Submission for FTC Privacy Roundtable 2

Updated December 23, 2009

Federal Trade Commission
Office of the Secretary, Room H-135
600 Pennsylvania Avenue NW, Washington, DC 20580
Re: Privacy Roundtables – Comment, Project No. P095416

Dear Commissioners,

The Online Trust Alliance (OTA) welcomes the opportunity to submit comments and to speak at the upcoming FTC privacy roundtable event in Berkeley, California on January 28th.

OTA's mission is to support the online trust community promoting business practices and technologies to enhance consumer trust and the long-term vitality of interactive marketing, ecommerce and governmental and financial online services.

OTA represents the broad Internet ecosystem including: ecommerce sites, financial institutions, technology providers, marketing service providers, ISPs and numerous global NGO organizations. Governed by a representative Steering Committee and Board, we are, by design, not beholden to any single business sector or interest group, assuring balanced perspectives and recommendations

OTA supports the Commission's goal of determining how consumers may use and benefit from modern technologies while retaining robust privacy protections. To this end, OTA released a comprehensive set of Principles and Guidelines this fall addressing consumer choice and control of personal and sensitive data collected.[1] OTA believes consumers should be provided clear notice across all online activities. Examples include a site's terms of use, a site's privacy policy and email practices when opting-in or subscribing for email.

As information breaches continue to afflict businesses and consumers, we believe it is imperative to expand the scope of data protection to not only include Personally Identifiable Information (PII), but to broaden the definition to include sensitive information and other elements of our digital life styles such as digital recordings and images. Such a definition is consistent with the earliest privacy concerns expressed by Justice Brandeis nearly 90 years ago.[2]

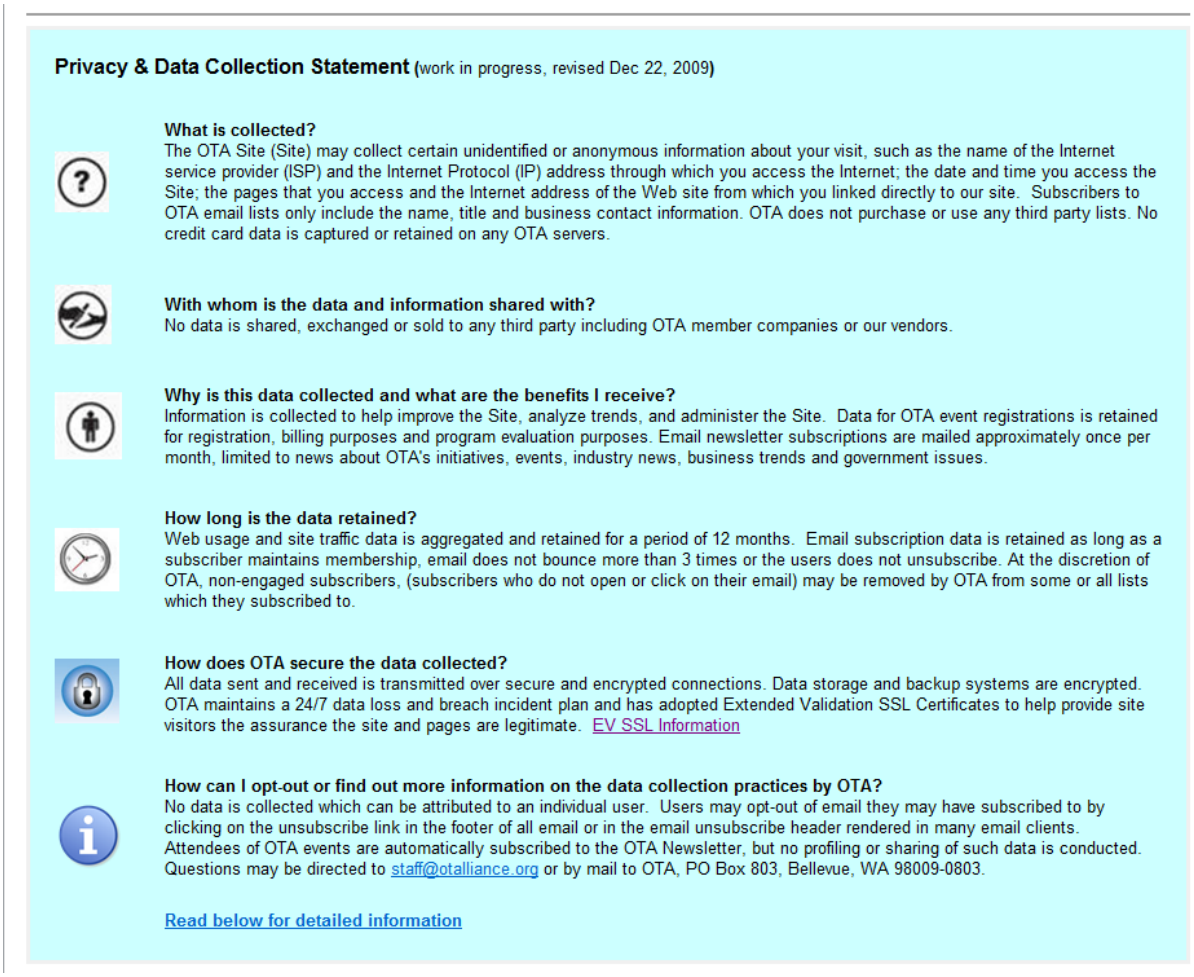
[1] https://www.otalliance.org/resources/principles.html
[2] http://www.brandeis.edu/legacyfund/bio.html

"Privacy & Data Collection Statement"

Not unlike a health department rating for a restaurant, an automotive "Monroney" Sticker or a nutrition label on a food product, a standardized framework is required to enable consumers to make informed choices regarding any data collection during online activities.[3, 4]

The benefits of such a framework includes but is not limited to providing consumers: 1) a concise and comparative view to how sites will use their data; 2) an understanding of the value they are receiving, and 3) an ability to manage their data that they submit or which may have previously been collected. Businesses benefit by: 1) consumers realizing an increased trust and confidence in their brand and 2) an ability to differentiate their business practices from their competition.

Working with our membership, OTA has published a conceptual framework referred to as the Privacy & Data Collection Statement. We are proposing such a standardized disclosure be required for all sites, online services, as well as retail points of collection which collect and track consumer behavior data. Such statement with recognizable icons would be used in conjunction with existing layered notices.[5, 6]



Privacy & Data Collection Statement (work in progress, revised Dec 22, 2009)

What is collected?
The OTA Site (Site) may collect certain unidentified or anonymous information about your visit, such as the name of the Internet service provider (ISP) and the Internet Protocol (IP) address through which you access the Internet; the date and time you access the Site; the pages that you access and the Internet address of the Web site from which you linked directly to our site. Subscribers to OTA email lists only include the name, title and business contact information. OTA does not purchase or use any third party lists. No credit card data is captured or retained on any OTA servers.

With whom is the data and information shared with?
No data is shared, exchanged or sold to any third party including OTA member companies or our vendors.

Why is this data collected and what are the benefits I receive?
Information is collected to help improve the Site, analyze trends, and administer the Site. Data for OTA event registrations is retained for registration, billing purposes and program evaluation purposes. Email newsletter subscriptions are mailed approximately once per month, limited to news about OTA's initiatives, events, industry news, business trends and government issues.

How long is the data retained?
Web usage and site traffic data is aggregated and retained for a period of 12 months. Email subscription data is retained as long as a subscriber maintains membership, email does not bounce more than 3 times or the users does not unsubscribe. At the discretion of OTA, non-engaged subscribers, (subscribers who do not open or click on their email) may be removed by OTA from some or all lists which they subscribed to.

How does OTA secure the data collected?
All data sent and received is transmitted over secure and encrypted connections. Data storage and backup systems are encrypted. OTA maintains a 24/7 data loss and breach incident plan and has adopted Extended Validation SSL Certificates to help provide site visitors the assurance the site and pages are legitimate. EV SSL Information

How can I opt-out or find out more information on the data collection practices by OTA?
No data is collected which can be attributed to an individual user. Users may opt-out of email they may have subscribed to by clicking on the unsubscribe link in the footer of all email or in the email unsubscribe header rendered in many email clients. Attendees of OTA events are automatically subscribed to the OTA Newsletter, but no profiling or sharing of such data is conducted. Questions may be directed to staff@otalliance.org or by mail to OTA, PO Box 803, Bellevue, WA 98009-0803.

Read below for detailed information

[3] http://www.bing.com/reference/semhtml/Automobile_Information_Disclosure_Act_of_1958

[4] http://www.fda.gov/Food/LabelingNutrition/ConsumerInformation/ucm078889.htm

[5] https://www.otalliance.org/privacy_demo.html

[6] Other approaches for a standardized notice include research and testing by Carnegie Mellon University utilizing a graphic representation, as proposed by, http://cups.cs.cmu.edu/privacyLabel/

Browser Controls

Today most browsers provide features and settings to aid consumers in maintaining their privacy though their implementation and usability are limited, and discoverability is extremely low. While third party privacy protection add-ins are available, their use is generally for advanced users. When engaged, such usage runs the risk of diminishing the online experience and interfering with a site's ability to drive advertising related revenues.[7]

OTA encourages browser vendors to continue to innovate for the benefit of the consumer, while providing web sites the ability to know when such features are enabled. This visibility helps sites better determine the impact to ads not being served and what content and access should or should not be provided. In order to achieve consumer control, these features are recommended to be 1) integrated into the browser, 2) discoverable, 3) intuitive and 4) provide teachable moments that all segments of users can easily comprehend.

At the same time, we need to be careful that we maintain balance providing consumers both awareness and choice. OTA believes such features should not be "on by default" as doing so would likely create unintended consequences. For example, sites may choose to limit access or to require consumers to provide payment for the content or services they wish to receive. This risk of doing so may disenfranchise segments of the population who cannot afford to pay.

Teachable Moments

Consistent with the OTA principles we are recommending all commence, financial services and government sites encourage users to upgrade their browsers. Users of outdated browsers lack essential data security and privacy controls, as well as adequate malware and phishing protection, which present a significant threat to their personal data and privacy. Through international testing in Singapore and Demark, banks are identifying the user's browser and respective version via the user string that sites use to optimize page rendering. When detecting the use of an insecure browser version at log in, users are encouraged to upgrade. While still in pilot testing, results are promising demonstrating "trust dividends" for both the consumers and brands who are adopting this practice.

[7] Options such as AdBlock Plus http://adblockplus.org and NoScript http://noscript.net/ are primarily designed for blocking advertising and adding security controls to prevent malicious code from executing. NoScript is designed primarily for security purposes allowing active content (such as Java) to run only from sites you trust, and help to protect against cross site scripting, (XSS), Clickjacking and other malicious threats. OTA does not suggest they be used since for two primary reasons; 1) increasingly this functionality is being integrated into leading browsers such as Google Chrome, Microsoft Internet Explorer and Firebox 3.5, and 2) such add ons typically interfere with content and third party information from being served. Examples include weather, stock and other dynamic third party content and news. While it has yet to be tested legally, some have suggested such usage is a form of site visitors "trespassing" and such tools illegally interferences with a site's ability to conduct commerce.

In summary, through a combination of standardized notice, integrated browser controls and teachable moments, we can contribute to the FTC goals, while helping to maximize online trust and confidence and the long-term vitality of online marketing, advertising and consumer services.

Representing OTA, I welcome the opportunity to participate in the January 28th Roundtable. I am prepared to share my decade plus experience at Microsoft where I was most recently the Director of Privacy and Security for Microsoft Internet Explorer. In this role I was responsible for the introduction of several privacy enabling features including the Microsoft's Phishing Filter, Smart Screen Filter, InPrivate Browsing, and InPrivate Filtering. Representing OTA membership including leading commerce sites, financial institutions, technology providers, NGOs and government organizations, I am prepared to provide the Commission a balanced and realistic view of the issues, constraints and possibilities.

Respectively Submitted

Craig Spiezle, Chairman and Executive Director
Online Trust Alliance

OTA Board Members
Tom Bartel, VP, CIPP, Return Path
Manish Goel, CEO Box Sentry
Dianna Koltz, Director of Best Practices, CIPP, Adperio