



Via electronic email to [privacy-noi-2010@ntia.doc.gov](mailto:privacy-noi-2010@ntia.doc.gov)

June 14, 2010

Office of the Secretary  
National Telecommunications and Information Administration  
International Trade Administration  
U.S. Department of Commerce  
1401 Constitution Avenue, NW  
Room 4725  
Washington, DC 20230

Re: Department of Commerce, Notice of Inquiry  
Information Privacy and Innovation in the Internet Economy  
Docket No. 100402174-0238-02

The Online Trust Alliance (OTA) hereby submits its comments to the Department of Commerce's Notice of Inquiry, dated April 20, 2010.

OTA is encouraged by the dialog regarding the evolving role and importance of privacy protections and the way in which it balances the impact to the vitality of online services and commerce. Balanced legislation and market based incentives are needed to provide a framework for legitimate businesses to follow which neither imposes an unreasonable burden, nor prevents aggressive enforcement towards bad actors.

We agree on the importance of innovation to not only provide consumer choice and control, but to re-define it so it is intuitive and comprehensible. Ensuring public trust and confidence is the foundation for participation and the growth of the internet. We recognize this means the importance of moving from a harm based model to one of meeting evolving consumer privacy expectations.

For background, OTA was founded in late 2004 to address the global spam problem and the lack of standards and practices to help detect forged email. In the past six years, OTA has grown significantly. As an IRS approved 501c6 member based non-profit, we represent the broad internet ecosystem and are not beholden to any special interest group. OTA membership is comprised of over 70 business, industry and technology leaders who share our mission to enhance online trust while promoting business practices and technologies which support the vitality of ecommerce and online services. Through our members and organizational partners in over a dozen countries, OTA represents over 1 million businesses and 750 million consumers worldwide, <https://otalliance.org>.

OTA is active worldwide working with US agencies such as the Departments of Treasury and Justice, the White House, and the Federal Trade Commission. Supporting our global view, Internationally OTA is members of the London Action Plan, (LAP), German Internet Society (eco), Dutch Email Marketing Association and other international efforts.<sup>1</sup>

This past twelve months has marked several OTA milestones including the publishing of:

- Proposed Data Collection & Privacy Statement [https://otalliance.org/privacy\\_demo.html](https://otalliance.org/privacy_demo.html)
- Online Principles & Business Guidelines <https://otalliance.org/resources/principles.html>
- Data Loss & Breach Readiness Guide <https://otalliance.org/resources/Incident.html>
- Online Safety Honor Roll [https://otalliance.org/news/releases/2010honor\\_roll.html](https://otalliance.org/news/releases/2010honor_roll.html)
- Compliance & Online Trust Training programs held in San Francisco, Philadelphia, Singapore, Copenhagen, Amsterdam & Germany.
- Submissions to the Privacy Act staff discussion draft from Rep Boucher & Stearns [https://otalliance.org/docs/OTA\\_Privacy%20Bill\\_finalx.pdf](https://otalliance.org/docs/OTA_Privacy%20Bill_finalx.pdf)
- National Strategy for Secure Online Transactions (NS OST)

---

In response to the Department's Notice of Inquiry, the following is a summary of comments in areas most relevant to OTA members and representative of our members' subject matter expertise.

#### US Privacy Framework

OTA supports the concept of a standard and comprehensible set of laws and statues which enables businesses to understand and implement policies required for compliance. The recent staff discussion draft privacy act from Representatives Boucher and Stearns is a positive effort towards this goal. Today there is a patchwork of some 44 state laws and regulations which by their very nature become insurmountable for businesses to comply with. With inconsistent terminology, all but the largest businesses are often confused and may unknowingly find themselves out of compliance.

As the definition of privacy has evolved, so must the concept of notice and choice. Today privacy and data collections notices are typically overwhelming to the average consumer. As outlined in our submission to Representative Boucher and Stearns, we suggest the importance of moving to an enhanced notice framework, written for the intended site visitor and comparable from one site to another.<sup>2</sup>

We believe greater synchronization of such laws with Safe Harbor provisions and market based incentives are essential. We need to aid businesses who in general want to fulfill privacy requirements, but this can only be accomplished with clear direction in a consistent manner across jurisdictions without the need of excessive technical investments, legal and consulting fees.

---

<sup>1</sup> London Action Plan <http://www.londonactionplan.org/>

<sup>2</sup> OTA Standardized Privacy & Data Collection Statement [https://www.otalliance.org/privacy\\_demo.html](https://www.otalliance.org/privacy_demo.html)

### Sectoral Privacy Laws & Guidelines

As data collection expands beyond the PC to mobile devices, the appending of data files and information grows and businesses expand internationally, the complexity of navigating laws and legal frameworks with overlapping jurisdictions is impacting businesses of all sizes. In the US alone, regulations are being directed by the Federal Trade Commission, Federal Communications Commission, FDIC with specific requirements under HIPAA, FCRA, COPPA and others.

Internationally “Safe Harbor” is critical for US business to avoid experiencing conflicts with the EU and the risk of facing prosecution under their respective privacy laws. Continued support of safe harbor certification will help assure that EU organizations recognize complying US businesses provide “adequate” privacy protection. Combined, efforts to reconcile these sectoral requirements must be supported, providing a means for US businesses to operate competitively and globally.<sup>3</sup>

### New Privacy Enhancing Technologies

OTA sees significant promise and urgency to spur the development of integrated privacy enabling technologies in browsers and web sites. While today many of these are available via “add-ins”, we believe they need to be integrated into all browsers and web sites. They need to be discoverable, with an intuitive explanation of their purpose, value-proposition and impact. We believe as a fundamental design requirement, users must be able to enable them at will and have them remain persistent if so selected. At the same time when a user visits a site when such features or technologies enabled, we believe it is reasonable to provide the sites they are visiting the ability to detect such usage. This is essential because such controls have the ability to potentially disable analytics and disrupt legitimate business models which rely on such data collection.<sup>4</sup>

Since the passage of CAN-SPAM we have seen several efforts of self-regulation emerge providing users and businesses preference controls. For example the development of an Internet Engineering Task Force (IETF) standard (RFC 2369) for the inclusion of an unsubscribe header has enabled the majority of email providers and email service providers to provide users a safer and more convenient mechanism to unsubscribe, versus relying on the unsubscribe footer.<sup>5</sup> When such a header is detected by the ISP and the email is verified coming from a known sender, an unsubscribe button is enabled in the email user interface.<sup>6</sup>

Other examples including the development of Extended Validation SSL Certificates (EV SSL), and the adoption of suppression list encryption (practices endorsed by OTA), Feedback Loops (FBLs) and Abuse Reporting Format (ARF) supported by ISPs worldwide. Further examples include email authentication technologies such as SPF, Sender ID (SIDF) and Domain Keys Identified Email (DKIM), which provide ISPs, government and corporate networks added control and ability to protect user’s inboxes from spam, forged and malicious email.<sup>7 8</sup>

---

<sup>3</sup> [http://www.export.gov/safeharbor/eg\\_main\\_018236.asp](http://www.export.gov/safeharbor/eg_main_018236.asp)

<sup>4</sup> To be provided via the “user string” or other mechanism. Vast majority if not all browsers provide baseline data including the browser version to the site to optimize page rendering. Specific to the use of privacy features, Internet Explorer 8 provides sites the ability to know if InPrivate Filtering is on. This is provided via a JavaScript API, [http://msdn.microsoft.com/en-us/library/dd425013\(VS.85\).aspx](http://msdn.microsoft.com/en-us/library/dd425013(VS.85).aspx).

<sup>5</sup> Required for all OTA members who send commercial email.

<sup>6</sup> Supported by Google Gmail, Microsoft Hotmail, Yahoo mail and others.

<sup>7</sup> OTA email authentication and industry resources <https://otalliance.org/resources/authentication/index.html>

Combined these are just a few examples of how industry and business are working together. These and other recommendations comprise the OTA Online Principles & Guidelines, a set of voluntary best practices.<sup>9</sup>

Companies are wrestling with the balance of providing users granular control and supporting their business objectives while at the same time trying not to overwhelm users with too many choices. Going forward such efforts need to be intuitive and consumer centric by design. Businesses need to focus on teachable moments, at the point of data collection, to help prevent unintended data collection from occurring.

Today we are starting to see similar efforts in the area of behavioral targeting, preference management and reputation systems. OTA member companies such as Authentication Metrics, Better Advertising, Lashback, Return Path, True Domain, TRUSTe and UnsubCentral are to be commended for their solutions which help address these issues. While it is too early to tell where these solutions, collaborative efforts and standards will land, they represent a strong commitment by business and industry towards consumer and privacy protection.

We believe through the promotion of research, public and private partnerships, and incentives that we can most effectively spur the development of such technologies and services. To support this goal we recommend any such policy and regulations should embrace market incentives.

#### Small & Medium Business Entities & Start Up Companies, (SMB)

It is essential policy recommendations take into the consideration the impact to SMBs. SMBs are the majority of businesses and often the most ill prepared to navigate the complex set of rules, laws and regulations. OTA annual score cards reports and research indicates the vast majority are unprepared to address privacy, data governance, and marketing or security issues.<sup>10</sup>

While such legislation is important, it can also be a barrier and limit new business formation, ultimately reducing market competitiveness and consumer choice. Since these emerging entities may become tomorrow's market leaders, we need to support the development and availability of resources and services to enable them to be compliant without imposing undue burden.

OTA is working with the US Chamber of Commerce, the Direct Marketing Association, OTA member companies and other stakeholders to help provide guidelines, prescriptive advice, resources and affordable training to small businesses and governmental agencies. Supporting this objective, OTA will be providing half-day training as part of the OTA Academy in September 2010 including CAN-SPAM compliance and email authentication.<sup>11 12</sup>

---

<sup>8</sup> Submitted by OTA and currently recommended for all governmental agencies in the White House draft National Strategy for Secure Online Transactions (NS SOT).

<sup>9</sup> OTA Online Principles & Business Guidelines published Dec 2009,  
<https://otalliance.org/resources/principles.html>

<sup>10</sup> April 2010 Online Safety Scorecard [https://otalliance.org/news/releases/2010honor\\_roll.html](https://otalliance.org/news/releases/2010honor_roll.html)

<sup>11</sup> OTA Resource Center <https://otalliance.org/resources/index.html>

<sup>12</sup> 2010 Online Trust & Cybersecurity Forum Sept 22/24 Georgetown University  
<http://guest.cvent.com/EVENTS/Info/Summary.aspx?e=a8dc654f-32fd-4cb5-8ed5-a518f88dbd43>

As a leading non-profit, we are committed to aiding in these efforts and encourage assistance and funding be made available to qualified non-governmental organizations to make such efforts and resource more readily available to all businesses of all sizes and across all industry segments.

With the advent of cloud based services, SMBs are increasingly relying on service providers to provide integrated privacy, security and data governance enabling technologies. Leading email service providers today provide turnkey solutions for managing consumer email preferences including, and we need to look for similar privacy enhancing efforts.

Having exemptions for collection of covered information for small business is essential, but only with safeguards to prohibit data sharing and efforts to circumvent the exemptions. As recommended in OTA comments to the draft privacy bill from Representatives Boucher and Stearns, we recommended entities that collect less than 15,000 records annually be exempt from such regulations.<sup>13</sup>

#### The Role of Government and the Department of Commerce

OTA applauds the efforts of the Department and the long standing international thought leadership. We encourage the Department to continue its efforts to advance U.S. competitiveness by encouraging government and the private sector to work together to demonstrate U.S. leadership in developing and implementing best practices. Efforts to proactively engage businesses in this dialog will help assure the long term competitiveness and vitality of the market place.

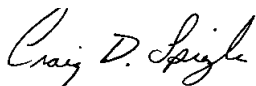
The free flow of information on the Internet is important to our Nation's fundamental democratic values, as is the protection of individual's privacy and business data. Without both, we significantly risk disenfranchising millions of consumers and segments of the population who increasingly rely on the internet for their communication services, information, education and employability.

Thank you for the opportunity to meet last month and provides this input. In summary, we believe that consumers and the internet economy at large will benefit by the consolidation of privacy and data breach regulations, and by the support of market based incentives, self-harbor and technology innovation which support the needs of all business segments from SMBs to the Fortune 500.

OTA looks forward to continuing collaboration with the Department of Commerce on this and other initiatives and work streams including cybersecurity, protection of intellectual property and the free flow of information.

Working together we can help ensure the vitality of online services and commerce.

Respectfully,



Craig Spiegle  
Executive Director  
Online Trust Alliance

Cc: OTA Board of Directors & Steering Committee

---

<sup>13</sup> OTA submission dated June 4, 2010 [https://otalliance.org/docs/OTA\\_Privacy%20Bill\\_finalx.pdf](https://otalliance.org/docs/OTA_Privacy%20Bill_finalx.pdf)