Online Trust Principles

Updated October 5, 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 MAKE NO WARRANTIES, EXPRESS, IMPLIED, OR STATUTORY, AS TO THE INFORMATION IN THIS DOCUMENT. For updates visit https://otalliance.org/resources/principles.html

---

OTA Principles

As the Internet has developed, the value proposition to consumers and business has grown exponentially. At the same time it has unfortunately attracted online crime and deceptive business practices. Consumer anxiety continues to grow on multiple fronts: increases in identity theft, forged email and questionable data sharing practices, collectively impacting the promise of the internet.

As businesses accumulate considerable amounts of personal identifiable data, the responsibilities of data stewardship and governance have become amplified. Businesses need to act not only within the letter of the law, but within the expectations of the consumer. Compounded by the rise in compromised systems and sensitive data loss, we risk a continued decline of consumer confidence.

Responding to these challenges, the OTA Principles were released as a draft in April 2009. Over the past six months, Town Hall Meetings were held in Europe and North America resulting in the submission of over one-hundred comments. The resulting Principles reflect general consensus of OTA member companies. Combined, the Principles underscore the need and opportunity for: increased business accountability, data stewardship and practices to improve consumer choice, preferences and control of data.

At the same time, the Principles have been designed to help preserve the benefits consumers receive from online resources including access to free content, email and related services supported by advertising. It is our belief that businesses adopting OTA Principles will realize brand differentiation and a competitive advantage.

Since first published, key trade groups including the Interactive Advertising Bureau (IAB), the American Association of Advertising Agencies (AAAA), the Direct Marketing Association (DMA), and others have stepped forward and published comprehensive advertising privacy-related policies. Other leading organizations including the Anti-Phishing Working Group (APWG), BITS/Financial Services Roundtable and the Email Senders & Providers Coalition (ESPC) have published online marketing and security best practices. OTA supports these collaborative efforts and encourages businesses to consider them in addition to OTA's Principles.

As an independent non-profit OTA is a global organization addressing these challenges and advancing self-regulation. This autonomy allows us to advance balanced recommendations and policies that are in the best interest of the consumer, while being practical and cost effective for businesses, without the risk of being self-serving.

OTA looks forward to working with business, industry and governmental agencies in advancing these Principles helping to enhance online trust and the long-term vitality of the internet.

OTA Board of Directors & Steering Committee Companies

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

OTA believes in a compliance measurement framework for any such guidelines. Not unlike health departments who publically post scores for restaurants, similar online compliance measurements need to be established and reported. Such information can aid consumers in making informed choices regarding the security and privacy practices of the sites they frequent. Consistent with existing OTA scorecards for email authentication and adoption of EV SSL Certificates, it is proposed that tracking and reporting include the Fortune 100, Interactive Retail 100 and top financial institutions. In addition, the reporting shall include OTA membership. It is OTA's goal to work with our organizations and industry partners to implement tracking and reporting by mid 2010.[1]

In reviewing and considering these Principles we recognize they may not apply to every business or industry sector. For some the Principles may already be part of your corporate governance and aligned to your mission. For others, the Principles may become goals you will strive toward. With a commitment to consumer choice while self-regulating, we suggest you -assess your current practices for areas to improve. OTA has outlined the following questions as an aid.

1. Is the frequency and subject matter of your email campaigns aligned to 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 consumers 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 consumers notified to policy adjustments?
5. Are you taking the opportunity through teachable moments to provide consumers with recommendations to help them protect their data?
6. Are you implementing technologies, processes and safeguards to protect the data collected from potential data misuse and leakage?
7. Are you implementing industry best practices to help protect your web site and email from being spoofed and forged?
8. Are consumers provided notice prior to or at the time personally identifiable information is collected, and not only stated within the privacy or terms of use statements?
9. Do you have a Data Loss Prevention (DLP) published and up-to-date, accessible for all employees?

[1] May include a combination of third party and self-reporting mechanisms. It is recommended any self-reporting to be signed by corporate officer, to help assure accountability, not unlike required for Sarbanes Oxley.

SUMMARY OF OTA ONLINE TRUST GUIDELINES & PRINCIPLES

Description	Required	Recommended
1. Maintain and audit internal systems		
a) Regularly scan systems and applications for known vulnerabilities.	✓	
b) Implement protection against phishing, spam, viruses, data leakage, and malware.	✓	
c) Encrypt all wireless data access points of data collection.	✓	
2. Implement EV SSL Certificates for all consumer facing sites which collect credit card, bank account or other sensitive data (such as social security numbers) including ecommerce, government agencies, banking and online billing sites which have existing SSL Certificates.	✓	
3. Establish a domain management program.	✓	
4. Audit all third party code, links and site applications.	✓	
5. Authenticate all outbound email for all domains.	✓	
6. Notify users of outdated browsers when attempting to authenticate to ecommerce and banking sites.		✓
7. Publish an Data Loss Prevention Plan (DLP)		
a) Develop contingency plan including 24 x 7 incident response.	✓	
b) Encrypt all data files that include PII and email lists, which are transmitted to external third parties.	✓	
8. Implement policies that are comprehendible to the site's target segment's reading literacy level.		✓
9. Site's Privacy Policy MUST be clearly and conspicuously discoverable from the point of consumer interaction.	✓	
10. Companies must 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. All senders MUST 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 three categories:

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

SYSTEM INFRASTRUCTURE:

1) To help protect against internal system and data compromises and access breaches, all companies MUST;

   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 MUST 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 are now supported by nearly every browser.[2] More>

3) Establish a Domain Name System (DNS) management program. Within six months, all companies MUST 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.[3]

4) MUST conduct security audits of all third party code, links to external sites, plug-ins, applications and scripts prior to installation or integration on a company site and re-validated at a minimum each quarter. With the increased incidence of malvertising, deceptive links and click fraud, such audits shall be established including analyzing and monitoring third-party sites and content providers whose content (including news, stock data, weather and or advertising), is integrated into a site for transactions or other direct-to-customer services.[4] [5]

[2] Implementation requirements are the same as existing SSL certificates.

[3] Threat of "drop catching" http://www.cadna.org/en/newsroom/press-releases/drop-catching-study

[4] Such code shall include but not be limited to third party ads, ad servers, content providers and analytics.

[5] 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 MUST 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.[6] Learn More

6) As a guideline, where possible, should recommend users of end-of-life browsers to upgrade to the current versions, (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.[7] (It is recognized some businesses have standardized browsers and may not be able to upgrade due to compatibility issues with internal line of business (LOB) applications).

DATA LOSS PREVENTION (DLP)

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 including 24 x 7 incident response handling, internal reporting policies, and processes to contact affected users and law enforcement in a timely fashion or as required by law;

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.

USER CHOICE, CONTROL & PRIVACY

8) Provide consumers comprehendible policies including email, terms-of-service (TOS) 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.[8] Entities who are multi-channel (retail and online), should adopt policies which are consistent irrespective with the point of data capture.[9]

9) Site's Privacy Policy MUST 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.

---

[6] Senders and domain holders must implement production Sender Policy Framework (SPF) / SenderID (SIDF) records and/or Domain Keys Identified Mail (DKIM). Companies may want to consider third party solutions such a Goodmail Certified email, Iconix Email ID and others for enhanced consumer protection.

[7] User will be presented with 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. 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.

[8] OTA Privacy policy is now available in English and Spanish www.otalliance.org/privacy.html

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

10) Companies MUST 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 MUST 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 a trusted global online ecosystem and foster the elimination of email and Internet fraud, abuse and cybercrime; thereby enhancing trust, confidence, and the protection of businesses and consumers. 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, Datran Media, Epsilon, Goodmail Systems, Iconix, Internet Identity, Intersections, IronPort (a division of Cisco Systems), 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

