



June 4, 2010

The Honorable Rick Boucher
Chairman, Committee on Energy and Commerce
Subcommittee on Communications, Technology and the Internet
United States House of Representatives
2187 Rayburn House Office Building
Washington, D.C. 20515

The Honorable Cliff Stearns
Ranking Member, Committee on Energy and Commerce
Subcommittee on Communications, Technology and the Internet
United States House of Representatives
2370 Rayburn House Office Building
Washington, D.C. 20515

Re: Comments to Discussion Draft Privacy Act

Dear Chairman Boucher and Ranking Member Stearns:

The Online Trust Alliance's (OTA) hereby submits its comments and proposed revisions to the staff discussion draft privacy legislation issued on May 3, 2010 (Discussion Draft).

OTA is encouraged by many elements of this Act which we believe can benefit both consumers and businesses. At the same time we are concerned with the risk of causing unintended consequences. As drafted there is a risk of disrupting legitimate business models which will likely disenfranchise large segments of consumers who depend on access to online content and services supported by advertising for their communication, education and employability, yet we believe with the prescribed changes we can strike the needed balance.

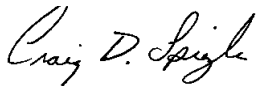
OTA was founded in late 2004, to address global spam problem and the lack of standards and practices to help detect forged email. (Since that time OTA has grown significantly. As an IRS approved 501c6 member based non-profit, we are representative to the broad internet ecosystem and not beholden to any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

OTA is active with many governmental agencies including the Departments of Commerce, Treasury, and Justice, the White House, the Federal CIO Council and the Federal Trade Commission. This past twelve months has marked several OTA milestones including the publishing of:

- Proposed Data Collection & Privacy Statement 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
- Compliance & Online Trust Training Events in San Francisco, Philadelphia, Singapore, Copenhagen, Amsterdam & Germany.

Thank you for the opportunity to provide this input. On behalf of OTA, I look forward to our continued dialog with you and your staff.

Respectively,



Craig Spiegle
Executive Director
Online Trust Alliance

Cc
OTA Board of Directors
OTA Steering Committee

Amy L. Levine
Subcommittee Counsel
Committee on Energy and Commerce
316 Ford House Office Building
Washington, DC 20515

Attached: discussion draft mark up

Sec. 2 (4) (B) (ii) Covered Entity Exclusion - Page 2 Line 20

We support the exclusion of small businesses that collect a minimal amount of collected information. Based on our research and understanding of small business promotional and marketing practices, we submit this should be increased to 15,000, (less than 300 names per week). FTC regulations need to prevent this from becoming a loop hole for deceptive businesses and bad actors to create multiple DBA's and affiliates for the purpose of circumventing this exclusion. The current limit of 5,000 would create an unacceptable burden and excessive cost to small business and small business formation.

Proposed Revision:

(ii) any person and or its affiliates that collects covered information from fewer than ~~5,000~~ 15,000 individuals in any 12-month period and does not collect sensitive information, share data with any non-affiliated third party and their total number of collected individuals does not include more than 50,000 records.

Sec 2 (5) (H) Covered information – Page 3, line 20

Section H identifies a unique persistent identifier including an IP address to track a computer or device as covered information. An IP address is required for anti-fraud and security purposes to track a server's (or other device's) actions, reputation and or behavior using such mechanisms as block and allow lists. A requirement to have consent would impede the ability to detect and block malicious activity, distribute legitimate opt-in messaging or web pages, collect forensics data and analyze behavior of a server. While it is believed this is covered under "Operation Purposes", line 25, it is suggested that this be clarified here.

Proposed Revision:

..... identify information about a specific individual or a computer, device, or software application owned or used by a particular user or that is otherwise associated with a particular user, with the exception of servers or devices where an IP address is collected for the purpose of reputation analysis, detection, prevention or action against security threats, unsolicited email, and or for law enforcement and forensic purposes as outlined under Operation Purpose ii.

Sec 2 (5) (J) Covered Information J - Page 4, line 5

To comply with existing legislation and industry best practices, interactive marketers must retain opt-out preferences and suppressions lists which may include covered information. The current language conflicts with this requirement.

Proposed Revision:

Any other information that is collected, stored, used, or disclosed in connection with any covered information described in subparagraphs (A) through (I). Information that might otherwise be covered information under this subparagraph but which relates solely to honoring and retaining suppression lists or consumers self -reported preference information , such as opt-outs or opt-ins, shall not be considered covered information under this Act.

Sec 2 (7) (A) (ii) Operational Purpose -- Page 4, line 23- Page 5 – Line 2

Protecting the safety and integrity of online activities by companies should be encouraged. For example, companies should be allowed to use covered information for the purposes of investigating malicious activities such as brand infringement, phishing, spamming and spyware and illegal activities such as child pornography. Accordingly, the term "operational purpose" should be expanded to not just protection of products and services but to include efforts by companies to protect and promote safety of online systems, activities, and of vulnerable individuals generally as well as their brands and online reputation.

Proposed Revision:

(ii) detecting, preventing, or acting against actual or reasonably suspected threats ~~to the covered entity's product or service~~, including security attacks, unauthorized use or transactions, and illegal or fraudulent activities;

Sec 2 (9) Render Anonymous – Page 6, lines 15-19

The concept of "reasonable basis" has been an ongoing area of controversy between real life use cases, and experimental research and other edge cases. It is suggested the term "reasonable basis" be clarified as outlined below.

Proposed Revision:

(9) RENDER ANONYMOUS.—The term "render anonymous" means to use reasonable efforts to remove or obscure covered information such that the remaining information does not identify, and there is no reasonable basis, based on technology commercially available at the time information is collected, rendered anonymous and / or stored, that the information can and will be used to identify

Sec 2 (10) (B) Sensitive Information – Race or ethnicity (Page 7, line 7)

Increasingly sites are providing users the ability to set a language preference. Such information may be stored in a cookie so the site can recognize and honor a visitor's preference. We suggest the Act call out that the collection of a language preference alone does not constitute sensitive or covered information.

Proposed Revision:

(B) race or ethnicity; with the exception of an individual's language preferences

Sec 2 (10) (F) Sensitive Information – Precise Geolocation (Page 7, line 14)

We submit "Precise Geolocation" be defined to indicate a specific physical street address or city block for the purpose of identifying an individual's or device's physical location, versus the general community in which they may reside or be located. Users realize significant value from sites by providing a postal code for obtaining local news and weather as well as for locating merchants close to them.

Proposed Revision:

(F) precise geolocation information, for the purpose of identifying and or tracking an individual's specific physical location.

Sec 2 (11) Service Provider (Page 7, lines 15-23)

The definition and examples of service providers should be clarified to include but not be limited to entities acting solely on the behalf of the first party for the operational, maintenance and administrative support functions. This includes analytics used for operational purposes including but not limited to accounting and billing purposes. With the increased reliance on Internet based cloud services, the scope should be broadened and remain flexible to incorporate evolving internet and mobile applications and services

Proposed Revision:

The term “service provider” means an entity that collects, maintains, processes, stores, or otherwise handles covered information on behalf of a covered entity , including, for the purposes of serving as a data processing center, providing customer support, serving advertisements to the website of the covered entity, customer credit and identity validation, sending commercial electronic mail messages on behalf of a covered entity to individuals whose electronic mail addresses were collected in conformity with this Act and returning to the covered entity information regarding the performance of such advertisements or commercial electronic mail messages, maintaining the covered entity’s records, performing analytical services relating to traffic on the covered entity’s website or websites and relating to advertisements or other commercial and noncommercial messaging delivered by or on behalf of the covered entity , or performing other administrative support functions for the covered entity.

Sec 3 (a) (2) (A) (i) (II) Notice And Consent Requirements, Nature of Notice, page 9 line 10

Today most privacy notices are complex and not easily comprehensible to the typical consumer. We propose the Act stipulate the FTC define a framework and template for a standardized privacy notice. The standardized notice would outline a uniform data collection and use statement for covered entities, which would provide consistency and comparability from one site to another. The framework should also be written to the average literacy level of the intended consumer or target audience. (See OTA Recommendation https://otalliance.org/privacy_demo.html)

Proposed Revision:

(III) the act shall direct the FTC to develop a framework and template for a standardized privacy notice which is comparable from one site to another and written at the average literacy level of the intended consumer.

Sec 3 (a) (2) (A) (ii) Notice And Consent Requirements, page 9 line 11

This section establishes the need for covered entities to receive express affirmative consent from individuals before sharing individuals’ covered information with unaffiliated parties. The consumer interest that this bill most effectively champions is a level of consumer control that exceeds that established under the old “notice and choice” standard of 1990s and 2000s. As such, we believe that requiring covered entities to provide a robust notice around data sharing, coupled with a clear and conspicuous opt-out mechanism, sufficiently advances the consumer interest while adequately protecting legitimate businesses. Conversely, the express consent standard exceeds this interest, for it would have detrimental effects on consumers’ access to the currently free valuable content and services provided by affected covered entities.

Proposed Revision:

ii. ~~MANUAL~~ COLLECTION OF INFORMATION BY MEANS OTHER THAN THROUGH THE INTERNET. If the covered entity collects covered information by any means that does not utilize the Internet, including but not limited to retail point of sale, manual collection and or telesales, the privacy notice required by this section shall be made available to an individual in writing, verbally or by other readily accessible means providing the ability to opt out of ~~before the covered entity collects~~ the collection of any covered information from that individual.

Sec 3 (b) (1) Express Consent Required For Disclosure of Covered Information to Unaffiliated Parties

This section establishes the need for covered entities to receive express affirmative consent from individuals before sharing individuals' covered information with unaffiliated parties. The consumer interest that this bill most effectively champions is transparency and choice. This consumer interest is fulfilled by the notice and opt-out requirements of the draft bill as well as the robust self-regulatory efforts currently being adopted by the industry. OTA supports the need to improve consumer protection, but believes the draft would have a detrimental effect on consumers' access to the valuable content and services provided by affected covered entities for free or otherwise subsidized rates. This would impede their access to information and online services impacting their communication, education and employability.

Proposed Revision:

(1) IN GENERAL—A covered entity may not sell, share or otherwise disclose covered information to an unaffiliated party unless such covered entity--

(A) makes available to such individual a privacy notice that specifically details the sharing practices of the covered entity and provides a clearly and conspicuously displayed method for objecting to the sharing of the individual's covered information; and

(B) obtains the consent of the individual to such collection and sharing as set forth in 3(a)(3)

Sec 3 (b) (e) (2) Deletion of anonymous data, Page 17, line 22

OTA is in favor of a maximum period for retention of any consumer data. Data minimization is a best practice which reduces the potential of harm and supported by OTA's Online Principles. We recommend the retention period be revised to no more than 13 months, providing for a reduced timeline for storage, yet allowing for seasonality in the planning and execution of marketing initiatives – for the benefit of consumers.

Proposed Revision:

(2) the covered entity deletes or renders anonymous any covered information not later than 13 (thirteen) 18-months after the date the covered information is first collected with the exception of data retention required for compliance and regulatory purposes or as required for an Operational Purpose;

Sec 4 (b) Security of Covered Information, Page 19, line 17

OTA recognizes that appropriate security measures are ever evolving and changing to keep up with technological changes as well as new threats posed by malicious actors. OTA is also in favor of supporting the continued development of robust and responsive industry standards and guidelines around data security. Accordingly, we recommend that this bill apply a reasonableness standard already utilized in almost a dozen states and currently employed by the FTC. This would allow security measures to evolve and will provide an environment to help promote development of new and better security measures not yet contemplated.

b) SECURITY OF COVERED INFORMATION.—

(1) IN GENERAL.—A covered entity or service provider that collects covered information about an individual for any purpose must establish, implement, and maintain reasonable and appropriate administrative, technical, and physical safeguards ~~that the Commission determines are necessary~~ to—

Sec 4 (b) (1) (A) Accuracy & Security of Covered Information, Page 19, line 17

With the increased use of third party service providers and cloud services, safeguards need to be in place for data not only collected and stored but across the entire data use life cycle – data in use, at rest and in motion should be accurate and have adequate security protections.

Proposed Revision:

(A) ensure the security, integrity, and confidentiality of such information including information collected, used, stored and shared with affiliates and agents;

Sec 4 (b) (1) (D) Accuracy & Security of Covered Information & Consumer Education, Page 20, line 1

Reactive efforts to data breach or loss incidents do not adequately limit risk of harm or identity theft for users. The faster a business acts on the loss of data the lower the risk for damages and harm. It is recommended that all covered entities have a data breach incident loss plan in place and have trained first responders to execute the plan. OTA advocates this as a best practice.

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

Proposed Revision:

(D) To prepare against a possible data breach or loss event, a data loss incident response plan must be established before any covered information is collected, providing management, employees and their agents an action plan to mitigate consumer harm; in the event of a security breach, determine the scope of the breach, make every reasonable attempt to prevent further unauthorized access to the affected covered information, and restore reasonable integrity to the affected covered information.

Sec 4 (c) Accuracy & Security of Covered Information & Consumer Education, Page 20, line 16

Research indicates teachable moments can be more effective than a broad consumer campaign. It is recommended the Act provide for the inclusion of market incentives for businesses to educate site visitors as they engage in activities including but not limited to accessing content on their site, communications and logging in and sharing covered information.

Proposed Revision:

(c) CONSUMER EDUCATION.—The Commission shall conduct a consumer education campaign to educate the public regarding privacy notices and opt-out and opt-in consent rights afforded by this Act, and provide incentives to business to provide teachable moments to users.

Sec 8 (3) Enforcement – Page 23, lines 16

It is important to provide for the capability of safe harbor and to encourage self regulation.

Proposed Revision:

(3) RULEMAKING AUTHORITY AND LIMITATION.—The Commission may, in accordance with section 553 of title 5, United States Code, issue such regulations it determines to be necessary to carry out the provisions of this Act. In promulgating rules under this Act, the Commission shall not require the deployment or use of any specific products or technologies, including any specific computer software or hardware. Pursuant to this Act, the Commission may also authorize safe harbor programs, provided that those programs meet the requirements of this Act.

Sec 12 Effective Date – Page 27, line 9

As drafted there is a high level of uncertainty on the application of data collected before the Act is enacted. The purpose of this proposed change is to ensure that the new set of baseline rules for notice and consent prior to the collection of data take effect only for data collected after the effective date.

Proposed Revision:

Add “provided, however, that the Act’s requirements for notice and consent prior to the collection of data, including those in Section 3, shall apply only to covered information collected after the effective date of this Act,”