among other things: (1) propose or adopt a regulation only upon a reasoned determination that its benefits justify its costs (recognizing that some benefits and costs are difficult to quantify); … (3) select, in choosing among alternative regulatory approaches, those approaches that maximize net benefits….[4]

While the FTC is not formally proposing a regulation, and is an independent agency not formally subject to the executive order, the Staff Report violates its spirit. To the extent the Staff Report's recommendations are adopted, they will have the effect of regulation. It is useful for the agency to gather information from roundtables and comments from interested parties, as it has done. However, as the expert agency on privacy issues, the FTC needs to do more to generate the data needed to address the questions listed above.

Privacy regulation is in many respects *s*imilar to safety regulation. Agencies such as the Consumer Product Safety Commission (CPSC) or the Occupational Safety and Health

---

[3] FTC Staff Report at v

[4] Improving Regulation and Regulatory Review – Executive Order, January 17, 2011 available at http://www.whitehouse.gov/the-press-office/2011/01/18/improving-regulation-and-regulatory-review-executive-order>

Administration (OSHA) propose new safety standards based on data on current industry practices, injury rates, consumers' and workers' willingness to pay for reduced injury risk, the expected benefits of the proposed standard in terms of reduced risk, and a comparison of the expected benefits with the expected costs. The FTC should perform such analysis with respect to its proposed privacy framework.

II. Current Privacy and Data Management Practices

Policymakers cannot make informed policy decisions without having an accurate understanding of the practices prevalent in the marketplace. The most recent data appear to be from 2001. Given the changes in the online world, these data are no longer current, but the studies illustrate the type of data collection and analysis that should be a prerequisite to privacy policy and that the FTC should undertake.

Between 1998 and 2002 researchers undertook four surveys of the privacy practices of commercial web sites:

- A 1998 survey by the FTC.[5]
- A 1999 survey conducted by Professor Mary Culnan, which resulted in a second FTC report.[6]
- A 2000 survey by the FTC.[7]
- A 2001 survey undertaken by The Progress & Freedom Foundation and Ernst & Young which replicated the FTC's 2000 methodology.[8]

---

[5] Federal Trade Commission, Privacy Online: A Report to Congress (June 1998) ("FTC 1998 Report") (available at http://www.ftc.gov/reports/privacy3/index.htm).

[6] Georgetown Internet Privacy Policy Survey: Report to the Federal Trade Commission (June 1999) (available at http://www.msb.edu/faculty/culnanm/gippshome.html). The results of this study of the top 100 Web sites are reported in Online Privacy Alliance, Privacy and the Top 100 Sites: Report to the Federal Trade Commission (June 1999) (available at <http://www/ftc.gov/os/1999/9907/index.htm#13).

[7] Federal Trade Commission, Privacy Online: Fair Information Practices in the Electronic Marketplace: A Report to Congress (May 2000) ("FTC 2000 Report") (available at http://ftc.gov/reports/privacy2000/privacy2000text.pdf).

The period covered by the studies saw general improvement in the privacy practices of commercial web sites. The most recent (2001) survey found that relative to the 2000 survey:

- Web sites were collecting less information.
- Fewer web sites were using third-party cookies.
- Privacy notices were more prevalent, more prominent and more complete.
- Consumers had more opportunities to choose how personally identifiable information (PII) was used.
- More sites were offering opt-in and fewer opt-out.
- More sites were offering a combination of fair information practice elements.
- Seal programs were growing relatively slowly.

The Staff Report references the 2000 FTC survey, noting that "only about one-quarter of the privacy policies surveyed addressed the four fair information practice principles of notice, choice, access, and security."[9] However, the 2001 survey found that 80 percent of the most popular domains implemented notice, choice, and security—up from 63 percent in the 2000 survey—and 48 percent of a random sample (which included much smaller sites) implemented those three practices—up from 27 percent a year earlier.[10]

No one knows whether the period since 2001 saw further improvement in privacy practices or what commercial website practices are today. The FTC needs to have updated information in order to make informed recommendations.

---

[8] William F. Adkinson, Jr., Jeffrey A. Eisenach, and Thomas M. Lenard, Privacy Online: A Report on the Information Practices and Policies of Commercial Websites (March 2002) (available at http://www.pff.org/issues-pubs/books/020301privacyonlinereport.pdf).

[9] FTC Staff Report at 8.

[10] The 2001 survey, while the same as the 2000 survey in all other respects, did not address access practices because of its "unique implementation issues." See FTC 2000 Report at 17 and discussion of Access in this paper, Section IV.E.

III. The Need for Cost-Benefit Analysis

The debate about privacy has engendered strong opinions, but relatively little data or analysis. The FTC staff proposal is based on "the major themes and concepts developed through the roundtables."[11] However, "themes and concepts" developed from roundtables are an inadequate basis for the formulation of new privacy policies. Instead, any proposal should be based on a careful evaluation of the benefits and costs of alternative privacy regimes (including the status quo) to determine which would best serve the interests of consumers. Each element of a proposal would have benefits and costs. Because the report presents no data on either benefits or costs, it is impossible to know whether the proposed framework, or any or its elements, would improve consumer welfare.

The commercial use of information online produces a range of benefits, including advertising targeted to consumers' interests, advertising-supported services, such as free email, search engines, fraud detection, and a reduction in other threats such as malware and phishing.[12] The FTC Staff Report mentions some of the benefits produced by consumer data, but does not evaluate the tradeoffs inherent in greater privacy protections.[13]

More privacy, in the current context, means less information available for the marketplace and therefore potentially fewer benefits to consumers. Indeed, the proposed framework is generally designed to make it easier for consumers to limit the amount of information firms collect and retain. The principal purpose of cost-benefit analysis is to make this tradeoff explicit and evaluate it.

---

[11] FTC Staff Report at iv.

[12] The benefits of information are laid out in detail in Thomas M. Lenard and Paul H. Rubin, "In Defense of Data: Information and the Costs of Privacy," Policy & Internet, Vol. 2: Iss. 1, Article 7 (2010), 149-183.

[13] See, for example, FTC Staff Report at 21, 33-35.

On the cost side, a recent study by Goldfarb and Tucker found that the European Privacy Directive reduced the effectiveness of online advertising by about 65 percent.[14] This means that privacy protections make advertising less useful to consumers and less valuable to advertisers. Advertisers pay less for less-effective ads, which decreases the resources available to support online content. The authors found the effect to be particularly pronounced for more general (less product-specific) websites, such as newspapers.

These results are reinforced by a study by Howard Beales, which shows the rates for behaviorally targeted advertising to be more than twice the rates for untargeted ads.[15] Again, this result stems from the greater value that consumers receive from ads targeted to their interests, which ultimately increases the revenue available to support content.

Although only a few empirical studies of the costs of privacy regulation exist, even less information is available on benefits. There are two related ways to think about the benefits of privacy. First, the benefits of privacy are the reduced harms associated with too much information being available or misused. The Staff Report rejects the harm-based approach because:

> it focuses on a narrow set of privacy-related harms—those that cause physical or economic injury or unwarranted intrusion into consumers' daily lives. But, for some consumers, the actual range of privacy-related harms is much wider and includes reputational harm, as well as the fear of being monitored or simply having private information 'out there.' Consumers may feel harmed when their personal information—particularly sensitive health or financial information—is collected, used, or shared without their knowledge or consent or in a manner that is contrary to their expectations. For instance, the Commission's online behavioral advertising work has highlighted consumers' discomfort with the tracking of their online searches and browsing activities, which they believe to be private."[16]

---

[14] Avi Goldfarb and Catherine Tucker, "Privacy Regulation and Online Advertising," Management Science, vol. 57, no. 1, January 2011, at 57-71.

[15] Howard Beales, "The Value of Behavioral Targeting," available at http://www.networkadvertising.org/pdfs/Beales_NAI_Study.pdf

[16] FTC Staff Report at 20-21.

Harm can include all those things—whatever consumers think is harmful. Physical or economic injury would appear to be easier to quantify than some of the other forms of harm, but the Staff Report contains no data on any harm, however defined. The reason that demonstrating, and to the extent feasible quantifying, harm is important is that it can be the starting point for assessing benefits, which are the reduced harms associated with increased privacy protection.

The Staff Report also does not demonstrate that such benefits would result from its proposals. For example, assume that consumers' discomfort with their information being "out there" is a major element of harm. The Staff Report provides no evidence or explanation as to how or whether its proposed framework would make consumers feel significantly more comfortable. Without a dramatic change in the Internet ecosystem, a substantial amount of information would remain "out there."

Another way to approach benefits is by measuring how much consumers are willing to pay for more privacy. Economists usually prefer basing consumers' willingness to pay on observed market behavior, because how people behave when confronted with actual market choices better reflects their real preferences than do responses to survey questionnaires or behavior observed in experiments. The widespread use of free services such as email and online news subscriptions suggests that people routinely give up some information about themselves in return for access to content, more useful advertising, and other services, although the transaction is indirect. This "revealed preference" approach—preference revealed by actual market behavior—suggests that consumers' willingness to pay for privacy is smaller than the value they receive.

Acquisti, John and Loewenstein try to estimate the value of privacy with a series of experiments and surveys. They find that the results are greatly affected by factors such as how much money or privacy participants are granted when beginning the experiment, the way in which choices are presented to participants, and the way in which questions about the value of

privacy are asked.[17] Their findings "cast doubt on the ability to infer consumers' exact evaluations of personal privacy from market experiments."[18] This seems to be the case, at least with respect to the experiments they present. Their conclusion that "this research raises doubts about individuals' abilities to rationally navigate issues of privacy"[19] is not warranted, however.

IV. The Proposed Framework

The proposed framework is intended to correct what the FTC staff views as shortcomings in the "notice-and-choice" and "harm-based" models. The Report claims the notice-and-choice model is unsatisfactory because consumers do not understand how their data are being used or the posted privacy notices.[20] Likewise, the harm-based approach is unsatisfactory because, as indicated above, it focuses on an overly narrow range of harms.

To correct these deficiencies, the Staff Report recommends companies should:[21]

1. Adopt "privacy by design." This includes providing "reasonable" security for consumer data, collecting only the data needed for a specific business purpose, retaining data only as long as necessary to fulfill that purpose, safely disposing of data no longer being used, implementing reasonable procedures to promote data accuracy, assigning personnel to oversee privacy issues, training employees on privacy issues, and conducting privacy reviews for new products and services.

---

[17] Alessandro, Leslie John, and George Loewenstein, "What is Privacy Worth," at 33, available at http://www.futureofprivacy.org/wp-content/uploads/2010/09/privacy-worth-acquisti-FPF.pdf

[18] Acquisti et al at 32.

[19] Acquisti et al at 33

[20] FTC Staff Report at iii.

[21] FTC Staff Report at v.

2. Provide choices to consumers about their data practices in a simpler, more streamlined way. The most practical way of doing this involves the placement of a persistent setting, sometimes referred to as "Do Not Track."
3. Make their data practices more transparent to consumers.
4. Provide consumers with reasonable access to their data.
5. Obtain affirmative consent for retroactive changes to data policies.

The Staff Report provides virtually no analysis of these proposals.

A. Privacy by Design

As discussed in Section II, the Staff Report contains no analysis of how companies currently address privacy within their organizations. The staff recommendations are made without any systematic data on current practices.

Major companies already have chief privacy officers and devote significant resources to privacy and data security. The Staff Report notes that the Commission has brought 29 cases against companies that failed to provide reasonable security.[22] The Report does not explain why the Commission's current enforcement authority, together with other substantial incentives that companies already have to protect data, are insufficient.

Building greater privacy protections into operations and products and services and assigning additional personnel to privacy issues entails costs that companies would likely pass through to consumers. There is no analysis of what the costs or the benefits of this "privacy by design" would be. Do consumers want companies to incur these costs, or would they instead prefer to pay lower prices?

---

[22] FTC Staff Report at 45.

B. Simplified Choice

The Staff Report proposes requiring companies to offer choice for practices that are not "commonly accepted." Commonly accepted practices are limited to product and service fulfillment, internal operations, fraud prevention, legal compliance and public purpose, and first-party marketing. The Staff Report does not explain how the staff arrived at its definition of what is commonly accepted nor does it analyze the implications of making it more difficult to use data for all the remaining "not commonly accepted" practices.

For example, the Report indicates that "deep packet inspection would likely warrant enhanced consent or even more heightened restrictions," because of several factors, including limited residential broadband competition.[23] Whether or not this assessment of broadband competition is accurate, the Staff Report does not apply the same criterion to other entities that collect and use consumer data, such as online retailers, search engines, travel sites etc. Would the staff propose in general to relate the level of consent required to measures of competition, such as concentration levels? This is important, because in singling out deep packet inspection, the Report seems to be choosing among different technologies for collecting data. As a general rule, policies should be technology neutral, absent a good reason for deviating from that rule.

Moreover, the Report again contains no analysis of the costs and benefits of this proposal, which should include a broader assessment of the competitive effects of making it more difficult for ISPs to participate in the online advertising market. For example, cutting off a potential new revenue source could make the broadband market less competitive because entry would be less attractive. Online advertising revenues could help cover the costs of broadband buildout. Inability to take advantage of this revenue source could mean higher direct access costs for consumers. Finally, ISP participation could help make the online advertising market itself more competitive.

---

[23] FTC Staff Report at 62.

C. Do Not Track

The Staff Report endorses a Do-Not-Track mechanism for providing simplified choice, but at the same time asks commentors a series of questions on how such a mechanism should be designed and what its impact would be, including:[24]

- What are the potential costs and benefits of offering a standardized uniform choice mechanism to control online behavioral advertising?
- How many consumers would likely choose to avoid receiving targeted advertising?
- How many consumers, on an absolute and percentage basis, have utilized the opt-out tools currently provided?
- 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?

These are questions the FTC staff itself should research before endorsing the Do-Not-Track mechanism.

The term used to describe this mechanism could also be misleading. A Do-Not-Track mechanism may sound like a good idea, because the telemarketing Do-Not-Call List is popular. But the similarities between the two end at the names. For example, people sign up for the Do-Not-Call List in order to reduce unwanted marketing solicitations. A Do-Not-Track mechanism would not do that. Consumers would not necessarily receive fewer ads. (Indeed, for that reason it might be difficult for them to know if the mechanism was actually working.) They would just receive ads that are less-well-targeted to their interests. Several easily available tools let consumers block ads on the Internet, but a Do-Not-Track mechanism is unlikely to be one of them.

Some people may use a Do-Not-Track mechanism because they derive utility simply from knowing they are not being tracked. As the discussion above indicates, although this value

---

[24] FTC Staff Report at A-4.

is not easily quantifiable, the FTC staff should make some effort to summarize what we know and don't know about consumers' valuation of privacy and perhaps sponsor some research in the area.[25]

These potential benefits need to be weighed against the costs, assuming a Do-Not-Track mechanism is technically feasible.[26] First, what are the direct costs of implementation? Second, what are the indirect costs in terms of the quantity and quality of services and content on the Internet? Many of these costs would be borne not only by Do-Not-Track participants but by other Internet users as well. A Do-Not-Track mechanism (depending on how many people used it) would reduce the value of the Internet as an advertising medium, and therefore would reduce the revenues available to support Internet content. A Do-Not-Track mechanism would also affect the quality of major Internet services, such as search engines, which use data on search histories to update and improve their algorithms, and to protect against threats such as search spam, click-fraud, malware and phishing. The less data search engines have the less well they will perform. In sum, the information generated by online tracking generates positive externalities that support the services that everyone uses. Consumers who opted for a Do-Not-Track mechanism would be free-riding off those consumers who allowed their data to be used.[27]

Finally, consumers who used a Do-Not-Track mechanism would receive ads that were less-well-targeted and therefore less useful. The cost of this would depend on the value these consumers place on advertising.

The three major browser providers—Google, Microsoft, and Mozilla—have announced that their products will include Do-Not-Track mechanisms.[28] It is unclear whether this is a

---

[25] See discussion in Section III. This point is also made in Commissioner Kovacic's concurring statement. FTC Staff Report at D-1.

[26] See Commissioner Rosch's concurring statement. FTC Staff Report at E-6.

[27] This is in contrast to the Do-Not-Call List. Signing up for the Do-Not-Call List would not appear to impose costs on other consumers.

[28] See http://downloadsquad.switched.com/2011/01/26/do-not-track-analysis-of-google-microsoft-and-mozillas-solutions/

response to demands from consumers or to the specter of regulatory intervention. In any event, these "market" solutions should be permitted to develop without any additional pressure or requirements from the government.

D. Increased Transparency

The Staff Report notes that many consumers don't understand how their data are collected and used and that privacy notices are complex. This is undoubtedly true, because the use of data online is quite complicated. Accordingly, the framework proposes steps to make data practices more transparent to consumers. It recommends that privacy notices should be clearer, simpler to understand, and more transparent.

Transparency and simplicity are worthwhile goals, but are unlikely to be costless. Simplifying privacy notices would affect not only the notices, but also the ways companies use data, which would be constrained to conform to the notice standards. Thus, implementing transparency and simplicity requirements could reduce benefits to consumers and impose costs on businesses. Whether this is an important issue is unclear, but it should be analyzed.

E. Access

Previous FTC reports have acknowledged the complexity of providing consumers with access, i.e., the ability to examine data about themselves and potentially challenge its accuracy. The FTC 2000 Report stated that "the Commission believes that Access presents unique implementation issues … including what categories of data must be made available; the costs and benefits of providing access; and how to ensure adequate authentication."[29] The FTC staff needs to address whether access really is valuable to consumers, how it would actually be implemented, and its potential to reduce the security of personal information.

---

[29] FTC 2000 Report at 17

F. Affirmative Consent for Retroactive Changes to Data Policies

Requiring consumers to be afforded the opportunity to consent to "new uses" of data may mitigate against their use, because of the strong tendency of consumers to stay with the default.[30] The recent Department of Commerce Green Paper, while proposing that companies should incorporate "purpose specifications" and "use limitations" in their notices and privacy practices, also notes that "[t]he current privacy policy framework has created an environment in which 'creative re-use of existing information' has led to innovations."[31] The Green Paper provides a useful hypothetical that illustrates the potential tradeoff:

> Suppose that company executives have grown concerned with security threats against its network equipment and customers' computers. The Chief Executive Officer (CEO) approves a proposal to provide … Internet usage records … to in-house researchers, so that they can analyze network traffic and develop security countermeasures. This use of personal information has the clear potential to bring privacy and security benefits to the ISP and its customers. The proposed use, however, would also be contrary to the ISP's specified purposes for collecting the information in the first place.[32]

There are likely to be new commercial uses (unrelated to security) that also might benefit consumers. It is important to carefully weigh the privacy benefits against the costs of not being able to use data for new uses. Obviously, new uses will not be known at the time a privacy rule or practice is being implemented. Innovations foregone are, by their nature, difficult to identify and measure.

---

[30] Lenard and Rubin *supra* note 12 at 174.

[31] The Department of Commerce, Internet Policy Task Force, Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework, December 2010, at 38, available at http://www.commerce.gov/sites/default/files/documents/2010/december/iptf-privacy-green-paper.pdf (hereafter Green Paper).

[32] Green Paper at 39.

V. Conclusion

The privacy debate is taking place in an empirical vacuum. The FTC Staff Report contains no systematic data on current privacy practices of firms or consumers, and no systematic analysis of the benefits or costs of alternative privacy regimes. While the staff acknowledges the need to assess the costs and benefits of its most prominent proposal, a Do-Not-Track mechanism, the staff endorses the proposal itself without benefit of such an assessment. Because the Staff Report provides virtually no new data or analysis, it is seriously deficient as a foundation for new policy recommendations. It also violates the spirit, if not the letter, of President Obama's recent executive order on regulation, which stresses the need to evaluate both benefits and costs. Without such analysis, there is no way of knowing whether a particular regulatory action will improve or reduce consumer welfare.