Electronic Frontier Foundation
Protecting Rights and Promoting Freedom on the Electronic Frontier

COMMENTS OF THE ELECTRONIC FRONTIER FOUNDATION

To The
DEPARTMENT OF COMMERCE INTERNET POLICY TASK FORCE

Regarding
COMMERCIAL DATA PRIVACY AND INNOVATION IN THE INTERNET ECONOMY: A DYNAMIC POLICY FRAMEWORK

The Electronic Frontier Foundation (EFF) is pleased that the Commerce Department and the Internet Policy Task Force (IPTF) recognize the significant consumer privacy issues raised by the current online environment.

We agree with many of the Green Paper's basic findings: that "privacy protections are necessary to encourage individuals to adopt new devices and services"; that "protecting privacy is critical to preserving the Internet's value as a tool for free expression, democratic participation, and forming and maintaining social bonds"; and that "changes in technology and business models have rendered parts of our privacy policy framework out of date."

In particular, we commend the IPTF for recognizing that:

• "Online privacy is important to many Americans," including younger Americans.

• "[C]onsumers generally—and incorrectly—believe that a company's posting of a privacy policy sets categorical limits on the company's sharing of personal information."

• "[C]onsumers do not always understand how and with whom their information might be shared, or the potential negative implications of sharing such information."

We also commend the IPTF for supporting the Federal Trade Commission's interest in the browser-header-based "Do Not Track" proposal and appreciate the IPTF's recognition that the FTC is the lead consumer protection enforcement agency for the U.S. government. However, we question the practical value of the suggested Commerce Department Privacy Protection Office (PPO). We fear that the PPO would divert resources and attention from the FTC's privacy work by effectively creating a second agency process in the same area.

Finally, we strongly support the IPTF's call for reform of the Electronic Communications Privacy Act (ECPA).

454 Shotwell Street • San Francisco, CA 94110 USA
+1 415 436 9333 +1 415 436 9993 www.eff.org information@eff.org

I. "DO NOT TRACK" AND USER-FRIENDLY OPT-OUT MECHANISMS

EFF strongly supports a browser-header-based "Do Not Track" (DNT) mechanism,[1] and we urge the Department to do so as well.

We will discuss our views on DNT in greater detail in our forthcoming comments to the FTC. Useful background discussion of DNT's history, technical details, and policy implications is already widely available.[2] Our focus here is on process.

Many aspects of DNT are already moving today. Technologists have been publicly discussing DNT technical issues, and the Internet Engineering Task Force will soon consider a draft regarding DNT.[3] Browser vendors like Mozilla are incorporating DNT into new releases.[4] Microsoft's Tracking Protection, a complementary privacy mechanism, also helps fuel the discussion and further indicates the practical reality of incorporating advanced privacy features into browsers.[5] However, more work is needed to establish a standard framework for how tracking entities are expected to respond to consumers' preferences as expressed through a DNT header signal.

EFF believes that the Department can most help promote DNT in two ways. First, the Department can support legislation that would clearly authorize the FTC to act on DNT. We expect that the FTC would engage with the ongoing technical efforts to address compliance and other issues. Second, the Department and the Government at large could, without any legislation, "realistically embrace the header as an improved mechanism for tracking opt outs on government sites." As security and privacy researcher Christopher Soghoian notes, this can both "[a]void[] the chaos of 100+ different federal agency opt out cookies" and "provid[e] early support for the Do Not Track header at a time when the technology proposal could very much use a boost."[6]

We emphasize that our concern here is privacy: protecting consumers against the largely invisible, poorly understood, and continually escalating surveillance of their online activities. As Stanford's Arvind Narayanan explains, "Do Not Track isn't just about behavioral advertising" and implicates a "wider debate about the monitoring of user

---

[1] *See*, *e.g.*, http://www.eff.org/deeplinks/2011/01/mozilla-leads-the-way-on-do-not-track.
[2] *See*, *e.g.*, http://33bits.org/2010/09/20/do-not-track-explained/; http://paranoia.dubfire.net/2011/01/history-of-do-not-track-header.html; http://donottrack.us/; http://www.freedom-to-tinker.com/blog/harlanyu/some-technical-clarifications-about-do-not-track.
[3] *See* http://cyberlaw.stanford.edu/node/6597.
[4] *See* http://firstpersoncookie.wordpress.com/2011/01/23/more-choice-and-control-over-online-tracking/.
[5] *See* http://blogs.msdn.com/b/ie/archive/2010/12/07/ie9-and-privacy-introducing-tracking-protection-v8.aspx; http://blogs.msdn.com/b/ie/archive/2011/01/25/update-effectively-protecting-consumers-from-online-tracking.aspx.
[6] *See* http://paranoia.dubfire.net/2011/01/what-us-government-can-do-to-encourage.html.

activity online, and even more widely, the aggregation of personal information for a variety of purposes"; for example, "Facebook can keep track of all the pages you visit that incorporate the ['like'] button, whether or not you click it."[7]

Notably, as Stanford's Jonathan Mayer explains, most forms of online advertising—contextual advertising, demographic advertising, search advertising, placement advertising, and social network advertising—would not be affected by DNT, which is focused on protecting consumers against invasions of privacy and not against advertising itself, and therefore "would only affect a sliver of the online advertising market."[8]

We therefore doubt that a recent study of the effects of European Union (EU) privacy regulation is relevant to the U.S. policy debate over DNT.[9] According to that study, online behavioral tracking techniques cause a roughly 2.3 percent increase in advertising effectiveness. The magnitude of this effect, however, is based on *stated* purchased intentions, rather than actual purchases. Because stated purchase intentions do not always correlate to actual purchases,[10] the true magnitude (or the very existence) of the purported effect cannot be established from this analysis.

Importantly, the study further found that EU regulation had no statistically significant negative impact on advertising effectiveness for the vast majority of the ads considered: that is, larger ads, dynamic and/or media-rich ads, or ads on non-generic sites (*i.e.*, contextual ads that are targeted to consumers based on the content of the site – *e.g.*, car ads on car websites). In short, the study should be read as showing that regulation had no impact on ad effectiveness, except for a very specific subset of ads.

II. A GENERAL REGULATORY FRAMEWORK FOR COMMERCIAL DATA PRIVACY

A. FIPPs and the FTC

EFF believes that a baseline commercial data privacy framework built on the Fair Information Practice Principles (FIPPs) should be adopted via statutory delegation of regulatory authority over the FIPPs to the FTC. Congress should establish the FIPPs as general baseline principles and allow the FTC to elaborate upon those principles in both regulations and enforcement actions. The FIPPs should be a basis for FTC enforcement independent of, though likely in combination with, its Section 5 jurisdiction. We caution

---

[7] *See* http://cyberlaw.stanford.edu/node/6573.
[8] *See* http://cyberlaw.stanford.edu/node/6592.
[9] *See* Goldfarb and Tucker, *Privacy Regulation and Online Advertising*, available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1600259.
[10] *E.g.*, Thomas Juster, "Consumer Buying Intentions And Purchase Probability: An Experiment In Survey Design," *Journal of the American Statistical Association*, 61(315), 658-696 (1966); Charles Manski, "The Use Of Intentions Data To Predict Behavior: A Best Case Analysis," *Journal of the American Statistical Association*, 85(412), 934-940 (1990).

that the FIPPs cannot be limited to traditional notions of Personally Identifiable Information (PII), given advances in data re-identification.[11]

We see little policy justification for limiting the FTC's rulemaking authority here. The technical aspects of commercial data privacy are sufficiently complex as to require an agency with both significant technical expertise and experience with consumer privacy. While FTC elaboration may reveal conflicts between existing law and the FIPPs privacy landscape, such conflicts are unlikely to be fully anticipated in legislation, and will need to be resolved within agency rulemaking or enforcement actions. The FTC should have the primary role here.

Assignment of primacy to the FTC does not, however, require exclusivity. If legislation establishes the FIPPs as law, state attorneys general should be able to enforce the FIPPS prior to and without need for FTC regulatory elaboration. We also support private rights of action that allow for consumer class actions. While these other entities may choose not to litigate FIPPs violations until elaboration by the FTC, there is no reason to delay the possibility of such litigation over colorable violations of the FIPPs. Such a multi-pronged enforcement approach is likely to give industry strong incentives toward greater privacy protections.

Finally, any such legislation should provide the FTC with greater resources for investigation and enforcement, as well as greater authority to impose monetary fines or penalties. The FTC's recent recruitment of technologists has significantly enhanced its understanding of the online environment, and the need for such technological expertise will persist.

B. Transparency, purpose specification, and verifiable evaluation and accountability

We agree that enhancing transparency, improved purpose specification, and verifiable evaluation and accountability should receive high priority. In our view, transparency and purpose specification relate to what an entity *says* about what it is doing. Verifiable evaluation and accountability mechanisms should provide the link between an entity's statements and its actual practices.

These measures promote informed consumer choice. We know, however, that in practice consumer choice is exercised in a less-than-ideal fashion.[12] Thus, the more significant real-world value of these initiatives may be to expose companies' policies and practices to greater scrutiny by enforcers like the FTC, state attorneys general, consumer watchdogs, and the plaintiffs' bar.

---

[11] *See*, *e.g.*, http://33bits.org/2010/06/21/myths-and-fallacies-of-personally-identifiable-information/.

[12] *See* Aleecia M. McDonald & Lorrie F. Cranor, *The Cost of Reading Privacy Policies*, 4 ISJLP (2008), *available at* http://lorrie.cranor.org/pubs/readingPolicyCost-authorDraft.pdf, at 2.

While crucial, transparency is harder to achieve in practice than in theory. Disclosure obligations—chiefly, privacy policies—give firms incentives to be simultaneously too verbose and too vague. Even if customers do read privacy policies, most are "essentially unusable as decision-making aids,"[13] either because they are difficult to understand, or because the service itself is conditioned upon consent to the policies' contents.

For this reason we believe that DNT (and, we expect, future proposals that will be built upon it) are a key part of good transparency practices. Such standards will give businesses a clear way to know what each consumer expects of them, and to disclose privacy practices that are expressed clearly in relation to those expectations. For instance, if a website needs to track the user in order to fund the content it produces, that can be clearly and succinctly explained to users who have turned on a DNT header since their last visit. That type of circumstance and detail-specific disclosure is the only way to have informed choice that is actually informed choice.

We view purpose specification mainly as a subset of transparency; a disclosure that inadequately specifies purposes simply is not transparent. In EFF's work on smart grid privacy with the Center for Democracy and Technology, we found that even where relevant policies were available, they were often underspecified—lacking, for example, definitions for critical terms, such as the types of energy usage data protected. And, although policies often listed purposes for which data would be used, those purposes were often so broadly stated (e.g., "to provide you with a better experience") as to allow virtually limitless uses of the data. No energy service policy that we were able to collect explained whether the information collected from customers is limited to the minimum amount needed to fulfill any stated purpose, for example.[14]

Our general point is that the FIPPs will not and cannot function as intended unless terms are clearly specified. Vague specifications like "better user experience" tell consumers nothing useful in terms of choice, and fail as meaningful standards against which to measure a company's compliance. If common terms like "affiliate" vary too greatly, consumers will face a transparency Tower of Babel.

We also think that DNT is just one example of the way that technical measures may improve purpose-related disclosure. DNT is a consumer-expressed preference that says the user's browser information may be used for sending content to the user, but not for

---

[13] *See* Carlos Jensen & Colin Pitts, *Privacy Policies as Decision-Making Tools: An Evaluation of Online Privacy Notices*, 6 Proceedings of the SIGCHI conference on human factors in computing systems 471, 477 (2004), available at http://delivery.acm.org/10.1145/990000/985752/p471-jensen.pdf.

[14] *See* CDT-EFF, *Proposed Smart Grid Privacy Policies and Procedures* 5-9 (California Public Utility Commission Rulemaking 08-12-009) (Oct. 15, 2010) (Attached as "Exhibit 1 of 1").

recording the user's reading habits. Over time, we believe that similar standards should and will be developed for other kinds of purpose specification.

Transparency, purpose specifications, and verifiability and accountability are important in themselves, but the ultimate goal here is consumer privacy. The map must not be confused with the territory, and we are concerned that compliance and enforcement resources will address these mechanisms rather than privacy itself. If, on the other hand, companies face credible threats of enforcement, including financial liability, for failing to protect consumer privacy, we would expect companies to use these mechanisms in order to protect themselves. We assume that insurance entities will help companies manage their exposure, perhaps by requiring "best practices" similar to those that would be generated through multi-stakeholder processes. In short, these initiatives are important, but they must be combined with a credible threat of liability for failing to protect privacy.

C. Privacy impact assessments (PIAs)

Good PIAs are risk assessments. They need to evaluate the incremental risk the user is exposed to against a range of privacy adversaries including, in no particular order: employees of the company who happen to have a relation or past relationship with the user; data brokers and intrusive advertisers; private investigators; civil litigants and civil discovery processes; the user's family, most especially intrusive parents and abusive partners; employers; insurers; political opponents; and law enforcement. A PIA needs to consider the probability that the firm's practices causes a harmful disclosure of information to each of these types of adversaries, multiplied by the potential seriousness of the disclosure (for instance, an adverse disclosure to an authoritarian regime creates a risk of imprisonment or death, which is generally more severe than the risk of termination due to some private fact being disclosed to an employer).

D. The proposed PPO

Our position on the proposed PPO flows largely from our support for the FTC's primacy in the privacy area. First, we question any suggestion that the FTC's role here is or should be limited to enforcement. Policy and enforcement are not easily separated in an area so thoroughly involved with technology issues. Investigation and enforcement action will yield technical information that is highly relevant to policy concerns.

We are also concerned that the PPO multi-stakeholder process will interfere with the FTC's ability to act in this area, either by creating dual policy tracks or by fragmenting scarce resources. Privacy protection has been difficult even with one lead agency on consumer privacy.

The factual or empirical requirements of sound policy-making pose another problem. Traditional APA rulemaking is rulemaking on an administrative record, and much of judicial review of agency rulemaking is focused on whether and how well the record supports the rules. In this area, many questions should not be resolved based solely on political negotiation and cannot be resolved without facts about existing practices. For

instance, data minimization requires that entities only retain information for as long as is necessary to fulfill the specified purpose or purposes, yet any meaningful discussion of data minimization would require some verified factual basis about how the necessity of such data decreases over time. We are unclear as to how facts would be assembled and evaluated in the Department's contemplated multi-stakeholder process. We also are unclear on how the product of a PPO process would be subject to judicial review, challenge or interpretation.

We are also skeptical about the Department's emphasis on "voluntary, enforceable codes of conduct"; we are not sure what it means. We assume that this means codes of conduct voluntarily adopted by companies such that lack of compliance by a company would at a minimum subject that company to FTC enforcement under its Section 5 authority, as well as enforcement by state attorneys general and by private individuals under state laws such as California's Business & Professions Code § 17200 *et seq*. Because we support the creation of federal private rights of action, we would also generally preserve such rights of action.

If this is correct, however, we are confused by the notion of "legislation that would create a safe harbor for companies that adhere to appropriate voluntary, enforceable codes of conduct." What would the safe harbor protect against? Because we do not support federal preemption of all non-federal statutes in the privacy area, we would not support the notion that such adherence would insulate companies against stricter state laws. Furthermore, we are unsure about the legal status of legislative adoption of safe harbors based on voluntary codes of conduct under the U.S. Supreme Court's non-delegation cases.

We are also unclear as to the meaning of open, multi-stakeholder processes. Would funding be provided to the many small non-profit consumer and privacy advocacy groups that otherwise could not afford to travel to meetings? Would *ex parte* contact rules apply? More generally, how would procedural fairness be assured?

Outside of clear extreme cases, we are skeptical that there can be a meaningful definition of failure in this context. Consumer groups may well deem a result to be a failure when companies do not, and vice versa. Legal challenges to any code of conduct arrived at in the multi-stakeholder process are inevitable. Thus, tying the FTC to the PPO process may cause protracted delay. More generally, we see no reason for any FTC process to wait for the PPO process. Whatever one's view of the FTC's speed, sequencing the two processes is likely to take longer. Accordingly, we do not support any independent PPO process outside of an actual FTC rulemaking process, within the relatively clear confines of the APA.

III. PREEMPTION AND STATE ENFORCEMENT

It is often easier for states to act on privacy protection than the federal government. California's landmark data breach notification law is a good example. Many states have followed California's lead, but Congress has been unable to enact federal data breach

notification requirements. Industry has been able to adapt to state laws, and innovation by the states helps to spur industry innovation.

Accordingly, federal law should be a floor, not a ceiling, and we do not support preemption of state privacy protection or state unfair and deceptive trade practices laws. We do support state enforcement of privacy laws, and believe that any federal law should make clear that state attorneys general are authorized to enforce federal laws to at least the same extent as the FTC. We also support private rights of action. If both the states and their citizens can enforce federal law, there is far less need to worry about which law is more protective.

While the strength of the actual rule is important, so is the practical likelihood of enforcement action. The threshold issue here is the enforcer's initial burden. Requiring a showing of harm, for example, creates an enormous first-mover burden on plaintiffs and significantly reduces incentives to comply. The next criterion is remedies. Even if damages are not available, generous attorney's fee and cost provisions can increase the likelihood of enforcement.

IV. ELECTRONIC COMMUNICATIONS PRIVACY ACT REFORM

We agree that the Administration should review the Electronic Communications Privacy Act (ECPA), with a view to addressing privacy protection in cloud computing and location-based services. As a member of the Digital Due Process Coalition (http://www.digitalddueprocess.org) we fully support its proposals for ECPA reform. Because both governmental and private-sector data gathering threaten user privacy, however, we believe that additional reforms are warranted, including but not limited to the following:

1. ECPA should restrict communications providers' disclosures of non-content to non-governmental third parties. Currently, providers may freely share non-content information with anyone other than the government.

2. To the extent that communications providers do transfer content or non-content information to third parties, such as via consent or any other ECPA exception, such third parties should remain governed by ECPA, much as the Video Privacy Protection Act treats all recipients of customer information as covered providers with respect to such information.

3. A suppression remedy should be available wherever information is obtained by prosecutors in violation of ECPA. Currently, only the contents of illegal oral or wire intercepts are statutorily excluded from evidence; electronic communications that are illegally intercepted, or stored communications content and records illegally obtained from a communications provider, may be freely used.

4. ECPA should require meaningful, comprehensive reporting of how all its various authorities are used, akin to the reporting that is currently required (only) for wiretapping,

and should require eventual notice to anyone whose communications content or records are obtained under the statute.

Respectfully submitted,

Lee Tien, Senior Staff Attorney
Peter Eckersley, Senior Staff Technologist
Electronic Frontier Foundation