



February 15, 2011

Donald S. Clark, Secretary  
Federal Trade Commission  
Office of the Secretary  
Room H-113 (Annex W)  
600 Pennsylvania Ave., N.W.  
Washington, D.C. 20580

RE: FTC Staff Preliminary Report on Protecting Consumer Privacy - File No. P095416

Dear Mr. Clark,

Thank you for providing the Online Trust Alliance (OTA) 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 to mitigate privacy, identity, and security threats to online services, brands, organizations and consumers. Through our combined efforts our goal is to enhance online trust and confidence, business innovation and ultimately the vitality of online commerce.

OTA commends the Federal Trade Commission on this preliminary report. We believe this 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 enhancing the vitality of the internet.

Since this report was released we are encouraged by the response of the browser community, developing capabilities for consumers to help control the collection, sharing and use of personal data. In addition, innovative controls are now being offered by OTA members including TRUSTe, Evidon, eBay and PreferenceCentral. With this progress, in the months ahead consumers will have a broader choice of privacy and data collection controls than ever before.

Business accountability, data stewardship and data protection are equally important privacy issues. Any proposed privacy framework needs to address practical protection for consumer data from abuse, exploit, breach and loss without compromising security and fraud detection capabilities. Concurrently, OTA believes any changes to the regulatory landscape will also need to address the potential impact to ad-supported content services, innovation, and commerce.

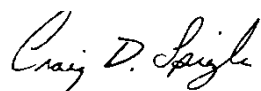
Innovative developments providing consumer notice and choice must also keep pace with the evolving definition of privacy. Current privacy and data collection notices may be overwhelming to the average consumer. OTA believes a simplified notice framework can address a majority of concerns while providing flexibility for businesses to optimize notice for their customers, industry and by technical innovations available. If guidance is provided, such privacy uniformity will allow consumers to easily compare data collection practices across various sites.

Embracing and applying online trust principles to the delivery of online services will build consumer trust and thereby increase the long term vitality and sustainability of online services. Such action by the online community is not only good for the consumer, but also the economy. It will extend the vitality of ad supported online services.

Although the comments in this document are independent of any trade organization or special interest group, they have been reviewed without objection by our general membership. Individual member companies of the OTA may not endorse every recommendation.

The following comments address selected questions as listed in the preliminary FTC Staff Report as well as OTA's submission to the Commerce Department for additional context. The OTA looks forward to continued collaboration with browser vendors, trade organizations, government agencies and advocacy groups in advancing the goal of consumer notice and choice. On behalf of the Board and membership of OTA we look forward to continued dialog on these issues.

Sincerely,



Craig D. Spiegle  
Executive Director and President  
Online Trust Alliance  
[Craigs@otalliance.org](mailto:Craigs@otalliance.org)  
<https://otalliance.org>  
+1 425-455-7400  
Cc: Board of Directors

Online Trust Alliances – Response to  
FTC Staff Preliminary Report on Protecting Consumer Privacy - File No. P095416

1. Are there practical considerations that support excluding certain types of companies or businesses from the framework – for example, businesses that collect, maintain, or use a limited amount of non-sensitive consumer data? As legislation is introduced or evolves, it should not hamper innovation nor stifle existing commerce or new business formation. We believe small businesses 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 comply or continually update 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 20,000 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 may not be entirely effective. OTA believes a simplified notice framework can address a majority of these concerns while providing flexibility for businesses to optimize notice to their customers. A simplified yet comprehensive notice and choice framework will ensure that privacy notices are understandable to site visitors. Used in a uniform manner across the internet it will allow consumers to easily compare data collection practices across of various sites.

In addition, 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.

7. Are there substantive protections, in addition to those set forth in Section V(B)(1) of the report, that companies should provide and how should the costs and benefits of such protections be balanced? Data governance and stewardship are critical to protecting data and consumer confidence. As legislation and best practices develop, data stewardship and governance are 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 and should be a fundamental part of a safe-harbor program. To help businesses in this area OTA recently released a 2011 Data Breach & Loss Incident Planning Guide. As prescribed, such plans help minimize the risk to consumers, business partners, and stockholders while increasing brand protection and the long-term sustainability of a business.

In addition, the OTA considers consumer education critical. Such education should occur at the time of data collection. Any FTC program in this area should focus on identifying and leveraging teachable moments such as detecting a user's unsecure browser and prompting them to upgrade, (see previous

submissions). Examples include campaigns from IAB “[Privacy Matters](#)”, the Center for Democracy & Technology “[Take Back Your Privacy](#)” effort.<sup>1</sup>

9. Is there a way to prescribe a reasonable retention period? What constitutes a reasonable retention period vary by industry, type of data and data usage. For example, SSL certificate providers are often required to keep documentation, including PII, for more than ten years. This time period may not be appropriate for other industries. Therefore, the OTA does not recommend a set retention period. Instead, businesses should use as a retention period that which is appropriate based on legitimate business or vertical-based regulatory requirements.
10. Should the retention period depend upon the type or the sensitivity of the data at issue? For example, does the value of information used for behavioral advertising decrease so quickly that retention periods for such data can be quite short? Appropriate retention periods vary by many factors. Any retention period should depend on the legitimate, proportional and appropriate needs of the business and the reason for collecting the information. As stated above, some businesses are required, by either industry standard or other regulation, to keep extremely sensitive data for long periods of time.
11. How should the substantive principles set forth in Section V(B)(1) of the report apply to companies with legacy data systems? Any framework should focus on reasonableness and general principles rather than specific requirements. A framework should not expect businesses to update legacy data systems in a manner that is unreasonable. Whether an update is reasonable depends on the risk and damage associated with data compromise and disclosure compared to the cost and effort of updating systems. Any company collecting PII should comply with the four principles described under Section V(B)(1). A data breach and disclosure of public information that occurs on a legacy system is no less damaging than one that occurs on a modern system. However, the risk and potential damage associated with non-PII is much lower and would not require legacy system updates.
14. How can the full range of stakeholders be given an incentive to develop and deploy privacy-enhancing technologies? See #43. The OTA recommends implementing a Safe Harbor from FTC for 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.
15. What roles should different industry participants – e.g., browser vendors, website operators, and advertising companies – play in addressing privacy concerns with more effective technologies. OTA believes having an open and constructive dialog with all stakeholders. Industry participants share the responsibility of respecting the consumer’s privacy and data collection intent by providing intuitive information to help allow them to make an informed choice. As new technologies and persistent controls are integrated into browsers, such controls need to also educate consumers on the value proposition they received from ad supported services and the impact to opting into the use of such controls. (see Comments #41)

---

<sup>1</sup> <https://otalliance.org/resources/initiatives.html#PRIVACY>

16. Is the list of proposed “commonly accepted practices” set forth in Section V(C)(1) of the report too broad or too narrow? OTA believes the list of commonly accepted practices will evolve and therefore is a reasonable starting point as long as the list is governed in such a way as to remain flexible and open to change as industry practices evolve. The number of legitimate business purposes for collecting and using information is as great as the number of industries. For example, registrars may collect information to validate the individual’s identity when applying for a new TLD domain. Although this area could qualify as product and service fulfillment, the actual practice varies greatly from the provided description. We recommend the listed categories be described in more general terms and be flexible to allow for future “commonly accepted practices”.
19. Even if first-party marketing in general may be a commonly accepted practice, should consumers be given a choice before sensitive data is used for such marketing? Users should be provided the option and choice before sensitive data is collected and used for non-transactional purposes including marketing.
20. Should first-party marketing be limited to the context in which the data is collected from the consumer? Business should only use information for previously disclosed purposes. However, broad disclosures are acceptable provided the consumer is aware of the disclosure and such disclosure is discoverable and comprehensible to the average user or customer, i.e. written in clear, plain English.
23. Should marketing to consumers by commonly-branded affiliates be considered first-party marketing? OTA defines commonly-branded affiliates as those where the affiliate shares common ownership and not in the context of marketing affiliates who may share revenue for the provision of data with a company for which there is no common ownership. OTA believes there are scenarios where such affiliate marketing may be considered first party marketing. This assumes that affiliate’s products are related and data usage is directly related to the initial first party and each affiliate has materially the same privacy and data use policies. Where two affiliated entities share neither a common name nor offer similar services, consumers cannot be expected to know or intuitively understand the affiliated nature of the entities. From a consumers’ perspective, some affiliated entities may appear indistinguishable from unaffiliated entities creating a privacy “loophole”. Therefore consumer expectations regarding the disclosure of their information cannot be met when there is no clear, identifiable relationship between the entity collecting the information and the entity to which they are disclosing the information. It should be noted this issue could be rectified by a clear and conspicuous disclosure of the data transfer or sharing of information.
24. What is the most appropriate way to obtain consent for practices that do not fall within the “commonly accepted” category? The framework should allow any reasonable practices. This encourages innovation and new ideas. For example, businesses might obtain data sharing consent through an opt-in subscriber agreement and share information with allowed third parties that have similar privacy policies which address the fundamental areas of data collection, data usage and data sharing. At a minimum, such notices must be clear, conspicuous and in plain English.
25. Under what circumstances (if any) is it appropriate to offer choice as a “take it or leave it” proposition, whereby a consumer’s use of a website, product, or service constitutes consent to the company’s information practices? “Take it or leave it” options must be grounded in reasonableness, appropriateness, and proportionality in the data requested. Otherwise this will become the “safe haven” of aggressive data collectors. Depending on the context, a “take-it-or-leave it” proposition is appropriate under certain circumstances, e.g. if opting-out would cripple the sites ability to provision service properly due to compromised security and anti-fraud mechanisms or other reasons including but not limited to financially crippling the sites ability to provide service appropriately.

29. What additional consumer protection measures, such as enhanced consent or heightened restrictions, are appropriate for the use of deep packet inspection? Deep Packet Inspection (DPI) and other technologies when used in the context of examining internet traffic and content attributed to a single or range of IP addresses may be acceptable when used for purposes of threat, security and fraud detection and vulnerability mitigation purposes. Similar exemptions should apply to persistent cookies, device fingerprinting and other technologies used to identify a machine or user transacting with a service in order to prevent fraud or abuse. The use of DPI and related technologies may also be permissible when consumers have the ability to opt-in and receive appropriate and proportional quantifiable benefits in return. Providing that consumers understand what data is being collected or examined, who it is being shared with, how it is being used and have the ability to opt-out at any time and other protective safeguards should eliminate much of the risk. However, it is important to recognize that technologies change rapidly over time. Only the principles of use and obligation aligned to FIPPs remain static, and therefore FTC must concentrate oversight on use and obligation models and evaluate all technologies and practices against those. OTA recommends that the type and amount of consumer information collected and how it is used, not the technology used to collect such information be the focus for any consumer protection measures. (See OTA recommended ISP best practices)<sup>2</sup>
32. Is it feasible for data brokers to provide a standardized consumer choice mechanism and what would be the benefits of such a mechanism? A standardized choice mechanism that established a floor, but not a ceiling, for policy description may accelerate user comprehension, utilization, and comparability. However, any standardized set of requirements for choice mechanisms may need to vary by industry and data usage, or may even vary on a localized level, site-to-site depending on what additional disclosures a site is required to make in addition to those captured by the standardized choice mechanism. Standardized choice mechanisms and standardized privacy disclosures may allow consumers to more easily compare business practices and make informed decisions. See OTA proposed framework submitted to the FTC in December 2009.<sup>3</sup>
33. How should a universal choice mechanism be designed for consumers to control online behavioral advertising? The OTA supports choice mechanisms with baseline requirements including transparency and discoverability. Business can offer choice mechanisms to consumers directly through customized web-based solutions, trade organizations, third party add-ons, and / or integrated within a browser. Adopted choice mechanisms may go above any baseline requirements and add consumer controls and granularity. Because of this, the OTA does not support a single universal choice mechanism, but we do support uniform common requirements for choice mechanisms. Over time consumers will migrate to the choice mechanisms that best address their needs and requirements.
34. How can such a mechanism be offered to consumers and publicized? Based on the implementation, web sites, and advertisers have multiple alternatives. For example browsers can make integrated privacy controls and options available in a “First Run Scenario” or sites could make them discoverable on log-in sessions.<sup>4</sup> The controls should be integrated in a manner that makes them easy to discover and activate. Privacy controls may also inform consumers about the value of ad-supported content and the potential impact that the controls will have on their online experience and

---

<sup>2</sup> [https://otalliance.org/resources/initiatives.html#ISP\\_BEST\\_PRACTICES](https://otalliance.org/resources/initiatives.html#ISP_BEST_PRACTICES)

<sup>3</sup> [https://otalliance.org/privacy\\_demo.html](https://otalliance.org/privacy_demo.html)

<sup>4</sup> “First Run Experience” is the starting screen that is presented to a user the first time an application is opened or used. They provide the choice of selecting default or recommended options.

security. Such mechanisms need to be clear, conspicuous, intuitive, and have more than a single access point. Furthermore, a one-time explanation to a consumer is not always sufficient. The concept of continuing disclosure and consent so that users know and remember what is happening on an ongoing basis also needs to be included in the mechanism. What's important is that innovation will continue to drive best-of-breed solutions<sup>5</sup>.

39. How many consumers, on an absolute and percentage basis, have utilized the opt-out tools currently provided? The OTA does not believe an accurate answer to this question is available. Any framework should balance the upgrade migration of an operating system or browser, discoverability of the specific option and resulting rate of utilization. Second, the impact needs to delineate the resulting usage from search, first party and third party advertising.<sup>6</sup>
40. 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? It is important to validate the scope and potential of any large scale consumer adoption, and to understand the factors that may drive such usage. The possible actions by publishers and advertisers will likely vary. It is important to consider the historic impact when past privacy and security technologies were enabled by default to determine why consumers will be impacted. In response to intrusive popup ads and malicious email, browsers and email clients, blocked pop-up ads and images and links in email by default. The net impact on ad revenues has been positive as new business models and services have emerged and revenues have shifted.

Other potential impacts upon consumers include third-party advertising migrating to first-party interest based advertising, advertising shift to contextual advertising, and / or sites may move towards fee-based subscription models. Sites experiencing a negative impact on ad revenues may choose to increase space allocated to advertising or provide opted-out users with limited content, delayed content access and / or limited site functionality.

41. In addition to providing the option to opt out of receiving ads completely, should a universal choice mechanism for online behavioral advertising include an option that allows consumers more granular control over the types of advertising they want to receive and the type of data they are willing to have collected about them? The OTA believes granular controls are necessary in order to cover the vast array of possible data collection practices, use, and obligations as it only applies to interest based or behavioral targeted advertising. Granular control can include options to limit the way businesses can collect or share data without eliminating the practice altogether. Innovative options and controls are already being offered by OTA members such as TRUSTe, Evidon, eBay and PreferenceCentral. It is anticipated many more options and controls will be developed in the near future. Therefore OTA supports uniform guidance from FTC, but not a specific universal choice mechanism as per our previous answers to similar "universal choice" questions.
42. Should the concept of a universal choice mechanism be extended beyond online behavioral advertising and include, for example, behavioral advertising for mobile applications? Any adopted framework and choice mechanism requirement set needs to be flexible in order to keep pace with technological innovation and must apply in all data collection contexts: online, mobile, and offline. Such controls need to apply for any data collection, tracking, share and use. Choice mechanisms need to be technology neutral and apply equally to online, offline and mobile applications.

---

<sup>5</sup> <http://announcements.ebay.com/?s=adchoice>

<sup>6</sup> <http://marketshare.hitslink.com/browser-market-share.aspx?qprid=2>

43. If the private sector does not implement an effective uniform choice mechanism voluntarily, should the FTC recommend legislation requiring such a mechanism? The OTA supports offering incentives for meaningful self-regulation of information collection, use, and sharing. One possible incentive is to create a self-regulatory safe-harbor excluding private-right of action and FTC enforcement action from participants in an approved program
44. What is the feasibility of standardizing the format and terminology for describing data practices across industries, particularly given ongoing changes in technology? Uniform guidance and requirements for these mechanisms from FTC is welcome. But a standardized format should not be expected to be any more successful / usable by industry than the standard format provided by GBLA<sup>7</sup>. To the extent standardization is required it should involve the FTC but be conducted within existing standard setting bodies to generate consensus standards. Specifically, the work of W3C on P3P should at least be considered before any new machine-readable standardization is introduced.<sup>8</sup>
45. How can companies present these notices effectively in the offline world or on mobile and similar devices? Notices need to be tailored for the device on which they will be displayed. FTC must be mindful of this rapidly changing, multi-platform environment and not establish any brittle requirements that would stifle usability innovation. Presenting notices on mobile devices is extremely important as they have rapidly become the “device of choice” by millions of users worldwide and are becoming tightly integrated into marketing initiatives. Businesses are adopting and using multi-channel data collection procedures and as such, offline disclosures need to be presented to users. Already new and innovative means of notice are being created. Just-in-time notice and layered notices will need to evolve. Regardless of the mechanism organizations that use layered notices, etc. such organization should still make available from some resource the whole policy in a comprehensible, plain language format. In addition the concept of a continuing disclosure and consent may be used so that users know and remember what is happening on an ongoing basis. This should be considered a best practice. As new devices such as smartphones and other devices become the “device of choice”, such notices may need to address the visual limitations of an aging population.<sup>9</sup>
46. Should companies increase their use of machine-readable policies to allow consumers to more easily compare privacy practices across companies? To the extent this does not interfere with the efficacy of their notification and assuming there is a positive net-effect by introducing machine-readable policy, i.e. standards supported across the web, then the OTA supports their use. Machine-readable policies hold the promise of increasing awareness, educating consumers and aiding them to make informed decisions and make it easier for browsers to implement privacy controls.

---

<sup>7</sup> <http://www.sec.gov/rules/final/2009/34-61003.pdf>

<sup>8</sup> <http://www.w3.org/P3P/>

<sup>9</sup> <http://www.agelight.com/webdocs/designguide.pdf>

47. Should companies be able to charge a reasonable cost for certain types of access? The OTA supports a model where users are able to access and update their personal information for accuracy. A well-known model with both advantages and disadvantages is the one used today in the EU. In the EU, companies are allowed to charge users a nominal fee to partially off-set operational costs. But there is controversy regarding the effectiveness of this method. How many users actually even know this is there? Are the requests legitimate or nefarious? Is it achieving its goals or is it only raising the cost on consumer access to online services? FTC is advised to not rush into this model without further analysis.
56. How can individual businesses, industry associations, consumer groups, and government do a better job of informing consumers about privacy? See question #57.
57. What role should government and industry associations have in educating businesses? The OTA supports increased collaboration among all interested parties, including the private sector, NGOs, and trade organizations. The FTC should review the lessons learned from the recent “Stop Think Connect” security education initiative from the Department of Homeland Security. A “Smokey the Bear” campaign on consumer privacy could be created using scalable and reusable materials including web graphics, customizable collateral and public service announcements (PSA’s).<sup>10</sup>

---

<sup>10</sup> <http://www.dhs.gov/files/events/stop-think-connect.shtm>

## **Appendix A**

### **OTA Submission to the US Department of Commerce**

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



January 28, 2011

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>11</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 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

---

<sup>11</sup> <https://otalliance.org/resources/Incident.html>

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.

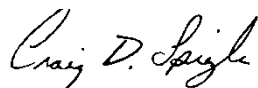
Embracing and applying online trust principles in the delivery of online services today will build online trust and bolster the long term vitality and sustainability of online services for the future. Doing so now, is not only good for the consumer, but also for businesses and our economy.

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>12</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>12</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>13</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

---

<sup>13</sup> <http://www.fcc.gov/pshs/advisory/csric/>

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.

**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>14 15</sup>

---

<sup>14</sup> <https://otalliance.org/resources/Incident.html>

<sup>15</sup> <https://otalliance.org/resources/malvertising.html>