

# OTA Online Trust Principles & Business Guidelines



*Creating an online trust community, promoting business practices and technologies to enhance consumer trust and the vitality of interactive marketing, ecommerce, and online financial and governmental services*

Revised December 14, 2009

---

This paper is for informational purposes only. The Online Trust Alliance (OTA) makes no assertions or endorsements regarding the security or business practices of companies who may choose to adopt such Principles. OTA MAKES NO WARRANTIES, EXPRESS, IMPLIED, OR STATUTORY, AS TO THE INFORMATION IN THIS DOCUMENT. For updates visit <https://otalliance.org/resources/principles.html>



## **Background**

As an independent non-profit, OTA is a global organization addressing online trust and abuse, helping to protect consumer and businesses. OTA promotes self-regulation and best practices by working with the online trust community, a coalition of leading stakeholders. Members include leading interactive marketers, advertisers, technology and solution providers, government representatives, privacy advocates, academics and merchant card processors. OTA supports them through balanced recommendations in the best interest of the consumer, while being practical and cost effective for businesses.

As the Internet has developed, the value proposition to consumers and business continues to grow. At the same time criminal activity of truly bad actors has similarly increased – as well as misguided business practices from legitimate businesses. Both of which contribute to a steady erosion of online trust. As online businesses accumulate vast amounts of user data, the responsibilities of data stewardship and governance have become amplified. Compounded by the rise in compromised systems and sensitive data loss, we risk a continued decline of consumer confidence. Consumer anxiety continues to grow, impacting the promise of the Internet.

## **OTA Online Trust Principles**

In April of 2009, in response to these challenges, the OTA released for public comment, a set of Online Trust Principles, (“Principles”). Over the next eight months, Town Hall Meetings were held in Europe, Asia and North America resulting in the submission of over one-hundred comments. The resulting Principles reflect a consensus of OTA member companies and the Online Trust Community. They include a mix of “core requirements” and “recommended practices” which outline the opportunity for increased trust online, primarily through business accountability; data stewardship and best practices.

The Principles have been designed to protect the consumer, preserving the benefits they receive from access to free content, email and related services from the advertising supported Internet. It is our belief that businesses who adopt the Principles will realize brand differentiation and a competitive advantage through increased trust with their users.

Since the Principles were introduced, other industry organizations have also published various advertising, marketing, security and privacy-related policies, and best practices, mirroring many of the principles outlined in this document. OTA supports these complementary efforts and encourages businesses to consider them in addition to OTA’s Principles.

OTA believes in the need to create a measurement framework for any such guidelines. Not unlike health departments who publically post scores for restaurants, similar online measurements need to be established and reported. Consistent with existing OTA scorecards and benchmark reporting, it is proposed that reporting include the Fortune 100, Interactive Retail 100 and top financial institutions. It is OTA’s goal to work with our organizations and industry partners to implement tracking and reporting by mid 2010.<sup>1</sup>

---

<sup>1</sup> May include a combination of third party and self-reporting. It is recommended self-reporting to be consistent with existing legislation and accounting practices.



It is important to note that all principles may not apply to every business or may already be mandated or regulated by specific industries. With a commitment to consumer choice and self-regulation, we suggest you assess your current practices. OTA has outlined the following questions as an aid;

1. Does the frequency and content of your email marketing communications match the user's expectations set when they opted in?
2. Are your privacy policies and disclosure statements governing email, behavioral targeting and use of personal data written concisely and genuinely informative? Can the target audience understand the language in your policies?
3. Are users provided clear notice, choice and control of how their data is collected, used and shared?
4. Are your privacy notices and policies reviewed regularly to ensure they are accurate and up-to-date? Are users notified to policy adjustments?
5. Are you taking the opportunity to provide users with recommendations to help them protect their data?
6. Are you implementing technologies, processes and safeguards to protect data collected from potential data misuse, loss and theft?
7. Are you implementing best practices to help protect your web site and email from being spoofed and forged?
8. Are users provided notice prior to or at the time any personal information is collected, other than within the privacy or terms of use policy statements?
9. Do you have a Data Loss Prevention (DLP) plan published and up-to-date, accessible for all employees in the event of a breach, loss or intrusion?
10. Do your promotional offers provide clear notice regarding any and all recurring charges and data that might be shared with third parties including their credit card and billing information?

---

Special thanks to the following organizations for their collaboration and input; Anti-Phishing Working Group, (APWG), CA/Browser Forum, Center for Democracy & Technology (CDT), Council of Better Business Bureaus, Interactive Advertising Bureau, (IAB), Direct Marketing Associations (The-DMA, Singapore and Netherlands), The German Internet Society, Email Service Provider Coalition (ESPC) and the US Chamber of Commerce.

**OTA Board of Directors & Steering Committee Companies**

Adperio	Bank of America	BoxSentry Pte Ltd	Cisco Systems
Datran Media	Forrester Research	Epsilon	Iconix Inc.
Internet Identity	Intersections Inc.	LashBack LLC	MarkMonitor Inc.
McAfee Inc.	Message Systems	Microsoft	Publishers Clearing House
Return Path Inc.	Secunia Inc.	Symantec	TRUSTe
VeriSign Inc.			

OTA looks forward to working with business, industry and governmental agencies in advancing the Online Trust Principles to enhance online trust and the long-term vitality of the internet. Companies that adopt these and other principles should realize "trust dividends" for years to come, while other may face a "trust tax", impacting their bottom line and long-term prospects.

<b>SUMMARY OF OTA ONLINE TRUST GUIDELINES &amp; PRINCIPLES</b>	<b>Core Requirements</b>	<b>Recommended Practices</b>
1. Maintain and audit internal Information Technology systems		
a) Regularly scan systems including servers and desktops for known vulnerabilities.	✓	
b) Implement protection against phishing, spam, viruses, data loss, and malware.	✓	
c) Encrypt all wireless data access points.	✓	
2. Implement Extended Validation (EV) SSL Certificates for all consumer web sites which have login forms. EV SSL helps to protect against unintentional account disclosures. Priority implementation should be considered by government, banking and online billing sites with existing SSL Certificates.		✓
3. Establish a domain management program, to inventory and track domain registrations and renewals; identify and monitor potential brand name and trade mark abuse; and other related forms of abuse.	✓	
4. Audit all third-party code and links used for serving and publishing content on external sites.	✓	
5. Authenticate all outbound email for all domains and sub domains attributed to your company	✓	
6. Notify users of outdated web browsers when attempting to authenticate to sites.		✓
7. Publish a Data Loss Prevention (DLP) Plan		
a) Develop incident response plan and employee procedures for data loss	✓	
b) Encrypt all data files that include PII and email lists, which are transmitted to external third parties.	✓	
8. Implement policies that are comprehensible to the site's target segment's reading literacy level.		✓
9. Ensure privacy and data sharing policies are discoverable from the point of consumer interaction.	✓	
10. Provide prominent notice of material changes to all privacy and data collection policies.	✓	
11. Provide consumers an expectation on the frequency of email they will be receiving upon signup.		✓
12. Include the List-Unsubscribe header in all commercial email.	✓	
13. Adopt third-party security, privacy and opt-out seal and certification programs.		✓

The OTA Online Trust Principles are broken into “core requirements” and “recommended practices”. Core requirements are considered the foundation to secure consumers data; and all businesses are encouraged to implement them immediately. Recommended practices recognize other factors that may limit their ability to be implemented. Over time we expect these to evolve based on tools and technologies made available and external threats to consumers and online business.

The Principles include three categories:

1. Infrastructure (including protection of servers, web sites, desktop and mobile devices)
2. Data Loss Prevention (DLP)
3. User Choice, Control and Data Privacy

### **INFRASTRUCTURE:**

- 1) To help protect against internal system, data compromises and access breaches
  - a) Regularly scan systems and applications for known vulnerabilities. Installation of updates may be deferred pending compatibility testing for internal line of business (LOB) applications;
  - b) Implement protection against phishing, spam, viruses and malware. Such protection may include but not be limited to perimeter, edge security mechanisms and client PC protection.
  - c) Encrypt all wireless data access points of data collection.
- 2) EV SSL Certificates - Upon the expiration of existing Secure Socket Layer (SSL) certificates, all consumer-facing sites that collect credit card, bank account or other sensitive data (such as social security numbers) including ecommerce, government agencies, banking and online billing sites should upgrade to Extended Validation SSL Certificates (EV SSL). EV SSL certificates are designed to help restore confidence among users that a website operator is a legally established organization with a verifiable identity. EV SSLs communicate their presence by providing a green identifier in a browser’s address bar and supported by every leading browser.<sup>2</sup> [More>](#)
- 3) Establish a Domain Name System (DNS) management program. Within six months, all companies need to complete an annual inventory of all domains owned, institute a centralized domain acquisition and renewal process. Companies should implement “Domain Locking” a security enhancement to help prevent unauthorized transfers of domain to another registrar or web host by “locking” your domain name servers. When a domain is locked, the domain is protected from unauthorized third parties who might try to misdirect name servers or transfer a domain without your permission. These measures help prevent consumer deception and detect brand infringement, before deceptive sites are deployed.<sup>3</sup>
- 4) Conduct audits of third party code, links to external sites, plug-ins and site scripts prior to installation or integration on a company site and re-validated at semi-annually. With the increased incidence of malvertising, deceptive links and click fraud, such audits shall be established including analyzing content providers whose content (including news, stock data, weather and or advertising), is integrated into a site.<sup>4, 5</sup>

---

<sup>2</sup> Implementation requirements are the same as existing SSL certificates.

<sup>3</sup> Threat of “drop catching” <http://www.cadna.org/en/newsroom/press-releases/drop-catching-study>

<sup>4</sup> Such code shall include but not be limited to third party ads, ad servers, content providers and analytics, but not intended for internal infrastructure or data warehouses.

<sup>5</sup> Examples include but are not limited to shopping carts and event registration services.

- 5) Implement outbound email authentication across all corporate, email and product related domains. In response to the prevalence of forged, spoofed and deceptive email, all consumer facing brands and companies shall implement one or more of the leading email authentication protocols. Email authentication should also be established for domains not used or acquired for a domain defense and not intended for deployment.<sup>6</sup>  
[Learn More](#)
- 6) As a guideline, where possible, sites should recommend users of end-of-life browsers to upgrade to the current versions, i.e. (“Why Your Browser Matters”) (Specific to transactional web sites including ecommerce and banking and any site requiring user names and passwords). Sites should help educate users by providing information, alerts and links.<sup>7</sup> *(It is recognized some businesses have standardized browsers and may not be able to upgrade due to compatibility issues with line of business (LOB) applications).*

#### **DATA LOSS PREVENTION (DLP) PLANS**

- 7) Create and implement data safeguards. Recognizing the likelihood of potential data loss, theft and or system breaches, all data that is collected and used for research, marketing and/or behavioral targeting, (including personally identifiable information (PII), and email addresses), MUST have a DLP plan including but not limited to the following;
  - a) Publish an internal company DLP contingency plan, for employee reference, including 24 x 7 incident response handling and processes to contact affected users and law enforcement in a timely fashion or as required by law. *Such plans may or may not be made public at the discretion of the company;*
  - b) Encrypt all customer data shared with external third parties and vendors. Such data shall include all files including PII, credit card data and email addresses or as specified by PCI and other data standards or organizations.

#### **USER CHOICE, CONTROL & PRIVACY**

- 8) Provide consumers comprehensible policies including email, terms-of-service (TOS), privacy and data sharing with third parties and affiliates. Such polices shall be written for the average literacy level of the site’s target user. Recognizing English may not be the user’s primary language; sites may consider publishing policies in Spanish and other languages.<sup>8</sup> Entities who are multi-channel (retail and online), should adopt policies which are consistent irrespective with the point of data capture.<sup>9</sup>

Over time, OTA advocates for a standardized notice, not unlike an auto “Monroney” sticker or a nutrition label offering a consistent framework helping consumers to make informed choices across all online activities including a site’s terms of use, privacy policy, use of search engines and when opting in or subscribing for email.

---

<sup>6</sup> Senders and domain holders must implement production Sender Policy Framework (SPF) / SenderID (SIDF) records and/or Domain Keys Identified Mail (DKIM)..

<sup>7</sup> Why Your Browser Matters - User will be presented or redirected to a landing page providing a “teachable-moment”, informing them of the risks of using an outdated browser and provide links for upgrading. Note trying to move a customer to a competing browser brand is not recommended nor endorsed by OTA. Sites may wish to disallow login for such users with EOL browsers. While it may not be permitted without user consent, sites may consider offering the ability of providing users a scan of their systems for such vulnerabilities as outlined in Principle #1.

<sup>8</sup> OTA Privacy policy is now available in English and Spanish [www.otalliance.org/privacy.html](http://www.otalliance.org/privacy.html)

<sup>9</sup> See efforts Wal-Mart to provide such multi-channel notice and user controls  
[www.informationweek.com/news/security/privacy/showArticle.jhtml?articleID=218501013](http://www.informationweek.com/news/security/privacy/showArticle.jhtml?articleID=218501013)

- 9) Site's Privacy Policy be clearly and conspicuously discoverable on the home page and all points where a user first interacts with the site. As a best practice, such policies should be available prior to at the time the information is collected. For example, on website registration forms or business reply cards, notices should be intuitively located above or alongside the area consumers submit their email address or other PII.
- 10) Companies to provide prominent notice of material changes to all privacy, TOS and data collection policies. Such changes cannot be retroactive to data collected. Examples of such notices may include, but not be limited to email notices to customers or subscribers and or a welcome screen upon user's revisiting their site. In addition site should take proactive measures to ensure their posted policies remain accurate and up-to-date.
- 11) Provide consumers a reasonable expectation on the frequency of email they will be receiving upon signup or registration. As an example, a customer would be informed prior to registration an average number of emails they will receive monthly, and if their names are shared with any third party. If a site is unable to provide a frequency assertion they shall state so. To maximize a brands email reputation, it is a recommended guideline that the subject of such emails be aligned to their expectations and users have the ability to review and modify such mail through a preference or subscription center. In addition consumers should be able to easily opt-out of having any data shared with third parties, with a recommended default setting be set to opt-out.
- 12) All senders shall include the List-Unsubscribe header in all commercial email, allowing for users to safely unsubscribe from known or validated senders as specified by IETF RFC 2369. In addition to the unsubscribe footer required by most regulatory authorities, this header enables leading email clients and mail providers to provide users an additional mechanism for unsubscribing.
- 13) Should adopt third-party security and privacy certification programs and utilize a trustmark to provide consumers an identifiable and easy to understand mechanism regarding their privacy assertions and establish measures to ensure such policies are up-to-date. As an alternative, a company officer may attest in writing the compliance and adherence to the integrity of their privacy, data sharing and email marketing policies.

---

#### **About The Online Trust Alliance (OTA) <https://otalliance.org/>**

*The mission of OTA is to create an online trust community, promoting business practices and technologies which enhance consumer trust and the vitality of interactive marketing, ecommerce and online financial and government services.*

Through its member companies and organization affiliates, OTA represents over one million businesses and 500 million users worldwide with regional chapters in Asia Pacific, Canada and Europe. OTA is a 501c6 IRS-approved non-profit, governed by a Board and Steering Committee including Bank of America, BoxSentry, Cisco Systems, Datran Media, Epsilon, Iconix, Internet Identity, Intersections, LashBack, MarkMonitor, Message Systems, Microsoft Corporation, McAfee, Publishers Clearing House, Return Path, Secunia, Symantec Corporation and VeriSign Inc.

For updated versions of this document visit <https://www.otalliance.org/resources/principles.html>