2016 Online Trust Audit & Honor Roll

Independent analysis and benchmark report tracking the adoption of best practices and adherence to standards in:

- Consumer Protection
- Site, Server & Infrastructure Security
- Privacy Practices, Transparency & Disclosures

Released June 14, 2016

TABLE OF CONTENTS

Overview & Background 3

Executive Summary & Highlights 4

Methodology & Scoring 10

Domain, Brand & Consumer Protection 11

Site, Server & Infrastructure Security 11

Privacy, Transparency & Disclosures 12

Best Practices & Sector Highlights 13

Best Practices Highlights 13

Sector Highlights 15

Domain, Brand & Consumer Protection 17

Email Authentication 18

Domain-based Message Authentication, Reporting & Conformance (DMARC) 19

Opportunistic Transport Layered Security (TLS) for Email 20

Domain Locking 20

Domain Name System Security Extension (DNSSEC) 20

Internet Protocol Version 6 (IPv6) 20

Site, Server & Infrastructure Security 21

Server Implementation & Vulnerability Analysis 22

SSL Certificate Types 24

Malvertising 25

Privacy, Transparency & Disclosures 25

Privacy Policies & Third Party Tracking 26

Icons & Multi-Lingual Policies 28

Do Not Track Disclosure & Policy 28

Tag Management Systems & Privacy Solutions 28

WHOIS Registrations 28

Data Breach Incidents & FTC Settlements 28

Conclusion 29

Appendix A – 2016 Honor Roll Recipients 30

Acknowledgements 35

OVERVIEW & BACKGROUND

Consumers worldwide are realizing significant benefits from online services, yet are increasingly becoming concerned about their data, privacy and risks from cybercrime, which is altering their online behavior.[1] Left unchecked, mistrust in privacy, security and the online experience may have chilling effects. There is a growing trend that business and data collection practices are moving out of alignment with consumer expectations, creating a threat to the internet economy. As observed in Europe and increasingly in the U.S., such practices are fueling the call for regulatory oversight and legislation. For the internet to prosper, users must trust that their personal information will be secure, preferences respected and their privacy protected. The ultimate impact is to consumer trust. OTA calls on all stakeholders to move beyond a compliance mindset to become data stewards. By increasing respect of consumers, their data and the online experience, the economy and society will be postured to reap long-term benefits.

OTA's Online Trust Audit, a benchmark analysis of businesses' commitment to security, privacy and consumer protection, endeavors to increase awareness and adoption of consumer protection practices and technologies. Since its inception in 1998, the importance of this Audit and adoption of the prescribed best practices has been heightened by the increased sophistication of cybercrime, account takeovers, data breaches, ransomware and identity theft. As cyber threats increase and privacy concerns expand, this report is more timely than ever, underscoring the imperative that data security, consumer protection and responsible privacy practices need to be integrated into every service and business process.

As part of the annual Audit, the 2016 methodology (see page 10) has been updated to reflect current standards and areas of risk, including baseline scoring and bonus points for emerging best practices. Input and review was solicited and obtained through a multi-stakeholder process including industry, NGO's and standards organizations worldwide.

It is important to recognize that the Audit is limited to a slice of time. Based on the dynamic nature of site and application configurations and the evolving threat landscape, sites' scores may have changed since the audit was completed. While OTA is not making an endorsement of any site or business, readers should consider companies who have consistently made the Honor Roll as well as question those that have been conspicuously absent.

All analysis was done anonymously without the active participation of the sites being analyzed. Sites were selected based on their ranking within their individual sectors or public lists (or membership in OTA). In instances where a significant vulnerability or risk was identified, OTA abided by responsible disclosure practices and attempted to contact the "at-risk" entity. Unfortunately OTA's efforts have been limited as many companies do not have mechanisms in place to accept such disclosures, and many have out of date "who is" data and fail to monitor email addresses provided via their sites and privacy policies.

[1] https://www.washingtonpost.com/news/the-switch/wp/2016/05/13/new-government-data-shows-a-staggering-number-of-americans-have-stopped-basic-online-activities/

EXECUTIVE SUMMARY & HIGHLIGHTS

The primary goal of the Audit and report is to help drive the adoption of best practices and provide prescriptive tools and resources to aid companies in enhancing their security, data protection and privacy practices. The secondary goal is to recognize companies who have demonstrated a commitment to online trust and consumer protection by designating them as recipients of the 2016 Online Trust Honor Roll. Last but not least, a third goal is to provide an incentive for consumer-facing brands to make security and privacy part of their brand promise.

Now in its 8th year, the 2016 Audit encompasses nearly 1,000 websites across multiple sectors, examining consumer protection, security and privacy protection practices, and has been embraced by organizations worldwide as an objective benchmark report.[2] Changes in the 2016 sectors include expanding the News 50 to the News 100, which includes the top 100 news/media sites by unique monthly visitors. The Social 50 has been re-designated as the Consumer 100, including leading sites requiring account creation across multiple sub-segments such as social networks, email, photo/file sharing sites, dating sites, travel, jobs, e-file sites, identity theft protection, ridesharing and other sites.[3]

Sectors examined and associated top-ranked organizations include:

- 2016 Internet Retailer Top 500 based on revenue[4] (IR 100 & IR 500) – Gap Inc.
- FDIC top 100 banks based on net assets (FDIC 100) – IBERIABANK
- Top U.S. federal government sites (Fed 50) – Dept. of Health and Human Services (healthcare.gov)
- Top 100 consumer services sites (Consumer 100) – Twitter
- Top 100 news and media sites (News 100) – Google News
- OTA member companies (OTA) – Twitter

In recognition of the increased number of organizations qualifying for the Honor Roll, a new designation has been added this year – "Top of the Class" – recognizing sites with a total score of 95% or higher. These sites are highlighted in bold in the Honor Roll listing in Appendix A. These organizations represented 10% of the overall sites, and approximately 20% of those achieving Honor Roll status. Viewing "Top of the Class" recipients by sector, OTA members led with 48%, followed by the Consumer (23%) and the Federal 50 (18%). Approximately 3-6% of the online retailers, FDIC 100 and News 100 received this designation.

The top 10 overall scores represented a variety of sectors, led by consumer sites – 1) Twitter, 2) HealthCare.gov, 3) Pinterest, 4) the White House, 5) Dropbox, 6) FileYourTaxes, 7) LifeLock, 8) Instagram, 9) 1040.com, 10) Gap Inc.

[2] 2016 Online Trust Audit – Virtual Press Room https://otalliance.org/2016-online-trust-honor-roll-virtual-press-room-vpr

[3] While sector definitions and criteria for inclusion have remained constant, individual companies may be added or removed from sector lists due to reported revenues, site traffic ranking and the impact of market consolidation and acquisitions. This consistency allows year-over-year analysis within a sector. The analysis also assesses the top 100 retailers ("Internet Retailer Top 100") in addition to the Internet Retailer Top 500, allowing comparison between larger and smaller companies. Note some sectors were increased to a sample of 100 or more reducing the impact of outliers and improving comparability from one sector to another.

[4] Source list from Internet Retailer® https://www.internetretailer.com/top500/. In some charts and tables, for the sake of brevity, the Internet Retailer Top 100 and Top 500 are abbreviated "IR 100" and "IR 500", respectively.

As shown in Figure 1, of the organizations evaluated, 50% qualified for the Honor Roll (vs. 30% in 2014 and 44% last year). All sectors grew in achievement, but the sector having the largest impact on overall results was the Consumer 100, jumping from 58% to 71%. Other sectors having a major impact included the FDIC 100 (grew from 46% to 55%) and the News sites (which both doubled in sector size and rose in achievement from 8% to 23%).

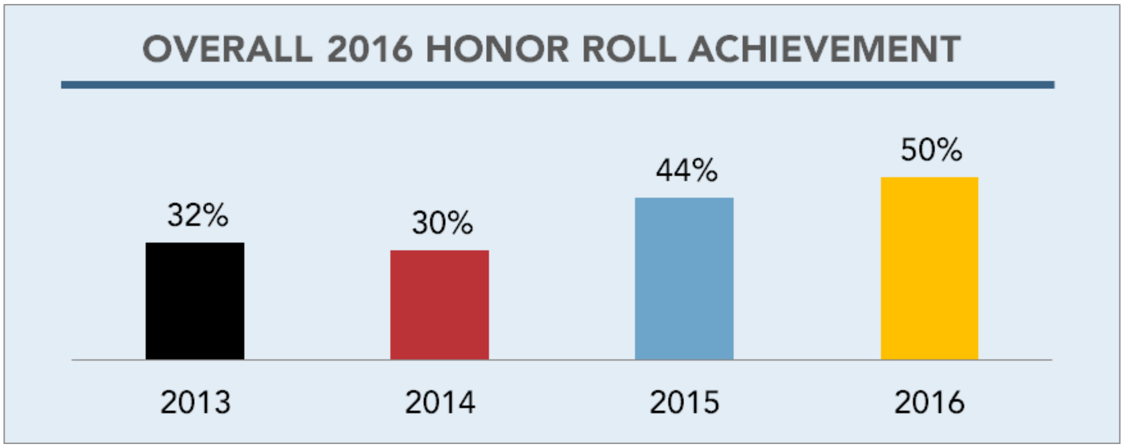


Figure 1 – Overall Honor Roll Achievement by Year, 2013-2016

As seen in previous years, a significant fraction of Honor Roll qualifiers are first time recipients – a total of 40% (183 sites, mostly from the Retail and Consumer sectors) were first-timers this year, down from 55% in 2015. A complete list of recipients is shown in Appendix A along with the number of consecutive years they have earned Honor Roll status. Approximately 12% of qualifiers (54) achieved Honor Roll status for the fifth year in a row, nearly 9% (40) qualified for the fourth year in a row, 8% (34) qualified for the third year in a row and 32% (143) qualified for the second year in a row.

The significant number of first-timers and the range of ranking of designees in the Internet Retailer Top 500 (from #1 to #493) shows that the Honor Roll is achievable by companies of all sizes and levels of technical resources and skills. By contrast, there were 78 sites (nearly 10%) that made the Honor Roll in 2015 but failed to repeat in 2016. This highlights that security and privacy practices are not a static process – sites need to continually monitor, update and evolve to keep pace with evolving threats.

As illustrated in Figure 2, Honor Roll achievement grew in all sectors despite more stringent criteria in this year's Audit. For the third year in a row, the Consumer 100 (previously the Social 50) outscored all sectors with 72% achievement. Many of these sites benefit from homogeneous and integrated system architectures in contrast to other sectors which have a higher percentage of legacy systems. Online retailers, banks and federal government sites all achieved results in the 45-55% range, while the News 100 lagged with 23% achievement.

It should be noted that OTA Members, 96% of which qualified for the Honor Roll, have been omitted from the chart since their scores were found to distort and compress the axis. OTA acknowledges the results may be biased since member organizations by the nature of their membership are committed to data stewardship and responsible privacy practices. While the methodology is public, OTA members' knowledge and awareness may be greater than others and the high achievement may somewhat skew the overall Honor Roll achievement shown in Figure 1. If OTA members were excluded, overall achievement this year would drop 4% to 46%.

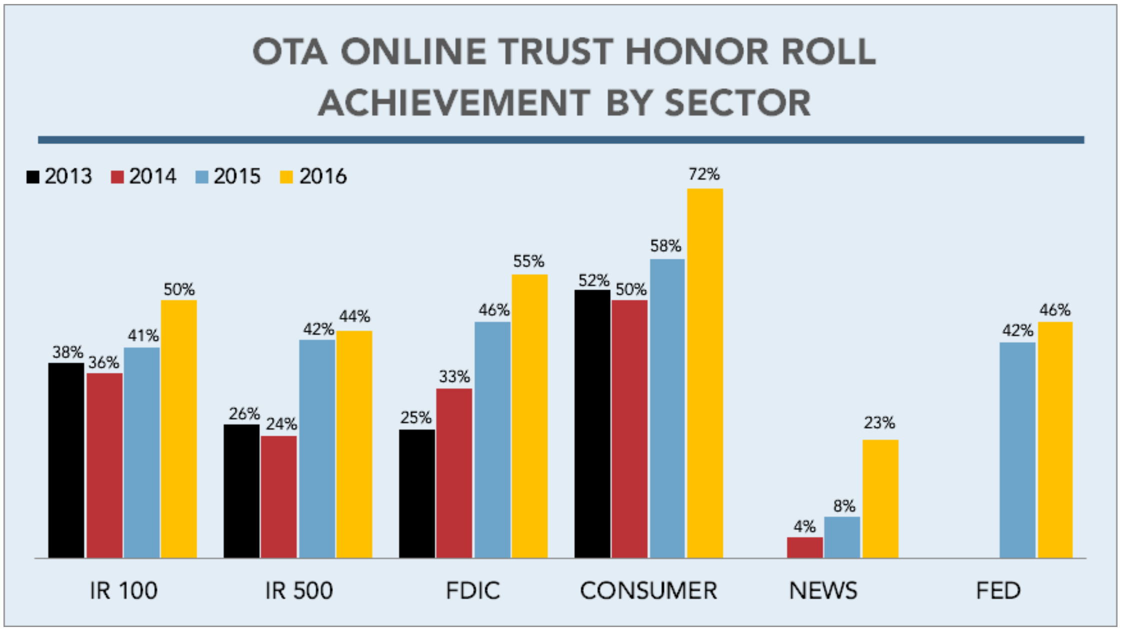


Figure 2 – Percent Achieving Honor Roll Status by Sector, 2013-2016

As seen last year, improved Honor Roll achievement was noted in all sectors, with many (IR 100, FDIC, Consumer, News) jumping more than 5%. Despite more stringent criteria, improvement in email authentication had the biggest impact on the rising achievement level. Site security scores also had a significant impact, with most sectors increasing their scores 3-5%. Overall, privacy scores actually dipped modestly in 2016, directly due to the more rigorous scoring of privacy policies. Many companies hover near the Honor Roll threshold – in the Internet Retailer Top 500 alone, nearly 90 companies are within 5% of reaching the Honor Roll, though many of those sites have a failure that would have to be addressed.

"Security and privacy remain the bedrock of consumer trust. As the overall top scorer in OTA's Online Trust Audit, Twitter is honored to be recognized for our efforts," said Twitter Trust & Information Security Officer, Michael Coates. "These best practices for our users' data are critical for the long-term health and future innovation of the Internet. We are committed to build on our collaboration between the public and sectors in driving their adoption."

It is also useful to examine the reasons why organizations did not achieve Honor Roll status. Of all sites analyzed, 42% had a failing grade (score of <55) in one or more categories (down from 46% in 2015), highlighting significant concerns regarding data security and privacy practices. Figure 3 shows the Honor Roll vs. Neither vs. Failure percentage breakdown for each sector. This chart clearly shows that results are nearly bi-modal, with only a small slice of sites in each sector that neither make the Honor Roll nor have a failure. Figure 4 breaks down the failures a step further to show which categories caused the failures.

Failures were most prominent in the News 100 sector, and least prominent in the Consumer 100 (the failure rate for OTA members, which is not shown, was 4%). For the fourth year in a row, the Internet Retailer Top 100 fared better than the Internet Retailer Top 500. As in 2015, results for the Federal 50 were bi-modal and slightly below the average of other sectors, with 46% achieving the Honor Roll and 54% failing in one or more categories.

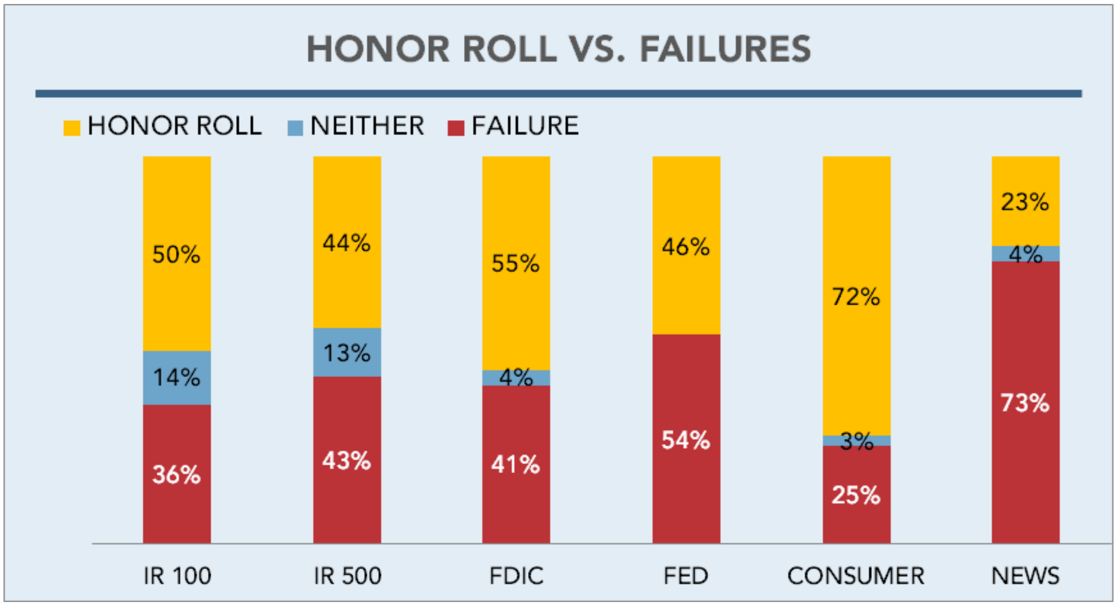


Figure 3 – Distribution of Honor Roll vs. Failures by Sector

Failure reasons and percentages varied widely by sector. Inadequate email authentication was the primary cause for failures in all but the News 100, led by Federal sites with a 50% failure rate. The main reason for failure in this category was a continued shift in scoring to place increased emphasis on email authentication at top-level domains and implementation of associated DMARC records. The absence of proper email authentication leaves consumers increasingly vulnerable to spearphishing and related exploits including ransomware, bank account takeovers and identity theft.

Inadequate privacy policies and practices were the second largest cause of failures, impacting more than one-half of the News 50 and one-seventh of online retailers. Significant improvement was made by retailers, which reduced privacy failures by half, and the FDIC 100, which continued its streak of reducing failures. The News 100 sector lags significantly in privacy scores primarily due to heavy use of third-party data collection and tracking, reflecting their reliance on third-party advertisers to drive revenue. All other sectors reduced their privacy failure rates, though as noted, overall privacy scores went down. This is indicative of many sites adopting the bare minimum elements to avoid failure, but the bulk of sites not keeping pace with the more rigorous criteria in the 2016 Audit.

Site security was the lowest cause of failure for all sectors, showing that the vast majority of organizations are tracking with the minimum recommendations for site security, though the overall failure rate did rise from 6% in 2015 to nearly 10% this year. This increase can be attributed to more rigorous scoring which maps a failure of a major subcomponent (e.g., protocol support) to a failure of the category.

“As cybercrime and tactics evolve, so must businesses’ adoption of security and privacy enhancing best practices. Microsoft is proud to be named to the Online Trust Honor Roll recognizing our leadership in security and privacy. While there is no perfect security or privacy, the Audit reinforces the importance of taking a holistic view of consumer protection, user empowerment and data stewardship," said John Scarrow, GM Microsoft Safety Services.

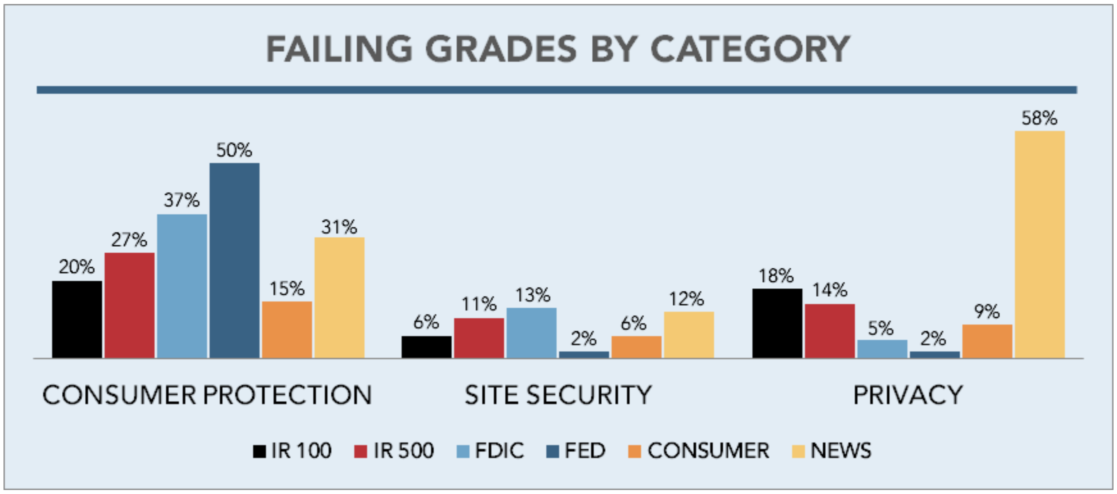


Figure 4 – Percent of Companies with Failing Grade by Sector and Category

Additional insight can be gained by normalizing the 300 baseline points to a 100-point scale (called the "Online Trust Index") and comparing the high, low and median scores across sectors, as shown in Figure 5. The Consumer 100 has the widest range, followed by the News 100 and FDIC 100. Note that some maximum scores exceeded 100 due to bonus points. This chart illustrates how the medians for several sectors (especially online retailers and the FDIC 100) sit at the 80% threshold, meaning many new sites could qualify for the Honor Roll through simple operational changes and support of best practices. Several sectors saw significant improvement in their median scores, with News sites rising 8 points, Federal sites rising 7 points and Consumer sites rising 5 points since last year.

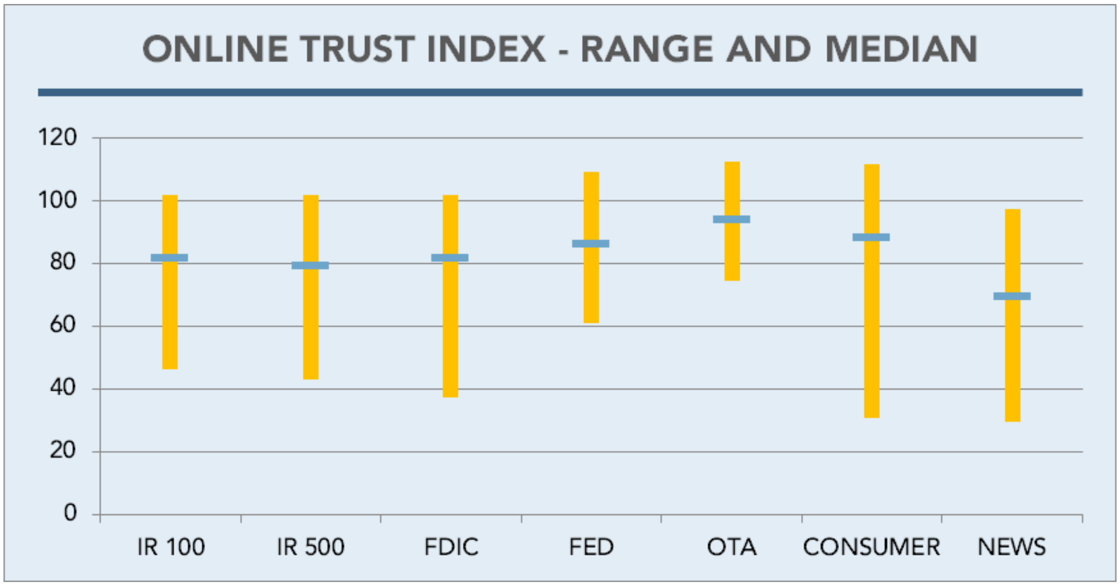


Figure 5 – Range and Median Online Trust Index Scores by Sector

Figure 6 shows the baseline scoring breakdown (out of 100) for all sectors by major category. This chart shows much more variability than the median scores, especially in the Consumer Protection and Privacy categories. Site security scores are more tightly clustered.

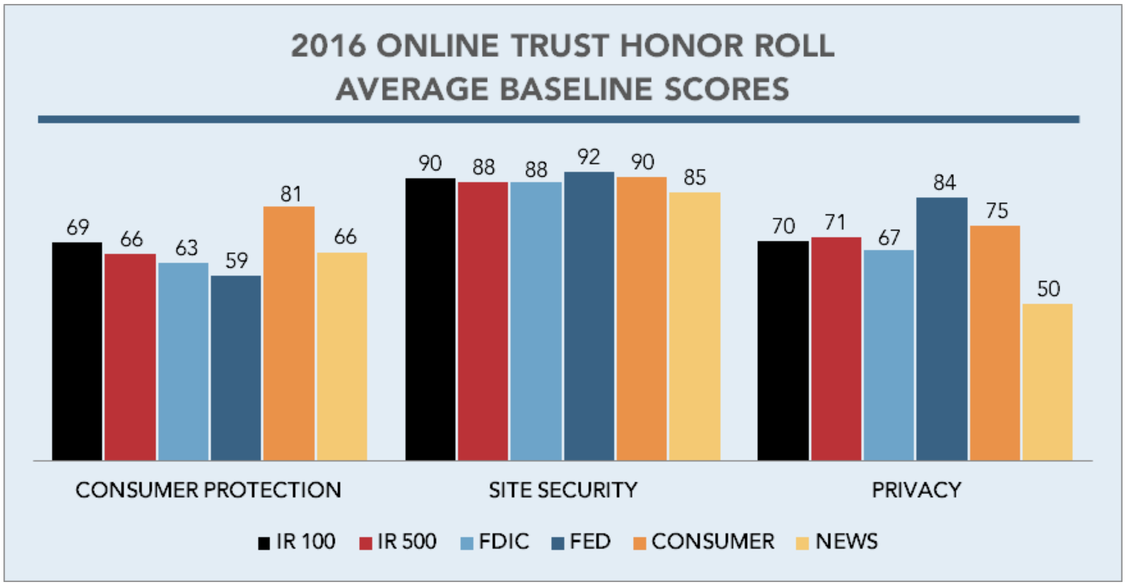


Figure 6 – Major Category Scores by Sector

The primary driver of Consumer Protection scores is the implementation of email authentication on top-level and subdomains. Low scores are primarily due to lack of support at the top-level domains. This remains a concern since the majority of spoofing and malicious email purports to be sent from the recognizable corporate domains rather than marketing subdomains which are often delegated to email service providers. While marketers have embraced email authentication to drive inbox placement, increased focus and engagement is needed to maximize consumer protection for all domains.

Building on these email authentication protocols, DMARC provides ISPs and corporate networks direction on how to handle email that fails authentication. Since use of DMARC has no cost or impact to server performance, the low adoption is concerning and may be indicative of low awareness of the criticality and business value.

"Publishers Clearing House is proud to have evolved our data stewardship and privacy practices to meet the higher bar and be recognized by OTA for our efforts. Data stewardship, self-regulation and commitment to taking a holistic view of security & privacy is a cornerstone of any business looking to strive in today's evolving landscape. We believe continued success and growth is based on a long term commitment and investment in data security as we strive to continually maintain transparency and trust with our members," said Sal Tripi, AVP Digital Operations and Compliance, Publishers Clearing House.

Overall privacy scores dipped modestly this year – in general, policy scores improved slightly while tracking scores dropped, yielding a net loss. Sector scores vary widely (a 34 point range). Several new elements were introduced into the baseline privacy policy scoring this year (e.g., layered notice, Do Not Track disclosure) which lowered scores in some sectors. Nearly one-third more "promiscuous" trackers were observed this year than in 2015, dragging down overall privacy scores. OTA encourages all sites to evaluate their privacy policies and practices and take steps to update them to reflect actual practices and respect for consumer privacy.

METHODOLOGY & SCORING

The Audit criteria are highly relevant to the security and privacy practices companies must implement to maximize online trust and consumer protection. Created through a public call for comments and in consultation with subject matter experts, they reflect widely accepted industry standards and practices. In addition, several U.S. government agencies were consulted, incorporating some of their core security and privacy directives including Fair Information Practice Principles (FIPPs), NIST standards, and Office of Management and Budget (OMB) cybersecurity and privacy related directives.[5] Feedback and recommendations were incorporated into the 2016 methodology published in March.[6]

The 2016 Online Trust Audit includes a composite analysis focusing on three major categories:

- Consumer Protection
- Site, Server & Infrastructure Security
- Privacy, Transparency & Disclosures

Sites were eligible to receive 300 base points (up to 100 points in each category), and up to 70 bonus points for implementing emerging best practices. Additionally, organizations could lose up to 80 points for having regulatory settlements, data breaches, observed vulnerabilities and other key deficiencies. The criteria are adjusted annually, raising the bar to address the evolving threat landscape and responsible privacy practices. Combined, they underscore the need for sites to continually monitor their security and privacy practices.

> *"Consumers need confidence that their data is secure and privacy is respected," said Roxane Divol, senior vice president and general manager, Website Security, Symantec. "As an Honor Roll recipient, Symantec encourages all sites to embrace these practices including encrypting all their site traffic, helping to enhance the privacy and security as consumers browse, bank, and buy online."*

To qualify for the Honor Roll, sites had to receive a composite score of 80% or better ***and*** a score of at least 55 in each of the three main categories. In addition, if any site had multiple data breaches within the past twelve months, they were disqualified, independent of their aggregate score. The minimum scoring requirement was instituted recognizing that sites are built on a "chain of trust" that is only as strong as its weakest link.

Data sampling was completed between April 15 and May 10, 2016 by OTA and over a dozen data providers. It is important to note that a site's configuration or practices may have changed since the sampling and the data only reflects findings during this snapshot in time.

[5] OMB Directive October 30, 2015 https://www.whitehouse.gov/sites/default/files/omb/memoranda/2016/m-16-03.pdf

[6] 2016 methodology and resources https://otalliance.org/initiatives/2016-methodology

DOMAIN, BRAND & CONSUMER PROTECTION

Best practices to help detect and block malicious and spoofed email. Adoption helps protect consumers and email recipients from distribution of malware, key loggers and related threats including ransomware and account takeovers, while additionally protecting the reputation of the target brand.

- Email authentication (Sender Policy Framework (SPF) and DomainKeys Identified Mail (DKIM)) at top-level ("corporate") domains, and all email subdomains. The 2016 Audit increases weighting on the top level, with reduced points for separate delegated sub-domains – *part of base score* [7]
- Domain-based Message Authentication, Reporting & Conformance (DMARC) – *part of base score (increased weighting for "reject" policies)* [8]
- Implementation of "opportunistic" Transport Layered Security (TLS) for email – *bonus points* [9]
- Domain Name System Security Extension (DNSSEC) – *bonus points* [10]
- Implementation of Internet Protocol version 6 (IPv6) – *bonus points* [11]
- Domain locking – *penalty if domain not locked*

SITE, SERVER & INFRASTRUCTURE SECURITY

Best practices to secure data in transit and collected by websites, and prevent malicious exploits running against clients' devices. Sites were eligible to score up to 100 base points, provided any single core criteria (ciphers, key exchange or protocol support) did not score below 55. Sites were tested with several tools to look for known vulnerabilities, HSTS configuration and mismatched certificates. [12, 13]

Bonus / Penalty Points

- Extended Validation SSL Certificates (EV SSL) – *bonus points* [14]
- Adoption of Always On SSL (AOSSL) – *bonus points (increased weight in 2016)*[15]
- Evaluation of SSL Certificate type (Domain Validation [DV] or Organization Validation [OV]) – *penalty for use of DV certificates*
- Web Application Firewall – *bonus points*
- Bot detection and mitigation solutions – *penalty if vulnerable to basic attacks*
- Testing for XSS, iframe exploits, malware, malicious links – *penalty if these threats exist*
- Malvertising incidents – *(new) penalty if incidents have been observed since January, 2015* [16]

[7] https://otalliance.org/eauth
[8] https://otalliance.org/DMARC
[9] https://otalliance.org/best-practices/transport-layered-security-tls-email
[10] DNSSEC https://en.wikipedia.org/wiki/Domain_Name_System_Security_Extensions
[11] IPv6 https://en.wikipedia.org/wiki/IPv6
[12] Qualys SSL Labshttps://ota.ssllabs.com/
[13] High-Tech Bridge SA https://www.htbridge.com/ssl/
[14] EVSSL https://otalliance.org/resources/extended-validation-certificates-evssl
[15] AOSSL https://otalliance.org/AOSSL
[16] Malvertising https://otalliance.org/malvertising

PRIVACY, TRANSPARENCY & DISCLOSURES

Best practices providing users clear notice and control of the data being collected, tracked and shared with third parties. The privacy score is comprised of up to 50 points for disclosures and structure of the privacy policy including generally accepted Fair Information Practice Principles (FIPPS), and up to 50 points for tracking and data collection by third parties.[17]

Privacy Policy – up to 50 points. Sites receive maximum scores by adhering to the following guidelines:

- Personal data not shared with any third party
- Vendor confidentiality – disclosure that service providers are prohibited from the use or sharing of data for any purposes other than providing services on behalf of the site.
- Data retention policy
- Link / discoverability from the home page
- Designed as a layered and/or short notice
- Disclosure and response on handling of a browser Do Not Track (DNT) setting
- Compliance with Children's Online Privacy Protection Act [18]

> *"We're honored to be recognized in the Online Trust Alliance Honor Roll for the second year in a row. Through its benchmarking work, the OTA is helping security leaders like LifeLock act as trusted stewards of the data we protect. We support its mission to make the internet a safer place by driving the adoption of security best practices industrywide." said Neil Daswani, Chief Information Security Officer at LifeLock.*

Third-Party Tracking on Site – 50 points possible for sites with no third-party trackers (with the exception of anonymous analytics for site performance and metrics). Each observed tracker known to share data resulted in reduction of the possible 50 points.

Bonus Points

- Date stamping of privacy policy on the top of the page
- Version tracking including posting of marked up previous versions
- Use of consumer-friendly icons to assist navigation
- Localized/multi-lingual policy in at least one language other than English
- Honoring of Do Not Track browser settings
- Implementation of tag management systems or privacy solutions

Penalty Points

- Public vs. Private WHOIS registration – *penalty if private*
- Data breach & loss incidents – *penalty if incident since January, 2015 (automatic failure if multiple incidents)*
- FTC / State legal settlements – *penalty if settlement since January, 2015*

[17] FIPPS http://www.nist.gov/nstic/NSTIC-FIPPs.pdf

[18] COPPA https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions

BEST PRACTICES & SECTOR HIGHLIGHTS

In addition to assessing overall Honor Roll achievement, it is instructive to look at adoption trends for the various best practices as well as trends within sectors. The following sections summarize the key findings.

BEST PRACTICES HIGHLIGHTS

DOMAIN, BRAND & CONSUMER PROTECTION

- Email Authentication (SPF & DKIM) – Record levels of adoption were observed this year. Use of either SPF or DKIM averaged 97% overall, with growth in every sector. The most dramatic growth was observed in use of DKIM at the top-level domain (31% to 47%) and use of both SPF and DKIM (the recommended best practice), which grew from 71% to 82%. The sector making the biggest advance was the News 100, which grew from 56% to 75% in use of both SPF and DKIM (as well as growth from 16% to 50% in use of DKIM at the top-level domain).

> *"Consumer trust is the foundation for eCommerce companies like ours, and we work hard to earn that trust through ongoing efforts to adopt responsible security and privacy practices," said Jim Bramson, LivingSocial's head of corporate affairs. "We are pleased to be recognized on the Online Trust Honor Roll, and appreciate the efforts of OTA to socialize best practices for safeguarding consumer confidence."*

- Domain-based Message Authentication, Reporting & Conformance (DMARC) – Adoption nearly doubled from 17% to 31%. Consumer sites led with 64% adoption, while other sectors were in the 20-30% range. Considering the ease of implementation and quantifiable benefits, this is an area that deserves continued attention. For organizations with a DMARC record, use of "reject" or "quarantine" policies remains flat at approximately 20%.
- Opportunistic Transport Layered Security (TLS) – TLS encrypts email messages between mail servers, preventing eavesdropping in transit. Dramatic growth was observed, from 23% in 2015 to 61% this year. Adoption is above 50% in all sectors, with News sites leading at 69%. Industry momentum and attention, led by Google and Twitter, will likely cause continued growth and this element may soon move to baseline scoring.
- IPv6 – Examination of IPv6 adoption has been added to the 2016 Audit, recognizing the long-term importance to the growth and resiliency of the internet. The Federal 50 led adoption (84%), followed by OTA members (13%) and Consumer sites (10%). All other sectors had adoption of 2% or less.

SITE, SERVER & INFRASTRUCTURE SECURITY

- SSL Server Configuration – Despite more rigid criteria, scores rose in all sectors, and the overall average rose from 85 to 89. Federal sites had the largest increase, with scores rising from 84 to 92.
- Extended Validation SSL Certificates (EV SSL) – EV SSL offers added verification of a site's reputation, providing a browser visual trust indicator and increased transparency about the site's ownership. Adoption is led by FDIC sites (70%) with most other sectors in the 25%-35% range.

- **Always On SSL (AOSSL)** – AOSSL fully encrypts the web session between the client device and website, offering increased privacy and security when sharing information. Overall adoption saw solid growth, from 24% to 32%, with growth in all but News sites. FDIC sites lead all sectors with 81% adoption, and Consumer, Federal and OTA sites have reached the 50% mark. Because this standard is now being promoted by Google, several browsers and the Federal government, growth in adoption is expected to continue, with likely incorporation into baseline scoring in the near future.

- **XSS/iframe Vulnerability** – This area rose dramatically, from 8% last year to 26%, and was most pronounced in the online retailers (4% to 22%) which comprise over half of the audited sites. Based on these results, organizations should closely examine their sites to reduce such vulnerabilities.

- **Anti-bot Protection** – This area suffered a setback, revealing that 26% of sites are vulnerable to basic bot attacks (vs. 15% last year). Part of this gap is due to more rigorous testing criteria, but sites should ensure they are protected from emerging, more sophisticated bot attacks.

- **Malvertising** – Added in 2016, analysis was focused on the News 100 to assess malvertising incidents. 17% of sites had incidents, and many suffered multiple incidents (as many as 12) since January, 2015.

PRIVACY, TRANSPARENCY & DISCLOSURES

- **Overall Privacy Scores –** Overall scores dipped this year (from 73 to 70), mostly due to additional baseline criteria, more stringent scoring of privacy policies and a 30% rise in third-party trackers seen on sites. FDIC sites showed the largest drop (76.1 to 67.1), while Consumer sites and OTA members dipped slightly. Top retailers, News sites and Federal sites were essentially flat.

- **Data Sharing with Third Parties –** Inclusion of language stating that data is not shared (except for delivery of service) dropped significantly this year, from 77% to 64%. A reduction was observed in all but the Federal 50, and had the biggest impact on FDIC sites, where sharing among "affiliates" remains commonplace. In part the drop can be attributed to more rigorous scoring of privacy policy language. OTA encourages all organizations to evaluate and tighten their data sharing language.

- **Data Retention Disclosure –** This element has been a baseline component for several years, and measures whether sites address for what purpose and for how long they will retain data. Adoption grew from 26% in 2015 to 36% this year.

- **Vendor Confidentiality –** Assesses whether third parties are restricted from sharing or using data except to deliver core services. Consumer sites led with 78% adoption while most sectors are clustered around 55%. The notable exception is the FDIC 100 which has an adoption rate of only 27%.

- **Policy Discoverable on Home Page –** Added to baseline scoring this year. This practice is widely adopted, averaging 95% overall. The Internet Retailer Top 100 leads with 99% adoption while Federal sites trail with 88% adoption.

- **Date Stamp / Version Tracking –** Added in 2016 as bonus points. 74% of sites provide a date stamp, ranging from Federal sites at 58% to Consumer sites at 92%. Overall, 6% of sites provide access to previous versions, led by Consumer sites at 13%. Only the FDIC sector has no version tracking.

- **Layered Notice** – Adoption of this practice grew solidly (from 21% to 26%) as part of the baseline scoring. Leading sectors were the Federal sites and Internet Retailer Top 100 (44% and 43% respectively), followed closely by News sites (39%). FDIC sites lag with 12% adoption.
- **Do Not Track (DNT) Disclosure** – Introduced in 2014, this tracks whether the privacy policy discloses how a site responds to a DNT setting. It has seen solid, steady growth, from 13% to 23% to 33% over the past three years. News sites lead with 54% adoption followed closely by the Internet Retailer Top 100 at 51%.
- **Honoring of Do Not Track (DNT) Browser Settings** – Though growing (1% in 2015 to 4% this year), honoring of DNT remains at a very low adoption rate. Consumer sites lead with 8% adoption.
- **Support of Tag Management/Privacy Solution** – Tracks whether a site utilizes a tag management system or privacy solution, and was added to reflect the complexity of managing third-party tags. Adoption has risen from 42% to 55% to 66% over the past three years, and is well on its way to becoming a baseline scoring component. News sites lead adoption at 89% (likely due to their heavy use of third-party trackers and advertising), followed by the Internet Retailer Top 100 at 78%. Not surprisingly, Federal sites lag at 26% since they do not rely on advertising and therefore have little need for such solutions.
- **Data Breach & Loss Incidents** – 2015 had many high profile breaches. Of the audited sites, 35 had breaches in this year, up slightly from the 32 observed last year but well below the 58 noted two years ago. The Internet Retailer Top 100 had the highest rate (12%), followed by Federal sites (10%) and Consumer sites (8%). The penalty for such incidents was tripled last year, and a rule was instituted this year that multiple breaches since January 2015 would result in automatic failure.
- **FTC / State Settlements –** Ten organizations received a penalty for FTC suits or settlements (up from five last year), with more than half occurring in the Internet Retailer 500.

SECTOR HIGHLIGHTS

INTERNET RETAILER TOP 500

- Top five scores were 1) Gap, 2) LivingSocial, 3) Warby Parker, 4) (3-way tie) Google Play, Pep Boys and Weight Watchers.
- Solid increase in adoption of all forms of email authentication, best captured in the measure of support for both SPF and DKIM (grew from 78% to 85%). Nearly tripled adoption of DMARC records (8% to 21%).
- Growth of AOSSL securing the entire web session (13% to 18%), though there is room for improvement. Site security scores grew modestly, privacy scores were flat, and Honor Roll achievement grew slightly.

FDIC TOP 100 BANKS

- Top five scores were 1) IBERIABANK, 2) First-Citizen's Bank & Trust Company, 3) USAA Federal Savings, 4) Wells Fargo, 5) State Farm Bank.
- Consistent, significant growth in Honor Roll achievement (33% in 2014 to 46% in 2015 to 55% this year), despite lower privacy scores in 2016. Far outpaces all sectors in EV SSL adoption (70%) and AOSSL adoption (81%).
- Solid growth in email authentication and DMARC, yet more than one-third failed in this area. Privacy scores dipped significantly (76 to 67) due to more rigid policy scoring. Site security grew modestly.

CONSUMER SERVICES 100

- Top five scores were 1) Twitter, 2) Pinterest, 3) Dropbox, 4) FileYourTaxes, 5) LifeLock.
- Demonstrated the highest Honor Roll achievement (72%, up from 58% last year). This is due in part to the expanded number of sites in the sector since the new sites had a higher than average achievement rate. 64% of sites assessed in 2015 made the Honor Roll this year, which is still an improvement from 58% last year.
- Highest adoption of all email authentication elements, and saw significant growth in DKIM at the TLD (56% to 76%), support for both SPF and DKIM (76% to 86%) and use of DMARC records (48% to 64%). Strong growth in adoption of AOSSL (35% to 50%).

IRS Free e-file Audit Update

OTA released an audit of the 13 IRS free e-file sites in February, 2016, finding that 54% made the Honor Roll based on the 2015 methodology. As part of the 2016 Audit, the sites (now part of the Consumer 100) were re-assessed.

Since the February report, several e-File providers reached out to OTA for advice, attended public webinars and made improvements in email authentication, site security and privacy practices. As a result, 100% qualified for the 2016 Honor Roll.

FEDERAL 50

- Top five scores were 1) HealthCare.gov, 2) the White House, 3) the Federal Trade Commission, 4) the Social Security Administration, 5) the U.S Postal Service.
- This sector is a study in extremes. Honor Roll achievement is solid (46%, up from 42% in 2015). Privacy and Site Security baseline scores are the highest of all sectors yet the Consumer Protection baseline score is the lowest (59, well below overall average of 68). 50% of sites fail due to lack of email authentication.
- Bright spots are continued growth in email authentication (though still lagging), use of DMARC reject records (40%, the highest of all sectors), DNSSEC adoption (88%), use of IPv6 (84%), nearly tripling adoption of AOSSL (from 17% to 50%) and the highest adoption of "data not shared" language and layered notices (92% and 44% respectively).
- The FDIC was disqualified from the 2016 Honor Roll after their recent disclosure to Congress suggested that at least five major data breaches occurred since Oct. 30, 2015. While a single data breach or loss incident does not result in automatic failure, multiple incidents within a short time yields a failing score. Also, the FDIC failed to notify impacted consumers, raising additional concerns. Without their breaches, they would have ranked within the top 10% of U.S. federal government sites.[19]

Assessing States

OTA had planned to assess the 50 states as part of an expanded "Government 100" this year. During the analysis it became apparent that states are comprised of dozens of departments with widely varying practices.

Due to this disparity, OTA determined it would be misleading to assign a single score to a state since it may significantly misstate the adoption of best practices. Future Audits may include states, focusing on specific agency(s). OTA encourages states to examine their departments based on 2016 Audit criteria.

[19] FDIC data breaches http://www.pymnts.com/news/security-and-risk/2016/fdic-congress-data-breach-hearing/

NEWS & MEDIA 100

- Top five scores were 1) Google News, 2) Reddit, 3) Yahoo News, 4) BuzzFeed, 5) MSN News.
- Dramatic growth in Honor Roll achievement (nearly tripling to 23%), though by far the lowest scoring sector. Overall failure rate of 73%, mainly driven by failures in Privacy (58%) and Consumer Protection (31%). Low privacy scores are primarily due to heavy use of third-party site trackers.
- Though total privacy scores are low due to trackers, leads all sectors in several privacy-related components – use of tag management/privacy solutions (89%), Do Not Track disclosure (54%) and use of multi-lingual policies (12%). Also at the upper end of adoption of layered notices (39%).
- During the audit it was noted that several sites allowed signup/login with no obvious use of SSL/TLS, which is a security and privacy concern since private information is being transmitted "in the clear."

DOMAIN, BRAND & CONSUMER PROTECTION

By utilizing email authentication (SPF and DKIM), organizations can help protect their brands and prevent consumers from receiving spoofed and forged email. Email authentication allows senders to specify who is authorized to send email on their behalf. Building on email authentication protocols, DMARC adds a policy assertion providing receivers direction on how to handle messages that fail authentication. TLS provides a means to encrypt messages between mail servers, protecting both the brand and consumer. Domain locking ensures that domain ownership cannot be transferred without the owner's permission. Domain Name System Security Extension (DNSSEC) adds security and integrity to the DNS, helping to prevent "Man-in-the-Middle" (MitM) attacks, cache poisoning and related DNS attacks.

IPv6 has been added to the 2016 Audit providing early adopter sites bonus points for this enhancement in internet architecture, which expands the number of unique IP addresses with added security benefits.[20] [21]

Best practices include:

- Implement both SPF and DKIM for top-level domains, "parked" domains (not used for email) and any major subdomains seen on websites or used for email.
- Implement DMARC, initially in "monitor" mode to get receiver feedback and verify accuracy of email authentication, and eventually to assert a "reject" or "quarantine" policy to receivers.
- Implement inbound email authentication checks and DMARC on all networks to help protect against malicious email and spearphishing purporting to come from legitimate senders.
- Implement opportunistic TLS to protect email in transit between mail servers.
- Ensure that domains are locked to prevent domain takeovers.
- Implement DNSSEC to help protect a site's DNS infrastructure.
- Plan for IPv6 deployment.

[20] Why You Need IPv6 https://www.infoblox.com/solutions/ipv6-readiness

[21] IPv6 Security Considerations http://www.networkworld.com/article/2177807/tech-primers/8-security-considerations-for-ipv6-deployment.html

EMAIL AUTHENTICATION

The 2016 Audit included additional telemetry providing a more precise view of authentication across all sectors. Authentication technologies, namely Sender Policy Framework (SPF) and DomainKeys Identified Mail (DKIM), help prevent phishing and spam. OTA recommends use of email authentication at the top-level (or "corporate") domain (TLD) as well as any other domains used for sending email or that might be used to fool consumers. Authentication at the TLD was given increased weight in the 2016 methodology.

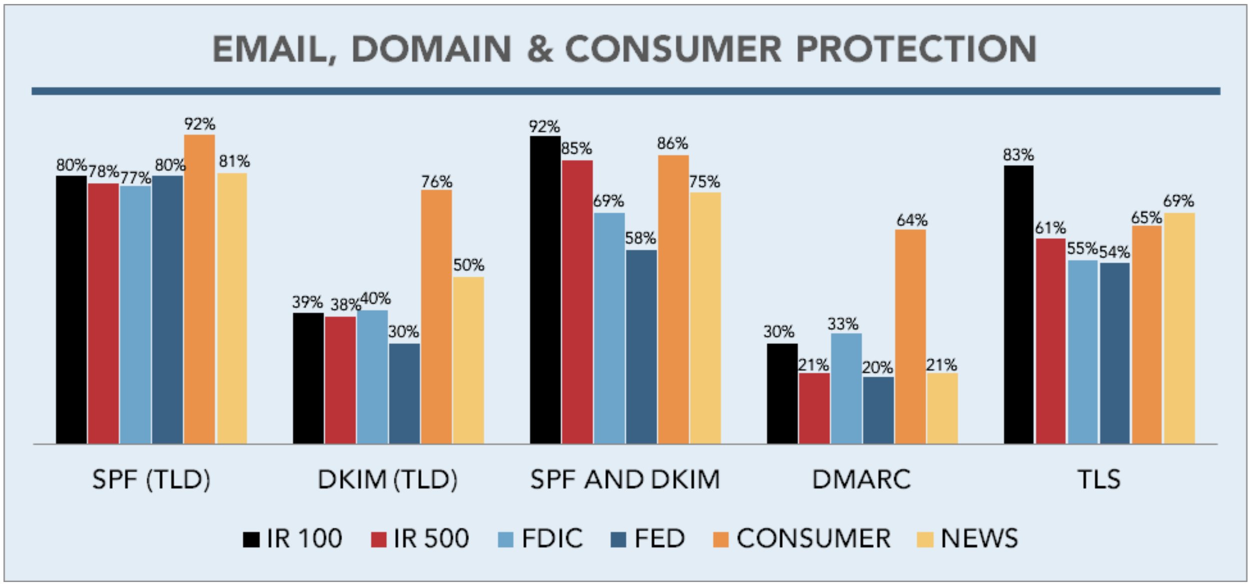


Figure 7 – Email Authentication, DMARC, TLS Adoption by Sector

Figure 7 above shows adoption of SPF and DKIM at the TLD, combined use of SPF and DKIM at any level, adoption of DMARC records and use of TLS. In general SPF adoption is higher than DKIM primarily due to its ease of implementation, whereas DKIM requires updates to outbound mail servers.

Adoption of both SPF and DKIM best enables receivers to detect and block malicious email, while reducing the risk of false positives. As seen in Figure 8, this dual approach grew in all sectors in 2016, most dramatically in the News, Federal and Consumer sectors. Online retailers and consumer services platforms, which are most heavily reliant on email interaction with their users/customers, have recognized the brand value of email authentication. Though encouraging overall, it is unfortunate that most of the growth in use of both SPF and DKIM has occurred via marketing specific subdomains (note the 25-50% gap between "DKIM TLD" and "SPF and DKIM" in Figure 7). Further effort is needed to implement DKIM to protect top-level and corporate domains from abuse.

Across all sectors, OTA found 43 instances of SPF records ending in "?all" (two-thirds of which were online retailers). This syntax indicates the record is for testing purposes only and should be ignored. Likewise, four instances of SPF records ending in "+all" were observed – this indicates that any IP address can send on behalf of the domain, which opens up the domain for abuse. Neither "?all" or "+all" records were counted as valid.

As noted in the recommended best practices, inbound authentication checks and application of DMARC policies is becoming increasingly important due to the increased precision of business email compromises.

CONSUMER PROTECTION
BOTH SPF AND DKIM

	2013	2014	2015	2016
Internet Retailer Top 100	76%	88%	90%	92%
Internet Retailer Top 500	56%	74%	78%	85%
FDIC 100	49%	49%	63%	69%
Federal 50	20%	22%	48%	58%
Consumer 100	72%	74%	76%	86%
News 100	-	50%	56%	75%
OTA Members	69%	83%	94%	99%

Figure 8 – Adoption of Both SPF and DKIM by Sector

DOMAIN-BASED MESSAGE AUTHENTICATION, REPORTING & CONFORMANCE (DMARC)

DMARC builds on SPF and DKIM results, provides a means for feedback reports and adds visibility for receivers on how to process unauthenticated email. Added to baseline scoring in 2013, additional weight was given for use of DMARC reject and quarantine policies in 2016, with maximum points awarded to reject policies.

As illustrated in Figure 9, adoption of DMARC grew in all sectors (except for a slight dip in OTA due to the addition of new members), and most made large leaps (top retailers nearly tripled, News sites more than doubled). Given the gap between SPF/DKIM adoption (above 90% in many sectors) and DMARC adoption (below 30% in most sectors), there is still significant room for growth in use of DMARC. The "R or Q" column shows the percentage of organizations with a DMARC record that publish a reject or quarantine policy, illustrating significant room for growth in nearly all sectors.

CONSUMER PROTECTION
DMARC ADOPTION

	2013	2014	2015	2016	
	Record	Record	Record	Record	R or Q*
Internet Retailer Top 100	5%	15%	20%	30%	17%
Internet Retailer Top 500	3%	6%	8%	21%	14%
FDIC 100	13%	21%	24%	33%	24%
Federal 50	4%	6%	14%	20%	40%
Consumer 100	22%	36%	48%	64%	29%
News 100	-	10%	10%	21%	14%
OTA Members	44%	59%	77%	75%	25%

Figure 9 – DMARC Adoption by Sector

*as % of those with DMARC record

OPPORTUNISTIC TRANSPORT LAYERED SECURITY (TLS) FOR EMAIL

Tracking of Opportunistic TLS was added in 2015 to help address mounting privacy concerns regarding email in transit. TLS encrypts messages in transit from one server to another and decrypts messages before they are delivered to a user's device. TLS adoption grew dramatically from 2015 (averaging 23%) to 2016, where it ranged from 54% (Federal sites) to 83% (Top 100 Internet Retailers), averaging 61%.

> *"As a leading provider of cyber insurance and reinsurance, HSB takes cyber security seriously. We share the OTA's focus on raising awareness and online safety best practices and we are pleased to be recognized for our commitment to cyber security." - - Eric Cernak, VP Cyber Risk Practice Leader, Hartford Steam Boiler*

DOMAIN LOCKING

Domain locking became a scoring element in 2013 due to its importance in prevention of domain takeovers (a penalty is assigned if the domain is not locked). More than 96% of organizations across all sectors lock their domains (vs. 94% last year). Consumer sites lead at 98%, while News sites trail at 95%.

DOMAIN NAME SYSTEM SECURITY EXTENSION (DNSSEC)

DNSSEC adds security to the DNS lookup. It is designed to help combat "Man-in-the-Middle" (MitM) attacks and cache poisoning by authenticating the origin of DNS data and verifying its integrity while moving through the Internet. DNSSEC is now deployed in the .com, .gov, .org and .net TLD's, potentially supporting more than 90 million .com domain name registrations worldwide.

DNSSEC adoption remained flat this year, with only Federal sites having significant adoption (88%) in response to a Presidential directive. Other sectors with DNSSEC adoption are OTA members (7%), News (2%), FDIC (2%) and online Retailers (0.6%). Broad implementation of DNSSEC continues to be hampered by legacy systems and lack of ecosystem infrastructure (hosting environments, registrars and browsers).

INTERNET PROTOCOL VERSION 6 (IPV6)

IPv6 is the most recent version of the Internet Protocol (IP), the communications protocol that provides an identification and location system for computers across the internet. In addition to significantly expanding the number of available addresses, IPv6 provides a range of benefits for security, integrity and performance. OTA supports broader deployment, awarding bonus points for early adopters.

The IPv6 specification mandates that IPsec be implemented, which helps enable sender authentication and end-to-end encryption for secure communications. While this technology was retrofitted into IPv4, it remains an optional extra that isn't universally implemented in all IPv4 stacks, or deployed in all IPv4 environments. The encryption and integrity-checking afforded by IPsec and used in current VPNs is available as a standard component in IPv6, supported by all standards-compliant devices and systems. Widespread adoption of IPv6 with IPsec enabled helps to prevent an array of attacks.

SITE, SERVER & INFRASTRUCTURE SECURITY

A site's trustworthiness is largely defined by the security of the infrastructure. Users need assurance that the site and their data are secure. Proper implementation of best practices in this category also protects the site itself from attack. Best practices include:

- Optimize SSL/TLS implementation using information gleaned from public tools,[22,23] focusing on vulnerabilities that earn a letter grade of "F" or that have failure (55 points or less) in a major subcomponent of the scoring (which normally leads to an overall grade of "C"). This includes eliminating support of SSLv2 and associated vulnerabilities to the DROWN exploit.[24]
- Use EV SSL for brands and sites which are frequently spoofed and for sites where users need to be assured they are visiting and browsing a legitimate site.
- Replace Domain Validated certificates with Organization or Extended Validation SSL certificates.
- Implement AOSSL or HTTPS on all pages to maximize data security and online privacy.
- Implement a Web Application Firewall to monitor HTTP conversations and block common attacks such as cross-site scripting (XSS) and SQL injections.
- Proactively scan sites for malicious links, iFrame exploits, malware and malvertising.[25]
- Implement bot detection and mitigation to help prevent brute force attacks, web scraping, account hijacking, unauthorized vulnerability scans, spam, and man-in-the-middle attacks.

> *"At Gap Inc., we work tirelessly to provide a safe and secure digital shopping environment for our customers, and we are committed to protecting the privacy of our customer data," said Rich Noguera, Chief Information Security Officer, Gap Inc. "We're honored to be recognized as the top retailer in the 2016 Online Trust Audit and Honor Roll."*

The bar was raised this year in security scoring by combining results from High-Tech Bridge and Qualys SSL Labs, providing a more thorough site security analysis. Further, additional bonus weight was applied to sites supporting AOSSL, and penalties were increased for use of Domain Validated (DV) certificates.

As illustrated in Figure 10, summary scores are in a relatively narrow range, while the adoption rate of key enhancements varies widely:

- SSL scores, which represent the baseline score in this category, are tightly concentrated around the overall average of 88.5.
- EV SSL adoption varies significantly across sectors – it is highest in the FDIC (70%, which outpaces all other sectors 2:1) and lowest for News sites (6%) and Federal sites (10%).
- AOSSL helps ensure that all data exchanged between the site and device is encrypted. Overall adoption of grew from 24% to 32%, yet adoption varies widely – from 81% in FDIC sites to only 4% for News sites. Dramatic growth was observed by Federal sites (17% to 50%) due in part to a White House mandate. Consumer sites grew significantly, from 35% to 50%.

[22] High-Tech Bridge SA https://www.htbridge.com/ssl/
[23] Qualys SSL Labs https://ota.ssllabs.com/
[24] DROWN (Decrypting RSA with Obsolete and Weakened eNcryption) https://drownattack.com/
[25] https://otalliance.org/resources/type/advertising-integrity-fraud

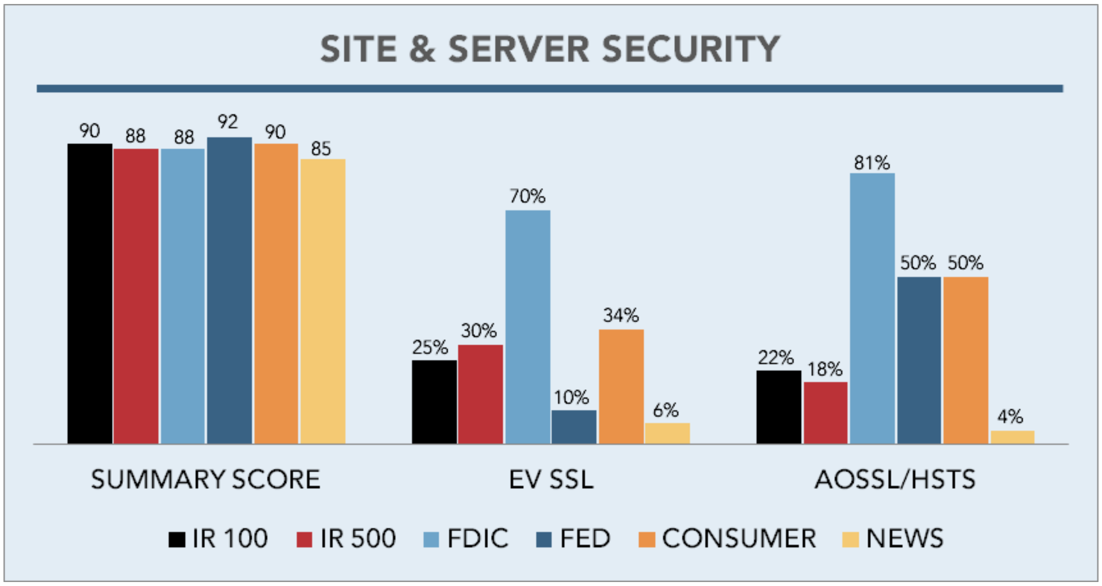


Figure 10 – Site & Server Security Scores/Adoption by Sector

SERVER IMPLEMENTATION & VULNERABILITY ANALYSIS

Ongoing SSL/TLS configuration is a core mechanism sites can use to minimize vulnerabilities. In the May 2016 SSL Pulse report, 43.1% of the 140,865 sites tested were considered secure, a dramatic increase from the 18.4% considered secure in June 2015 and from 28.4% in 2014.[26]

Site Security scores incorporated data from DigiCert, Distil Networks, GlobalSign, High-Tech Bridge, Qualys SSL Labs, SiteLock and Symantec. Collectively the data was used to evaluate sites' SSL/TLS implementation, EV SSL adoption, AOSSL adoption, use of web application firewalls and vulnerability to cross-site scripting (XSS), iframe exploits, malware, malicious links and bot exploits.

In the process of analyzing the site security scores, several trends were observed:

- Many sites still use old, vulnerable ciphers, which creates moderate risk when used in conjunction with older protocols and high risk when used with current protocols
- Many sites do not support TLS1.2, the latest, safest protocol (lack of TLS1.2 led to failure of the category)
- Many sites have mismatched certificates (i.e., the name on the certificate does not match the name of the site). Most browsers will flag this disconnect, dramatically reducing trust in the site. This issue was most prevalent in News sites (22%) and Federal sites (12%).
- A high percentage of sites have weak intermediate certificates, meaning that they use a SHA-1 hash algorithm in the chain of certificates – they should upgrade to SHA-2.
- Several sites still support SSLv2, which garners a grade of "F", and is associated with the DROWN exploit.

[26] Source: Trustworthy Internet Movement 2016 report https://www.trustworthyinternet.org/ssl-pulse

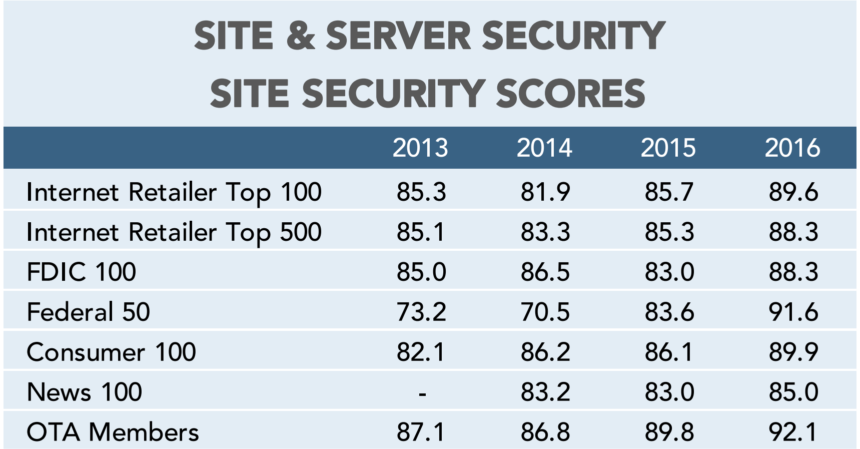
Presence of malicious links and malware was not found on any sampled site, though XSS/iframe vulnerabilities were observed on nearly 26% of sites, more than a three-fold increase from the 8% observed last year. The FDIC had the lowest presence of XSS/iframe vulnerabilities at 10%, but more than half of the News sites and nearly half of the Federal sites were vulnerable. This increase is concerning, and sites in all sectors need to focus on this area and address the vulnerabilities.

Use of a web application firewall can help block attacks on these vulnerabilities. Overall adoption was flat at 35%, led by the Internet Retailer Top 100 (49%) and Federal sites (46%), while Consumer sites had the lowest adoption rate (18%).

Increasingly, sites' vulnerabilities are being targeted by bot-orchestrated exploits as criminal networks leverage computing power for their illicit gain. Along with the proliferation of bot attacks, the severity and damage of these attacks has similarly increased. While earlier bot attacks were largely regarded as a nuisance, today's bot attacks can paralyze website infrastructure, pirate entire online directories, and destroy a company's competitive advantage.

> *"Trust is the foundation of the digital economy. The OTA's Online Trust Audit reinforces the need for all organizations to invest in security, privacy and the consumer experience", said Joseph Yanoska, Executive Director, American Greetings Interactive. "As a recipient of OTA's 2016 Honor Roll we are honored to be recognized for our efforts."*

In order to combat these alarming trends, companies should consider reinforcing their security strategy with the addition of proactive bot detection and mitigation solutions. Testing for basic anti-bot solutions this year was more rigorous, yielding a drop in overall adoption from 86% to 75%. Three additional levels of anti-bot scans were conducted, and showed that only 12% of sites were protected from "simple" bots, only 2% were protected from bots emulating browsers, and less than 1% were protected from "advanced" bots. Retailers had the best anti-bot protection while News and FDIC sites had the least. With the advent of more sophisticated bots, sites need to closely examine and address these vulnerabilities.



SITE & SERVER SECURITY

SITE SECURITY SCORES

	2013	2014	2015	2016
Internet Retailer Top 100	85.3	81.9	85.7	89.6
Internet Retailer Top 500	85.1	83.3	85.3	88.3
FDIC 100	85.0	86.5	83.0	88.3
Federal 50	73.2	70.5	83.6	91.6
Consumer 100	82.1	86.2	86.1	89.9
News 100	-	83.2	83.0	85.0
OTA Members	87.1	86.8	89.8	92.1

Figure 11 – Site Security Score Average by Sector

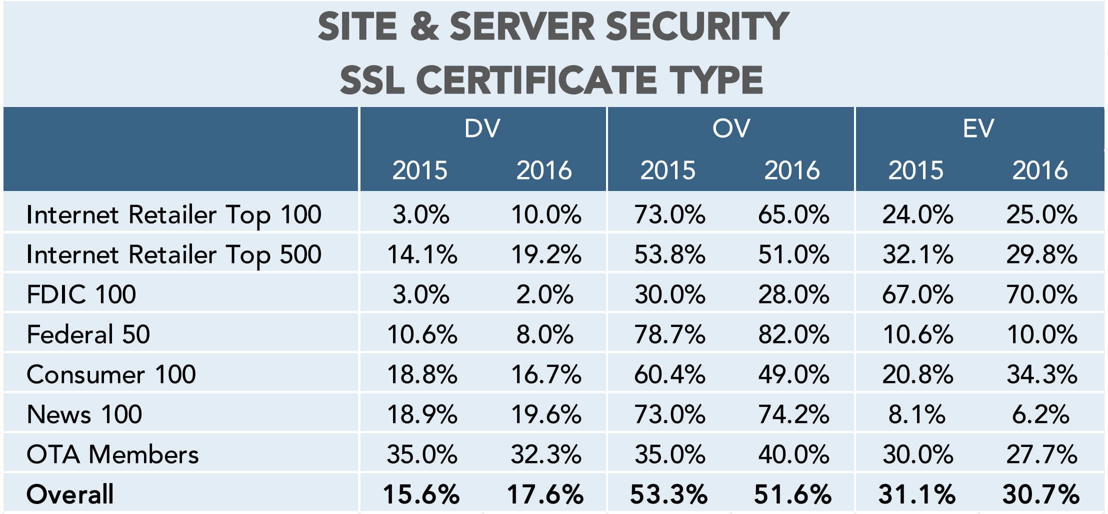
As shown in Figure 11, despite more stringent criteria, year-to-year security scores rose in every sector, led by Federal sites, which rose to 91.6. As new vulnerabilities appear frequently, sites need to implement continual monitoring and address protocol support, configuration issues and new vulnerabilities. OTA's experience has shown that changes can usually be made quickly and inexpensively once decision makers are engaged.

SSL CERTIFICATE TYPES

Recognizing the importance of trust certificates and increasing concerns regarding fraudulent certificate acquisition for lookalike sites purporting to be popular consumer destinations, OTA initiated tracking of certificate types in 2015. There are three major types of certificates – Domain Validation (DV), Organization Validation (OV) and Extended Validation (EV) – which have widely varying methods for validating the identity of the entity receiving the certificate. The official name and location of entities purchasing OV and EV certificates are verified and confirmed directly with the entity by certificate authorities and are included in the certificate. By contrast, DV certificates are typically verified through an automated process, making them more efficient and less expensive, but prone to fraud and abuse.

EV SSL certificates providing a higher level of verification, requiring a comprehensive audit process. EV SSL provides differentiation by displaying a green visual trust indicator in the address bar or browser chrome. As the number of phishing sites and fraudulent certificates grow, the value of EV SSL certificates has grown, now mandated by the IRS for e-file providers of individual tax returns and other organizations.[27] Based on data reported by Netcraft, overall adoption of EV SSL certificates increased 21% to nearly 150,000 deployed certificates in 2016.[28]

Figure 12 shows adoption rates for each type of certificate by sector. Disappointingly, retailers increased DV usage from 14% to 19%. Analysis revealed that this shift was almost entirely due to the addition of 32 new sites ranked in the Internet Retailer Top 500 which had higher than average use of DV certificates. Use of OV certificates grew in many sectors (News, Federal, OTA members), though it dropped significantly for Consumer sites, which fortunately had a corresponding increase in use of EV certificates. FDIC and Consumer sites lead in adoption of EV certificates (70% and 34% respectively).



SITE & SERVER SECURITY
SSL CERTIFICATE TYPE

	DV		OV		EV	
	2015	2016	2015	2016	2015	2016
Internet Retailer Top 100	3.0%	10.0%	73.0%	65.0%	24.0%	25.0%
Internet Retailer Top 500	14.1%	19.2%	53.8%	51.0%	32.1%	29.8%
FDIC 100	3.0%	2.0%	30.0%	28.0%	67.0%	70.0%
Federal 50	10.6%	8.0%	78.7%	82.0%	10.6%	10.0%
Consumer 100	18.8%	16.7%	60.4%	49.0%	20.8%	34.3%
News 100	18.9%	19.6%	73.0%	74.2%	8.1%	6.2%
OTA Members	35.0%	32.3%	35.0%	40.0%	30.0%	27.7%
Overall	**15.6%**	**17.6%**	**53.3%**	**51.6%**	**31.1%**	**30.7%**

Figure 12 - SSL Certificate Type by Sector, 2015-2106

[27] IRS eFile Security & Privacy Standards Mandate published January 1, 2010 https://www.irs.gov/uac/irs-e-file-security-privacy-and-business-standards-mandated-as-of-january-1-2010

[28] Source: OTA analysis completed May 15, 2016 utilizing data from Netcraft http://www.netcraft.com.

MALVERTISING

Cybercriminals have recognized the security vulnerability of the advertising ecosystem and are increasingly distributing ads with malicious payloads and code in an effort to compromise users' devices and business systems. Known as malicious advertising, or "malvertising," it poses a growing threat to everyone who accesses ad supported content online, as well as to ad supported services. Malvertising incidents have increased more than 250% since 2015. While the number of incidents has grown, the real impact is the number of malicious ad impressions served over the life of a malvertising campaign

The 2016 Audit evaluated incidents for the News and Media sector, tracking incidents occurring since January, 2015.[29] Similar to sites found to have malicious links or malware, sites which have experienced malvertising incidents receive penalty points. Overall, among the Top 100 News sites, 17 had at least one incident, and 10 had multiple incidents, collectively representing over 1 billion malicious impressions served. Not unlike the shift of spammers to spearphishing, criminals are becoming keen marketers. Just as advertisers use online tracking data to target potential users, criminals are using these same capabilities to target specific high net worth consumers, business professionals and companies.

OTA encourages investments in technologies to help protect against malvertising and increase collaboration and data sharing with the security community. OTA welcomes the industry to join the OTA Advertising Integrity Working Group[30] to develop tools, guidelines and technologies to help stem the increasing threats. OTA is encouraged by the work of Digital Content Next, a trade organization representing content publishers, and other working groups to instill trust in the advertising ecosystem.[31]

PRIVACY, TRANSPARENCY & DISCLOSURES

As the economy becomes increasingly reliant on big data and data collection, it is more important than ever for organizations to strike the balance between data collection, privacy and data stewardship. OTA has been advocating for increased transparency and discoverability of privacy policies since 2009, including recommending that policies provide disclosure of data collection, usage, sharing and retention practices. Best practices can be summarized as follows:

- Publish easy to find and comprehensible privacy policies that include the following:
  - Link / discoverability from the home page
  - Personal data is not shared with any third party except to deliver service to the user. Provide a clear statement including details if, what and for what purposes data is shared.
  - Vendor confidentiality. Disclosure that service providers are prohibited from the use or sharing of data for any purpose other than providing services on behalf of the site.
  - Data retention policy, including for what reason and how long data is retained as well as if data is retained after online interaction is terminated.

[29] Data from OTA analysis of publically reported incidents and data from researchers at Malwarebytes and RiskIQ.
[30] OTA Advertising & Content Integrity Working Group https://otalliance.org/resources/advertising-integrity-fraud
[31] Digital Content Next https://digitalcontentnext.org/

  - Designed as a layered and/or short notice. See OTA short form, linking to the full policy – http://otalliance.org/privacy-policy.
  - Compliance with Children's Online Privacy Protection Act (COPPA) [32]
- Use icons to help consumers navigate privacy policies in conjunction with layered/short notices.
- Date stamping reflecting the revision date of the privacy policy placed on the top of the page.
- Provide access to archived versions of the policy, allowing users to see what has changed.
- Write policies for the site's target audience and demographics. Consider providing bi-lingual versions representing the diversity of non-English speaking site's visitors. See Spanish version of OTA's privacy policy – https://otalliance.org/politica-de-privacida.
- Utilize tag management systems or privacy solutions to manage third-party trackers.

Audit of Presidential Candidates

As a follow up to the Audit of the 23 Presidential Candidates completed in September 2015, OTA reassessed the remaining 3 candidates (Clinton, Sanders and Trump). Previously all three had failed due to privacy issues.

Now, two still fail in privacy and the third neither fails nor qualifies for the Honor Roll. For more information see https://otalliance.org/2016candidates

- Disclose whether the site honors Do Not Track (DNT) settings in the site's privacy policy, and preferably honor users' DNT browser settings. Sample copy –

  > *XYZ respects enhanced user privacy controls. We support the development and implementation of a standard "do not track" browser feature, which is being designed to provide customers with control over the collection and use of information by third parties. At this time XYZ does not respond to DNT mechanisms. Once a standardized "do not track" feature is released, XYZ intends to adhere to the browser settings accordingly.*

- Make best efforts to provide notice to consumers if their data is requested by third parties due to legal requirements. Suggested draft copy includes the statement "*To the extent we are legally permitted to do so, we will take reasonable steps to notify you in the event that we are required to provide your personal information to third parties as part of legal process*."[33]

Figure 14 below shows the average privacy scores (including the privacy policy itself and third-party trackers seen on the site) as well as adoption of tag management or privacy solutions in each sector. Figure 15 shows adoption rates of core privacy policy best practices for each sector.

PRIVACY POLICIES & THIRD PARTY TRACKING

Privacy scores averaged 70 across all sectors (a dip from 73 last year, attributed to more stringent criteria and scoring as well as an increased number of trackers). FDIC sites showed the largest drop (76 to 67). Scores ranged from Federal sites at 84 to News sites at 50. Overall, 16% of organizations had failing privacy scores (vs. 24% last year), with the biggest impact on News sites (58%), indicating a need for intense focus on privacy policies and tracking practices.

[32] COPPA https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions
[33] Sites should conduct a legal review to ensure this draft copy is applicable to their site and business models.

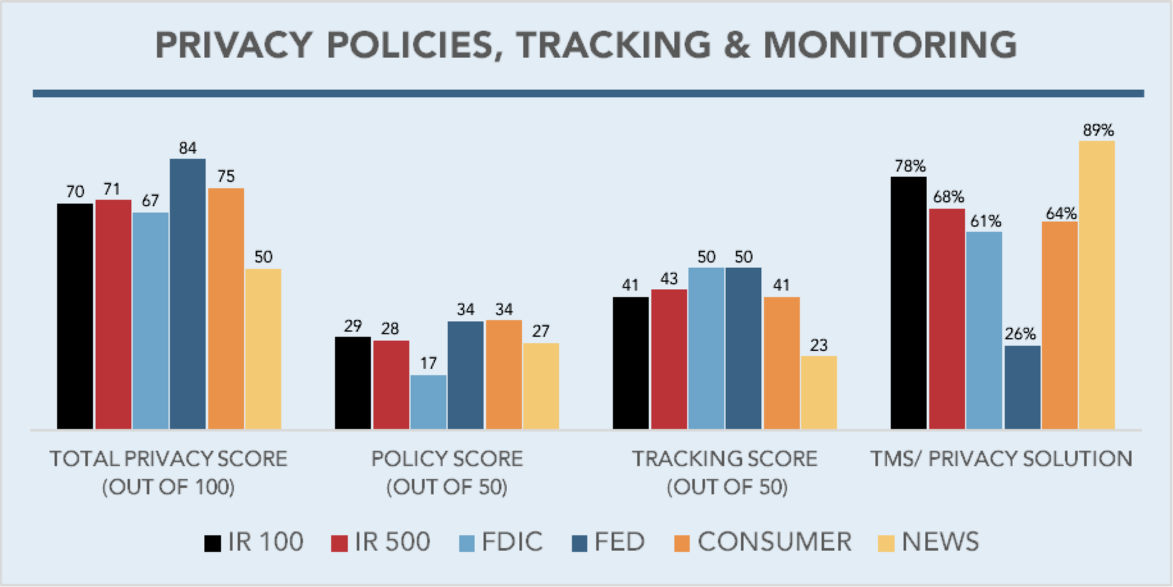


Figure 14 – Privacy Policy Scores and Monitoring by Sector

As seen in Figure 14, scores for the privacy policy component (worth 50 points) varied widely across sectors. The baseline elements least adopted were layered notice (25%) and DNT disclosure (33%), while the most adopted elements were “data not shared” (64%) and vendor confidentiality (57%). The largest year-to-year growth was seen in DNT disclosure (23% to 33%) and data retention disclosure (26% to 36%), while “data not shared” dipped significantly (77% to 64%). Third-party tracking scores also dropped this year (from an average of 45 to 42) due to presence of more trackers that freely share data. News sites, which rely heavily on third-party advertising to drive revenue, had by far the lowest tracking score (23).

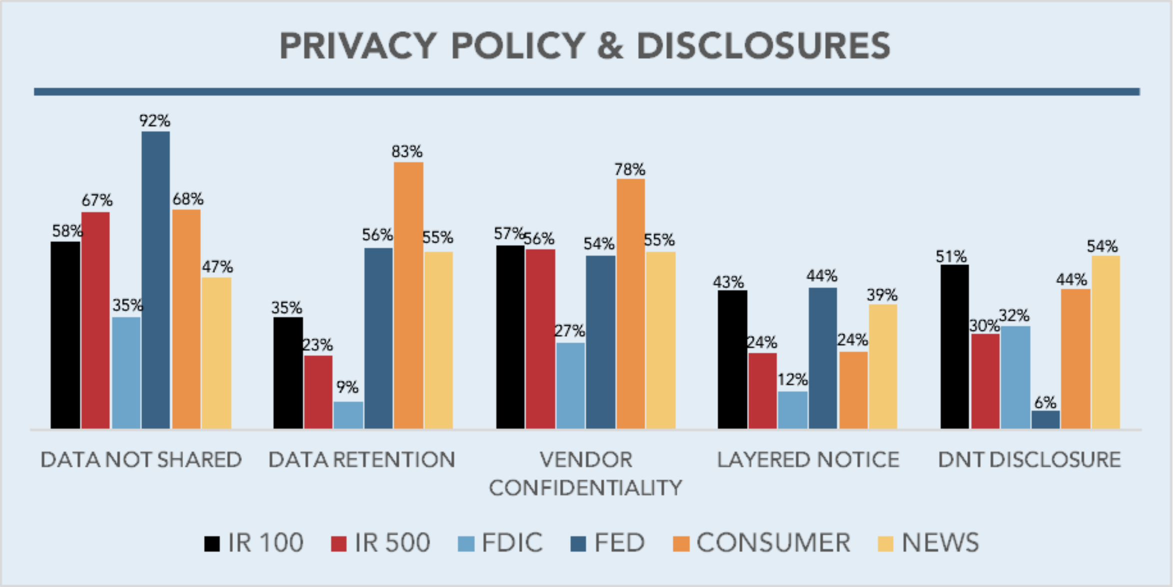


Figure 15 – Privacy Policy Implementation and Disclosure by Sector

ICONS & MULTI-LINGUAL POLICIES

The only sector other than OTA members with any meaningful use of icons is Consumer sites (4%). Support of multi-lingual privacy policies is also in the early stages, growing to 5% this year.

DO NOT TRACK DISCLOSURE & POLICY

As Do Not Track (DNT) becomes a legal requirement in many jurisdictions and issues regarding implementation are resolved, it becomes increasingly important for sites to both disclose their DNT policy as part of their privacy policy and to honor the browser's DNT setting as users visit the site. Overall disclosure of DNT policy grew from 13% to 23% to 33% over the past three years, led by News sites (53%). Disclosure became part of the baseline score this year because it is mandated by the State of California. Honoring DNT settings grew from 1% to 4% overall, led by Consumer sites at 8%.

TAG MANAGEMENT SYSTEMS & PRIVACY SOLUTIONS

Sites which rely on advertising and third-party analytics are faced with a complex challenge of managing third-party tracking, which can conflict with stated privacy policies. Tag management solutions monitor third-party data collection and sharing in real time. OTA awarded bonus points if they were present.[34] [35] Adoption grew to 66%, indicating the likely transition to baseline scoring in future audits. News sites led adoption (89%), followed by Internet Retailers (68%) and Consumer sites (66%). The lowest adoption was in the Federal 50 (26%), likely due to the fact that they do not rely on third-party advertising.

WHOIS REGISTRATIONS

When a company registers a domain name, the Internet Corporation for Assigned Names and Numbers (ICANN) requires businesses to submit contact information. This is posted in the WHOIS database which is available to anyone who chooses to find information about the site owner, providing the registration is not private. This year 90% of registrations were public. Sectors with the largest use of private WHOIS registrations are online retailers (13%) and the FDIC (12%). Private registrations limit consumers' ability to discover who the owner of a site is, impede transparency and reduce consumer trust.

DATA BREACH INCIDENTS & FTC SETTLEMENTS

Data breaches and FTC settlements can be indicative of poor data stewardship and privacy practices, impacting a site's brand reputation. Sites with such incidents or settlements receive a penalty impacting their overall score. Data breach incidents occurred in 35 (4%) of the evaluated organizations (up slightly from 32 total incidents last year, but significantly lower than the 58 incidents seen in 2014), impacting all but the News and OTA sectors. The Internet Retailer Top 100 had the highest rate (12%) followed by Federal sites (10%) and Consumer sites (8%). Ten organizations received a penalty for FTC suits or settlements this year (up from five last year), with more than half occurring in online retailer sector.

[34] Scanning capabilities provided by OTA member Ensighten, www.ensighten.com .
[35] Note while the presence of such solutions were verified, it is possible sites may not use the solutions or data.

CONCLUSION

The 2016 Audit saw an all-time high of 50% of companies earning Honor Roll status, recognizing excellence in consumer protection, site security and privacy practices. OTA congratulates all Honor Roll recipients and encourages all sites to make security and privacy part of their value proposition.

Every sector continues to demonstrate growth, with the most favorable gains observed in the Consumer 100 and News 100 segments. This growth is significant considering that added criteria raised the bar to qualify for the 2016 Honor Roll. Adoption of several criteria has surpassed 80%, including SPF at the corporate domain, use of DKIM and implementation of both authentication protocols, while the average site security score achieved an all-time high score of 89 out of 100. Year-over-year growth has been significant in other areas including DMARC, TLS, AOSSL and DNT disclosures.

Combined, this is evidence that companies are becoming more proactive in monitoring their sites, embracing responsible privacy practices, moving beyond compliance and increasing consumer disclosures with added control and choice.

The 2016 report serves four primary objectives:

- Promote best practices and provide tools and resources to assist companies in enhancing their security, data protection and privacy practices.
- Recognize excellence in consumer protection, security and responsible privacy practices.
- Raise awareness of the risks, helping businesses to improve their security and privacy practices.
- Provide consumers transparency regarding the security and privacy practices of sites they visit.

While we are observing progress and leadership across all sectors, more work is required to raise awareness of the threats and respective solutions for the remaining 50% of sites, while continually raising the bar for all sites. Collectively, the public and private sectors must double-down on security and privacy investments and renew commitments to consumer choice. Amplified by the increase of high-profile data breaches, ransomware and identity theft, consumer trust is at risk.

While the report's results are encouraging, recent developments are concerning. Rather than focus on the consumer experience and embrace best practices to help protect their supply chain and ecosystems, some trade organizations are moving in the opposite direction. They continue to shun offers of assistance and focus on defending their practices and at times attempt to disparage other organizations and consumer protection technologies. Such actions are short-sighted. It is incumbent on all parties to participate in the process, address consumer discourse, implement best practices and make data security and responsible privacy practices a priority. Left unchecked and without a commitment to meaningful self-regulation, the health of the internet is at risk.

OTA welcomes collaboration with all stakeholders to work toward improving the health of the internet, providing a trusted platform for innovation. For updates visit https://otalliance.org/HonorRoll.

APPENDIX A – 2016 HONOR ROLL RECIPIENTS

2016 Internet Retailer Top 500 – Honor Roll

- 1800Mattress.com
- A/X Armani Exchange
- ❷ AAFES
- Abt Electronics Inc.
- AED Superstore
- Aéropostale Inc.
- ❸ AJ Madison Inc.
- Alex and Ani LLC
- ❺ Alibris Inc.
- ❸ Allied Electronics
- ❺ Amazon.com Inc.
- American Eagle
- ❷ American Girl LLC
- ❺ **American Greetings Corp.**
- ❷ AmeriMark Direct LLC
- ❷ Amway
- Apple Inc.
- ❷ APMEX Inc.
- Ashford.com
- ❷ ASOS.com Ltd.
- ❷ Avon Products Inc.
- ❷ Balsam Brands
- ❸ Bare Escentuals Inc.
- ❷ BCBG Max Azria Group LLC
- ❷ Beachbody LLC
- Bealls Inc.
- ❹ Best Buy Co. Inc.
- ❺ BikeBandit.com
- ❷ BJ's Wholesale Club
- BlissWorld LLC
- Blue Apron Inc.
- Bluefly Inc.
- Bluestem Brands Inc.
- Boats.net
- ❷ **Bonobos**
- Bookbyte
- Boxed Wholesale
- ❹ Build.com Inc.
- ❹ BuildASign.com
- ❷ **BuildDirect Technologies Inc.**
- ❷ Burberry Ltd.
- BuyAutoParts.com
- ❺ Cabela's Inc.
- CafePress.com
- Cat5 Commerce
- Cheaper Than Dirt
- Chico's FAS Inc.
- Choxi
- ❸ Christianbook.com LLC
- ClickBank
- ❷ Coach Inc.
- Code42 Software Inc.
- ❷ Columbia Sportswear Co.
- ❷ **Costco Wholesale Corp.**
- Craftsy
- ❷ Crutchfield Corp.
- Cymax Stores Inc.
- Deckers Brands
- Dexclusive.com
- ❷ Discount Dance Supply
- ❹ DiscountRamps.com LLC
- ❹ Disney Store USA LLC
- ❷ **Dollar Shave Club**
- ❸ DoMyOwnPestControl.com
- ❷ eBags Inc.
- eCommerce Outdoors
- ❷ Eddie Bauer LLC
- ❷ Edible Arrangements
- eMusic.com Inc.
- ❷ Entertainment Earth Inc.
- ❷ **eSalon**
- ❷ Estee Lauder
- ❹ **Etsy Inc.**
- ❹ **evo**
- ❸ Express Inc.
- ❺ Fathead LLC
- **Fitbit Inc.**
- Follett Higher Education
- ❷ Forever 21
- ❷ Fossil Inc.
- FTD
- Gaiam Inc.
- ❹ GameFly Inc.
- ❺ GameStop Corp.
- ❷ **Gap Inc.** ◆
- GiftCardLab.com
- ❷ Gilt Groupe
- ❷ Golfsmith International
- **Google Play**
- GoPro Inc.
- Groupon Goods
- ❷ Hallmark Cards Inc.
- ❷ Hammacher Schlemmer & Co. Inc.
- **Harry's Grooming**
- ❺ Hayneedle Inc.
- hhgregg Appliances Inc.
- ❺ HSN Inc.
- Hugo Boss
- ❹ Ice.com
- ❷ iHerb Inc.
- ❷ IKEA.com
- Indochino
- Ipsy
- ❹ JackThreads.com
- ❷ Jenson USA
- ❷ Jimmy Jazz
- ❷ Joann.com
- ❷ Jomashop.com
- ❷ K&L Wine Merchants
- ❷ Kate Spade
- L.L. Bean Inc.
- ❷ Lamps Plus Inc.
- Lands' End
- ❷ LD Products

Bold – "Top of the Class" (95%+) ◆ – Top score in sector ❷ ❸ ❹ ❺ – Consecutive years as Honor Roll recipient

2016 Internet Retailer Top 500 – Honor Roll, continued

Levi Strauss & Co.
❷ **LifeWay Christian Resources**
❹ **LivingSocial Inc.**
Lowe's Cos. Inc.
LuLuLemon Athletica Inc.
❷ Luxottica Group S.p.A.
❷ MEC
❺ Microsoft Corp.
❹ Minted
❺ ModCloth Inc.
❷ Monoprice Inc.
Motorsport Aftermarket Group
❷ Musician's Friend Inc.
NakedWines.com Inc.
Nasty Gal Inc.
❷ National Builder Supply
❷ National Hockey League
NatureBox
❷ NBTY Inc.
❸ Newegg Inc.
❸ Nike Inc.
❸ Nordstrom Inc.
❷ Northern Tool & Equipment
❷ Nuts.com
❷ OmahaSteaks.com Inc.
❷ Online Stores Inc.
❷ OpticsPlanet Inc.
O'Reilly Auto Parts
❺ Overstock.com Inc.
❹ Pacific Sunwear of California
❷ Parts Express
❷ Party City Corp.
❺ Payless ShoeSource Inc.
Pep Boys
❷ Petco Animal Supplies Inc.
PetFlow.com

❷ Pier 1 Imports Inc.
❷ PlanetShoes
Power Equipment Direct
❸ PromGirl LLC
PropertyRoom.com Inc.
❷ Purchasing Power LLC
❷ PureFormulas.com
❹ Ralph Lauren Media
❷ RealTruck Inc.
❷ **REI**
Reitmans
❷ Rent the Runway Inc.
❷ RepairClinic.com Inc.
Restoration Hardware
Revolve Clothing
Ritani LLC
❷ Rock Bottom Golf
❹ RockAuto LLC
Saatva Inc.
Sheet Music Plus LLC
❷ Shindigz
❷ Shoebuy
Shoes.com
❷ ShoppersChoice.com
Signature Hardware
❷ Smarthome Inc.
Softchoice Corp.
❺ Sonic Electronix Inc.
❷ Sports Authority
❸ Spreadshirt Inc.
Stage Stores Inc.
❷ Stuart Weitzman LLC
Summit Racing Equipment
❸ Sweetwater
❹ **SwimOutlet.com**
Systemax Inc.

Tech for Less LLC
❷ The Children's Place
❷ The Clymb
❷ The Finish Line Inc.
❷ The Grommet
❺ The Gymboree Corp.
The Home Depot Inc.
❷ **The Honest Company Inc.**
The Limited
The Men's Wearhouse Inc.
❷ The Orvis Co. Inc.
The Real Real Inc.
The Yankee Candle Co. Inc.
❺ ThinkGeek Inc.
❹ Threadless.com
❷ Tilly's Inc.
❷ Tire Rack Inc.
❷ TJX Cos. Inc.
❷ TOMS Shoes Inc.
❹ Tory Burch LLC
❷ Touch of Modern Inc.
U.S. Auto Parts Network Inc.
❷ Ulta Beauty
❸ Under Armour Inc.
V2Cigs.com
Vermont Teddy Bear Co.
❷ VF Corp.
❷ **Warby Parker**
❹ Wayfair LLC
❹ **Weight Watchers**
Williams-Sonoma Inc.
Wine.com Inc.
❷ Yoox Net-a-Porter Group
❷ Zazzle Inc.
❷ Zumiez Inc.

Bold – "Top of the Class" (95%+)   ◆ – Top score in sector   ❷ ❸ ❹ ❺ – Consecutive years as Honor Roll recipient

2016 FDIC Top 100 Banks – Honor Roll

- Ally Bank
- ❺ American Express Bank, FSB.
- ❺ American Express Centurion Bank
- ❸ Arvest Bank
- ❺ Bank of America California, National Association
- ❺ Bank of America, National Association
- Bank of Hawaii
- Bank of the West
- BNY Mellon, National Association
- ❸ Branch Banking and Trust Company
- ❷ Capital One Bank (USA), National Association
- ❷ Capital One, National Association
- ❷ Chase Bank USA, National Association
- ❹ Citibank, National Association
- Citizens Bank of Pennsylvania
- Citizens Bank, National Association
- ❸ City National Bank
- ❷ Comerica Bank
- ❷ Commerce Bank
- ❷ Compass Bank
- ❷ Deutsche Bank Trust Company Americas
- ❷ Discover Bank
- East West Bank
- ❸ EverBank
- ❸ Fifth Third Bank
- First National Bank of Omaha
- ❷ First Republic Bank
- ❷ **First-Citizens Bank & Trust Company**
- ❺ Frost Bank
- ❷ **IBERIABANK** ◆
- ❸ JPMorgan Chase Bank, National Association
- KeyBank National Association
- ❹ Morgan Stanley Bank, National Association
- ❹ Morgan Stanley Private Bank, National Association
- ❷ MUFG Union Bank, National Association
- New York Community Bank
- ❷ PNC Bank, National Association
- ❸ Regions Bank
- ❺ Scottrade Bank
- Signature Bank
- **Silicon Valley Bank**
- ❷ **State Farm Bank, F.S.B.**
- SunTrust Bank
- ❷ TCF National Bank
- ❷ TD Bank USA, National Association
- ❷ TD Bank, National Association
- The Bank of New York Mellon
- ❷ The Huntington National Bank
- The PrivateBank and Trust Company
- ❺ U.S. Bank National Association
- ❹ UBS Bank USA
- Umpqua Bank
- ❺ **USAA Federal Savings Bank**
- ❺ **Wells Fargo Bank, National Association**
- Whitney Bank

Bold – "Top of the Class" (95%+)   ◆ – Top score in sector   ❷ ❸ ❹ ❺ – Consecutive years as Honor Roll recipient

2016 U.S. Federal Government Top 50 – Honor Roll

- Air Force (Consumer Facing)
- ❷ Census Bureau
- ❷ **Dept of Education**
- ❷ Dept. of Energy
- **Dept. of Health & Human Services (Healthcare)** ◆
- ❷ Dept. of Interior
- Dept. of Justice
- ❷ **Dept. of Transportation**
- ❷ Federal Bureau of Investigation (FBI)
- ❷ **Federal Trade Commission (FTC)**
- ❷ First Gov (USA.gov)
- ❷ House of Representatives
- **Internal Revenue Service (IRS)**
- Library of Congress
- ❷ National Aeronautics and Space Admin (NASA)
- ❷ National Institutes of Health (NIH)
- ❷ National Park Service (NPS)
- ❷ **Social Security Administration (SSA)**
- ❷ **U.S. Government Jobs**
- ❷ **U.S. Postal Service**
- U.S. Senate
- Veteran Affairs (VA)
- ❷ **White House**

2016 Consumer Top 100 – Honor Roll

- **1040.com**
- 1040NOW
- Airbnb
- AllClear ID
- Ancestry
- Ask.fm
- ❺ Badoo.com
- Booking.com
- ❸ **Box**
- CareerBuilder
- **DocuSign**
- ❸ **Dropbox**
- ❹ eHarmony
- ❷ eSmart (Liberty Tax)
- Expedia
- ❷ ezTaxReturn.com
- ❺ **Facebook**
- **FileYourTaxes**
- ❹ Fiverr
- ❷ **Flickr**
- ❹ **Foursquare**
- Free Tax Return.com
- ❷ FreeTaxUSA
- **Glassdoor**
- ❷ **Google Docs**
- ❷ H&R Block
- Hotwire
- ❸ **iCloud**
- **Identity Guard**
- Imgur
- Indeed
- ❹ **Instagram**
- **Jackson Hewitt**
- KAYAK
- LegalShield
- **LifeLock**
- ❺ **LinkedIn**
- **Lyft**
- ❷ Match.com
- MediaFire
- MeetMe
- Meetup
- Miniclip
- Monster
- **MyHeritage**
- OkCupid
- **OLT Online Taxes**
- Orbitz
- Pandora
- ❹ **Pinterest**
- Priceline
- **Reddit**
- Rotten Tomatoes
- Simply Hired
- Snapchat
- SoundCloud
- Spotify
- ❷ TaxACT
- ❷ TaxSlayer
- Tinder
- TransUnion
- Travelocity
- TripAdvisor
- ❺ Tumblr
- ❷ TurboTax
- ❺ **Twitter** ◆
- Uber
- VK
- ❹ Wordpress
- ❸ Yahoo!
- Yelp
- ❹ **YouTube**
- Zoosk
- ❺ **Zynga**

Bold – "Top of the Class" (95%+)   ◆ – Top score in sector   ❷ ❸ ❹ ❺ – Consecutive years as Honor Roll recipient

2016 News/Media Top 100 – Honor Roll

- American City Business Journals
- BBC.com
- Business Insider
- BuzzFeed
- Disney Interactive
- Engadget
- Fortune
- Fox News
- Gizmodo
- ❸ **Google News** ◆
- Independent
- Kotaku
- Mic
- MSN News
- ❸ New York Times
- NPR
- **Reddit**
- The Atlantic
- The Guardian
- Upworthy
- VICE.COM
- WebMD
- **Yahoo News**

2016 OTA Members – Honor Roll

- ❹ **ACT**
- ❸ **Act-On Software**
- AdBlockPlus
- ❷ ADT
- ❺ **AG Interactive**
- ❺ **Agari**
- ❸ **AVG Technologies**
- ❷ **BaseGrow**
- ❷ Brand Protect
- ❷ CertainSource
- ❸ Coles
- ❺ Constant Contact
- Device Authority
- ❺ **DigiCert**
- ❷ Disconnect
- ❸ Distil Networks
- Dmarcian Inc.
- ❺ **Ensighten**
- ❺ **Epsilon**
- **Eyeo**
- ❸ Flybuys
- ❷ **Gap**
- ❺ **GetResponse**
- ❺ **GlobalSign**
- ❺ Harland Clarke Digital
- Hartford Steam Boiler
- ❺ **High-Tech Bridge SA**
- ❺ Iconix
- ❺ **Identity Guard**
- ❺ IID
- **Infoblox**
- ❺ **Intersections**
- ❷ Kromtech Alliance Corp.
- ❸ LashBack
- ❷ **LifeLock**
- ❷ **MacKeeper**
- ❷ **Malwarebytes**
- ❺ **Marketo**
- ❷ Maropost
- ❸ MeetMe
- ❺ **Microsoft**
- National Association of REALTORS
- ❺ **Online Trust Alliance**
- ❸ Optizmo
- **PrivacyCheq**
- ❺ **Publishers Clearing House**
- ❺ **Return Path**
- ❹ RiskIQ
- ❺ Sailthru
- ❺ Silverpop
- ❷ Simpli.Fi
- ❹ **SiteLock**
- ❺ Symantec
- ❸ The Media Trust
- ❹ **ThreatWave**
- ❺ **TRUSTe**
- ❺ **TrustSphere**
- ❺ **Twitter** ◆
- ❷ UnsubCentral
- **ValiMail**
- ❹ **VeriSign**
- ❹ Vivaki
- Yesmail Interactive
- ❹ ZEDO
- Zeta Interactive

Bold – “Top of the Class” (95%+) ◆ – Top score in sector ❷ ❸ ❹ ❺ – Consecutive years as Honor Roll recipient

ACKNOWLEDGEMENTS

Data provided in part by Agari, DigiCert, Disconnect, Distil Networks, Ensighten, GlobalSign, Google, High-Tech Bridge SA, Infoblox, Malwarebytes, Microsoft, Return Path, SiteLock, Symantec, SSL Labs, Threatwave, Twitter, TRUSTe and Verisign. Special thanks for *Internet Retailer Magazine* and Vertical Web Media for the list of top online retailers from the Top 500 Guide®.

ABOUT THE OTA

The Online Trust Alliance (OTA) is a 501c3 charitable non-profit with the mission to enhance online trust and user empowerment while promoting innovation and the vitality of the Internet. Its goal is to help educate businesses, policy makers and stakeholders while developing and advancing best practices and tools to enhance the protection of users' security, privacy and identity.

OTA supports collaborative public-private partnerships, benchmark reporting, and meaningful self-regulation and data stewardship. Its sponsors and supporters include leaders spanning public policy, consumer protection, technology, e-commerce, social networking, mobile, email and interactive marketing, financial services, government, NGOs and industry organizations.

Supported by generous grants and donations from

UNDERWRITERS

Symantec.

act-on digicert distil networks SiteLock. THREATWAVE

Material in this publication is for educational and informational purposes only. Neither the publisher, the Online Trust Alliance (OTA), its members nor the authors assume any liability for any errors or omissions nor how this publication or its contents are used or interpreted or for any consequences resulting directly or indirectly from the use of this publication. OTA makes no assertions or endorsements regarding the security, privacy or business practices of companies that may choose to adopt such recommendations outlined. For legal advice or any other, please consult your personal attorney or appropriate professional. The views expressed in this publication do not necessarily reflect the views of OTA member companies or affiliated organizations.

OTA MAKES NO WARRANTIES, EXPRESS, IMPLIED, OR STATUTORY, AS TO THE INFORMATION IN THIS DOCUMENT. For updates visit No part of this publication may be reproduced or distributed in any form or by any means, or stored in a database, web site or retrieval without the written consent of OTA.