



January 28, 2011

Send via email to [privacynoi2010@ntia.doc.gov](mailto:privacynoi2010@ntia.doc.gov)

National Telecommunications and Information Administration  
U.S. Department of Commerce  
1401 Constitution Avenue NW.  
Room 4725  
Washington, D.C. 20230

RE: Commercial Data Privacy & Innovation in the Internet Economy: A Dynamic Policy Framework  
Docket No. 101214614-0614-01

The Online Trust Alliance (OTA) hereby submits its comments to the Department of Commerce request for comments on Docket No. 101214614-0614-01.

Thank you for providing the Online Trust Alliance with the opportunity to submit comments to the draft report. As a member-based entity with over 80 organizations representing the internet ecosystem, OTA's mission is to develop and advocate best practices and public policy to mitigate privacy, identity, and security threats to online services, brands, organizations and consumers, thereby enhancing online trust and confidence.

OTA commends the Department of Commerce for its "green paper" on innovation and privacy. We believe this draft report will make an important contribution to advance best practices, protect consumers, spur innovation and enhance online trust. Efforts to support the evolving role and importance of privacy protections and self-regulatory efforts are the foundation for commerce and the vitality of the internet. OTA believes any changes to the regulatory landscape needs to consider the impact to ad-supported content services, innovation, and commerce. Accountability, data stewardship and data protection are equally important as privacy concerns. Any framework needs to address privacy concerns and protect consumer data from abuse, exploits, breach and loss without compromising a business's security and fraud detection capabilities.

The OTA supports establishing a Privacy Policy Office (PPO) with clear ownership and distinction from the FTC as a regulatory and enforcement agency. An ideal PPO will serve as a resource, sounding board, and source of expertise for the business community and law makers. The PPO should leverage expertise through the use of legal, academic, as well as business technical leaders leveraging a "loaned executive" model to bring business and operational perspectives to the consensus building advisory body. The OTA

will support a PPO in developing and recommending a standard and comprehensible set of guidance, best practices, or laws.

As legislation is introduced or evolves, it should not hamper innovation nor stifle existing commerce or new business formation. We believe small business should be exempt from overly restrictive information storage and privacy requirements in order to avoid encumbering them with excessive regulatory obligations. A typical small business is not equipped to keep up-to-date or comply with stringent data use and privacy regulatory requirements. Therefore the OTA recommends an exemption for businesses based on amount of data collected, e.g. businesses that collect 15,000 records or less annually, or that have a database containing fewer than 25,000 records where the data is not sensitive or covered personal information.

The concepts of consumer notice and choice must keep pace with the evolving definition of privacy. Current privacy and data collection notices are overwhelming to the average consumer. As outlined in previous submissions, the OTA believes a simplified notice framework can address a majority of the effectiveness concerns, while providing flexibility for the businesses to optimize the notice to their business, industry and device used. A simplified yet comprehensive notice and choice framework will ensure that privacy notices are understandable to site visitors. Used in a uniform way across the internet it will allow consumers to easily compare data collection practices of various sites.

The OTA is encouraged by the recent innovation and business community leadership demonstrating consumers are increasingly being provided choices and control of the collection, use and sharing of their data. Innovative and robust controls are already being offered by OTA members such as TRUSTe, Evidon, eBay AdChoice™ and PreferenceCentral. With the recent announcement of integrated browser controls by major browser vendors including Google, Mozilla and Microsoft, in the very near future, consumers will have more privacy and tracking options than ever before.

A greater synchronization of privacy laws with Safe Harbor provisions and market-based incentives will encourage businesses to adopt more stringent privacy protection schemes. Having clear direction accompanied by a consistent application of incentives and safe harbors, will support businesses in fulfilling and exceeding privacy requirements without requiring excessive technical investments and legal and consulting fees.

As legislation and best practices develop, the concept of data stewardship and accountability is critical to protecting consumer confidence and online trust. Parties that collect such data must take steps to protect the data from abuse and protect their infrastructure from compromise. The OTA recommends all businesses create a data breach and loss response plan to prepare for the likelihood of a data incident. To help businesses in this area OTA recently released a 2011 Data Breach & Loss Incident Planning Guide. As prescribed in this resource, such plans help minimize the risk to consumers, business partners, and stockholders while increasing brand protection and the long-term viability of a business.<sup>1</sup>

Balancing privacy with security is another fundamental requirement in any public policy. For example Deep Packet Inspection (DPI) in the context of examining internet traffic and content attributed to a single

---

<sup>1</sup> <https://otalliance.org/resources/Incident.html>

or range of IP addresses may be acceptable when used exclusively for purposes of threat, security and fraud detection and mitigation purposes. Similar exemptions should apply to other technologies including persistent cookies, device fingerprinting and other technologies used to identify a machine or user transaction with a service in order to prevent fraud or abuse. It is important to recognize that anti-fraud, security and privacy enhancing technologies need to change rapidly over time. Conversely it is recognized such technologies may also be used for data collection and marketing purposes, with the intent to provide an enhanced online experience or other consumer benefits. In such case the user must be given clear and adequate understanding of the use including sharing with any third party, provide an explicit opt-in consent and ability to opt-out at any time. For example, a consumer may select such an offering to receive a discount on a purchase or save on their monthly ISP or carrier charges.

The OTA believes web analytics or similar types of research services, should be exempt from proposed legislation. Web analytics is generally performed by third party service providers for the purpose of providing insight into industry trends. This research helps inform industry investments in content and website feature development and facilitates efficient e-commerce and innovation. This activity occurs in accordance with industry best practices as the providers of such analytic services aggregate, weight, anonymize and otherwise process the collected data. Such processed data is not used to target any individual or device via on or off line advertising or alter content viewed by the individual based on his/her individualized behavior and activities.

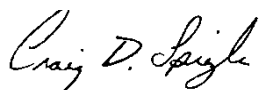
Embracing and applying online trust principles in the delivery of online services today will build online trust and bolster the long term vitality and sustainability of online services for the future. Doing so now, is not only good for the consumer, but also for businesses and our economy.

Although the comments in this document are independent of any trade organization or special interest group and represent the rough consensus of our membership, individual OTA members may not endorse every recommendation.

The following comments address selected questions listed in the preliminary Commerce report.

On behalf of OTA, we look forward to working with the Department of Commerce and other stakeholders to help increase online trust and confidence while enhancing innovation and the vitality of the internet.

Sincerely,



Executive Director and President  
Online Trust Alliance  
[Craigs@otalliance.org](mailto:Craigs@otalliance.org)

**1.a.** Should baseline commercial data privacy principles, such as comprehensive FIPPs, be enacted by statute or through other formal means to address how current privacy law is enforced? The patchwork of state laws and regulations that exists today makes compliance difficult for all but the very largest businesses. OTA supports baseline Federal privacy legislation in the belief it will aid companies to better understand requirements.

**1.b.** How should baseline privacy principles be enforced? Should they be enforced by non-governmental entities in addition to being the basis for FTC enforcement actions? The FTC may choose to implement its enforcement actions directly or through NGO authorities in the context of safe harbor provisions. In this way each industry may find marketplace options for certifying to the FTC framework and thus qualifying for safe harbor status. The NGO would be responsible for implementing oversight compliant to FTC guidelines.

**1.d.** Should baseline commercial data privacy legislation include a private right of action? A private right of action should only exist against companies that do not participate in an approved safe harbor program or meet safe harbor requirements. OTA believes that adopting a safe harbor program or requirement will incentivize businesses to proactively comply with privacy requirements and best practices. The safe harbor would not preempt any actions brought by a State Attorney General to protect the citizens of their state and uphold state laws.

**2.a.** What is the best way of promoting transparency so as to promote informed choices? Concise, easily discoverable and comprehensible notices promote both transparency and informed choices, discoverable at time and place of data collection. To this end, businesses should consider making policies and notices multi-lingual in order to ensure that users who speak English as a second language are adequately informed. For example, the OTA privacy policy is in both English and Spanish.<sup>2</sup>

**2.b.** What incentives could be provided to encourage the development and adoption of practical mechanisms to protect consumer privacy, such as PIAs, to bring about clearer descriptions of an organization's data collection, use, and disclosure practices? See 1c.

**2.i.** What incentives could be provided to encourage companies to state clear, specific purposes for using personal information? See Safe Harbor provisions and private right of action in 1c.

**2.p. / q.** Are technologies available to allow consumers to verify that their personal information is used in ways that are consistent with their expectations? Are technologies available to help companies monitor their data use, to support internal accountability mechanisms? Consumers are increasingly having choices and granularity in control of the collection, use and sharing of their data. Innovative and robust controls are already being offered by OTA members such as TRUSTe, Evidon, eBay AdChoice™ and PreferenceCentral. With the announcement of integrated browser controls by the major browser

---

<sup>2</sup> <https://otalliance.org/privacies.html>

vendors including Google, Mozilla and Microsoft, within months consumers will have more privacy and tracking options to control the collection and use of their data than ever before.

**4.b. How can the Commerce Department best encourage the discussion and development of technologies such as “Do Not Track”?** As new platforms and devices emerge, OTA does not believe there is a single tool or solution to provide consumer choice in the tracking and collection of their data and as such we need to help facilitate an environment which encourages innovation. “Do Not Track” has caused a great deal of confusion in the industry. Some businesses perceive “Do Not Track” as applying only to interest-based or behavioral advertising. Instead of addressing specific technologies, the Commerce Department’s discussion should focus on fundamental consumer concerns of data collection, usage/sharing and obligations. Distance the rhetoric from overloaded terms like “Do Not Track” which currently have several, competing definitions in the industry. The Commerce Department’s discussions should utilize procedures that allow a focused discussion on remedies and solutions with key stakeholders. The Commerce Department should consider ways of leveraging its unique role in the ecosystem as a convening authority for both private and public participants, e.g. the formation of a working group similar to how the Federal Communications Commission created the Communications Security, Reliability and Interoperability Council (CSRIC). The CSRIC provides recommendations from a broad yet representative group of stakeholders to help ensure, among other things, optimal security and reliability of communications systems, including telecommunications, media, and public safety.<sup>3</sup> Such a working group will facilitate an open and collaborative dialog.

**4.c. Under what circumstances should the PPO recommend to the Administration that new policies are needed to address failure by a multi-stakeholder process to produce an approved code of conduct?** The PPO should take action if there is an increased risk of harm to consumers (and business users) or when a business or industry fails to take necessary steps to protect consumers.

**5.d. Should non-governmental entities supplement FTC enforcement of voluntary codes?** Non-Governmental Organizations (NGO’s) can play an important role in supplementing the FTC’s enforcement (see answer to 1.b). NGO’s include alternative dispute resolution providers, auditors, Trustmark operators, regulatory safe harbor operators, in addition to the ultimate government regulator. NGO’s operate most effectively when they are free from real and perceived conflicts of interest. Independence is an important component of a self-regulatory framework. One method to help assure independence and mitigate perceived conflict of interests is to create a co-regulatory framework where the NGO must meet certain criteria (e.g. robust standards, monitoring of program members, dispute resolution) and then re-certify that the program continues to meet that standard. NGOs should also function to certify business solutions meet Safe Harbor requirement (as opposed to only certify Safe Harbor requirements are met through membership to a respective NGO’s solution or program). This multi-layered co-regulatory approach will provide enforcement alternatives. Global frameworks such as APEC are recognizing and are creating a multi-layered approach for using NGO’s to supplement enforcement, which is a must in any successful accountability system.

---

<sup>3</sup> <http://www.fcc.gov/pshs/advisory/csric/>

**5.e. At what point in the development of a voluntary, enforceable code of conduct should the FTC review it for approval? Potential options include providing an ex ante “seal of approval,” delaying approval until the code is in use for a specific amount of time, and delaying approval until enforcement action is taken against the code.** Early collaboration with the FTC is necessary to ensure that any adopted code is appropriate and practically enforceable. Early collaboration will also accelerate the development, approval, and implementation of any adopted requirements. However, businesses will need time to interpret, implement and adapt to any imposed requirements. Therefore, although the FTC’s input and collaboration should be obtained as early as possible, the FTC should delay approval until they are confident that they have thoroughly observed the impact and interpreted requirements of any new rules.

**5.f. What steps or conditions are necessary to make a company’s commitment to follow a code of conduct enforceable?** The safe harbor benefit is sufficient motivation, though working with NGO’s as certification authorities for such programs may offer incentives (see response to 1.b).

**7. What factors should breach notification be predicated upon (e.g., a risk assessment of the potential harm from the breach, a specific threshold such as number of records, etc.)?** The quickest way to render breach notifications ineffective is to require them for every benign, inconsequential violation. This situation is often referred to as “notification fatigue” and we observe it in many contexts. We do not want consumers to become numb to receiving a breach notification to the point where they no longer read the important ones. Therefore, we recommend notification requirements be limited to actionable information for the consumer where there is a real present danger of harm or risk (such as with data that enables identity theft). In addition, there should be uniform guidance for such notifications. The current breach regulatory landscape is a complex matrix that is driven by over 40 States, sectorial and industry specific requirements. This complexity is magnified by the fact that US law is not in synch with similar international breach requirements, including requirements imposed by Canada and the EU.

Redefining what constitutes covered and sensitive information will go a long way towards simplifying compliance. Data breach requirements should be applied uniformly to all entities including third party data providers that store and collect personal information, service and infrastructure providers alike, online and offline. Providing for action against businesses that fail to take reasonable security measures and fail to adopt self-regulatory guidelines, and increase supply chain accountability, will increase accountability and help to reduce consumer’s exposure to harm. Aiding businesses in developing an effective data security breach framework and readiness plan, the OTA recently published the 2011 Data Breach & Loss Incident Readiness Planning Guides and Anti-Malvertising Guidelines.<sup>4 5</sup>

---

<sup>4</sup> <https://otalliance.org/resources/Incident.html>

<sup>5</sup> <https://otalliance.org/resources/malvertising.html>