# 2017 Online Trust Audit & Honor Roll

Recognizing excellence in security, consumer protection and responsible privacy practices

Online Trust Alliance
an Internet Society initiative

# TABLE OF CONTENTS

# OVERVIEW & BACKGROUND


The 2017 Online Trust Audit and Honor Roll represents the 9th year that the Online Trust Alliance (OTA) has conducted benchmark research to promote security best practices, data stewardship and responsible privacy practices. The primary goals of this work include raising the level of data security and privacy, while recognizing organizations that have demonstrated security and privacy excellence. In addition to the Honor Roll status (Appendix C), this year's Audit includes the "Top of Class" representing the top 50 organizations based on their total score (Appendix B).

The 2017 report also reflects OTA becoming part of the Internet Society (ISOC). We share the mission to promote the open development, evolution and use of the Internet for the benefit of all people throughout the world. Further, OTA strives to enhance online trust, user empowerment and innovation through convening multi-stakeholder initiatives, and developing and promoting security best practices, responsible privacy practices and data stewardship.

The timeliness of this Audit is highlighted by last month's WannaCry ransomware attack impacting over 300,000 computers worldwide. This incident underscores the critical need for organizations to embrace best practices, including upgrading and patching systems. The 2017 CIGI-Ipsos Global Survey on Internet Security and Trust paints a bleak picture of the state of online trust. According to this study, a majority of those surveyed said they are more concerned about their privacy than the year before and only a little more than half agreed that they trust the Internet.[1]

Left unchecked, mistrust in privacy and security may have chilling effects, with business practices that are moving out of alignment with consumer expectations. For the Internet to prosper, users must trust that their personal information will be secure, their preferences respected and their privacy protected.

The recommendations and best practices advocated by OTA apply not only to websites and mobile applications, but increasingly to the expanded universe of Internet of Things (IoT) devices. Device manufacturers should review OTA's IoT Trust framework for specific recommendations.[2] The 2017 report has been expanded in several areas reflecting the broader set of sectors being analyzed and an expanded methodology, including nearly 100 data attributes (Appendix A). In nearly every area, new criteria have been added and the weighting re-allocated to reflect the evolving threat landscape, regulatory environment and globally accepted practices. As an aid to brands and sites, this year's report includes Sample Privacy Language (Appendix D), Best Practices Checklist (Appendix E) and Implementation Resources (Appendix F).

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, sites' scores may have changed since the Audit was completed. While OTA does not make explicit endorsements of any organization, readers may want to consider frequenting websites that have consistently qualified for the Honor Roll. 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 was identified, OTA abided by responsible disclosure practices and attempted to contact the "at-risk" entity providing them a chance to remedy the observed issue and be rescored.

# EXECUTIVE SUMMARY & HIGHLIGHTS

The 2017 Audit encompasses over 1,000 websites, examining consumer protection, security and privacy protection practices.[3] Enhancements to the Audit include normalizing all segments to a minimum of 100 sites and adding a new segment called "ISP/Hosts". This segment includes the top Internet service providers (ISPs), wireless carriers, cable companies, email providers and website hosting providers.[4] Sectors examined and associated top-ranked organizations include:

- 2017 Internet Retailer Top 500 [5] (IR 100 & IR 500)
- Top 100 Banks (Bank 100, previously the FDIC 100) [6]
- Top 100 U.S. Federal government sites (Fed 100, previously the Fed 50)
- Top 100 Consumer Services sites (Consumer 100) [7]
- Top 100 News and Media sites (News 100)
- Top 100 ISPs, Carriers & Hosters (ISP/Hosts 100)
- OTA Member Organizations (OTA)

*"Data is the 'oil' of the Internet. It is fueling innovation and revenue, yet if abused there is a risk of a negative impact to society," said Craig Spiezle, Founder and Chairman Emeritus of OTA. "The Audit underscores the urgency to embrace responsible security and privacy practices.*

While the majority of the segments remain the same, the actual companies (websites) can change based on revenue ranking and market consolidation. This year, with the addition of the ISP / Hoster category, doubling the size of the Federal segment, and shifting companies on the ranking lists, approximately a quarter of sites are new to the Audit.

As in previous years, 100 baseline points can be earned in each of the three major assessment categories (consumer protection, site security and privacy), while bonus points are applied for emerging best practices and penalty points for breaches, legal settlements and vulnerabilities. Criteria this year have been tightened, requiring a minimum score of 60 in each of the three areas, up from 55 in past years. In addition, the earning of bonus points has been reduced to a maximum of 20% of the baseline score. Sites qualify for the Honor Roll by achieving a score of 80% or higher overall with no failures in any one of the three core categories.

2017 marked a tipping point as 52% of sites qualified for the Honor Roll. This is impressive considering the revised methodology. OTA members outpaced all segments with 96.8% qualifying for the Honor Roll (up from 95.6% in 2016). Not including OTA members, all other sectors combined climbed from 46.5% to 49.7%.

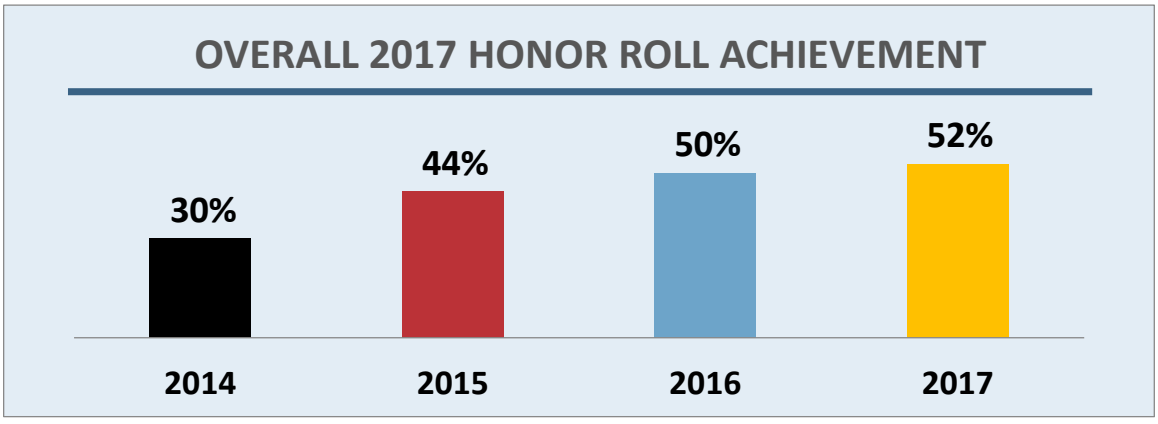


Figure 1 – Overall Honor Roll Achievement by Year, 2014-2017

As illustrated in Figure 2, Honor Roll achievement grew in most sectors despite more stringent criteria in this year's Audit.[8] For the fourth year in a row, the Consumer 100 outscored all sectors with 76.2% achievement. Many sites in this segment seemed to benefit from homogeneous and integrated system architectures in contrast to other sectors which have a higher percentage of legacy systems. Equally as impressive, online retailers surpassed a tipping point at 59%. Most concerning the Bank 100 dropped by more than half to 27% qualifying for the Honor Roll with over 65% received failing grades. Their failures were attributed in part to the revised failure threshold, increased number of data breaches, observed site security vulnerabilities and inadequate privacy disclosures.

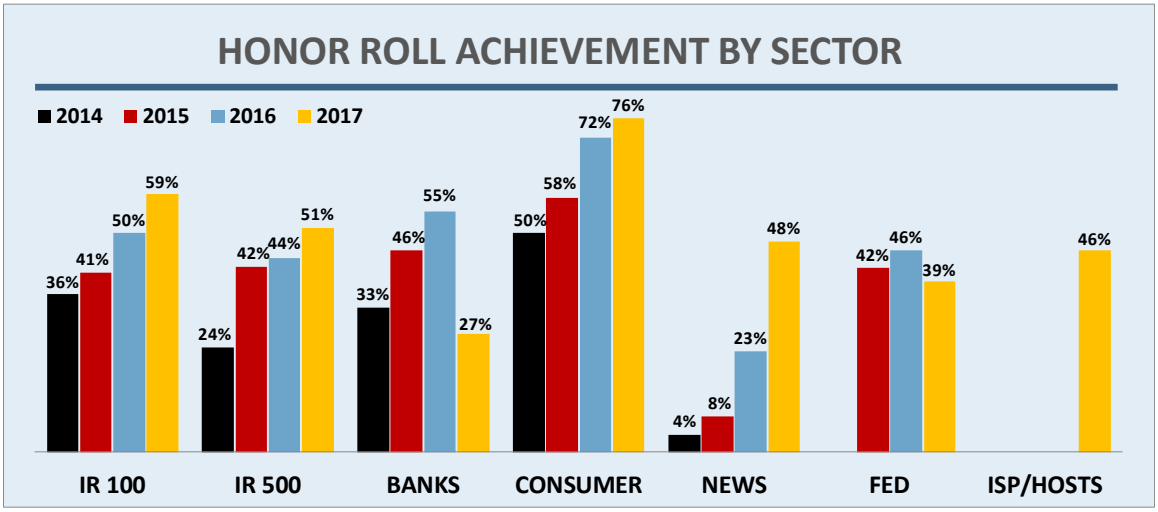


Figure 2 – Percent Achieving Honor Roll Status by Sector

Over the past three years a bimodal trend has developed, with a majority of sites either qualifying for the Honor Roll or failing in one or more areas. As illustrated in Figure 3 (netting out OTA members), in total only 4.2% neither failed nor qualified for the Honor Roll, ranging from 1% to 8% for individual sectors.

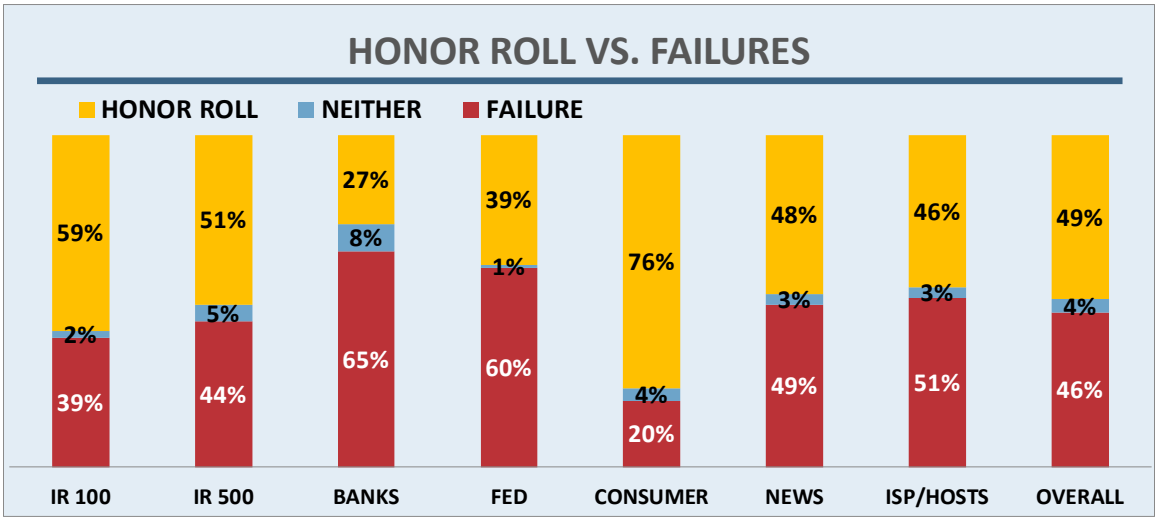


Figure 3 – Distribution of Honor Roll vs. Failures by Sector

New to the 2017 Audit, we created the "Top of Class" category representing the top 50 (Top 50) overall scores. As expected, the Consumer Services segment dominated top scores while not a single bank qualified. Note, as

8 of the brands are in multiple categories, the percentages exceed 100%. OTA members were excluded from this list because many are technology and service providers rather than primarily consumer facing brands. Had they been included OTA members would have represented 40% of all sites within the Top 50. See Appendix B for the sites which qualified for the Top 50.

| Top 50 Segment Performance | | |
|---|---|---|
| Code | Segment | % of Top 50 |
| C | Consumer Services | 52% |
| R | Internet Retailers | 20% |
| I | ISPs, Carriers & Hosters | 14% |
| G | Government | 12% |
| N | News & Media | 6% |
| F | Bank 100 | 0% |

Figure 4 – Top 50 Segment Performance

Overall failure results, as shown in Figure 5, revealed the composite site security score was the least prevalent cause of failure for all sectors at 9%, followed by privacy at 16% and consumer protection at 33%. Failures varied widely by sector (Figure 6). Combined 46.5% of sites failed in one or more area. Inadequate email authentication was the primary cause for failures including 55% of the Fed 100. Inadequate privacy policies were the second largest cause of failures, impacting more than 34% of the banking sector. For this sector, the primary issue was the use of a standardized privacy disclosure form which does not address all core Audit criteria.[9] Conversely, Consumer sites demonstrated a much higher level of transparency in their privacy disclosures with only 4% failing for the same reason.

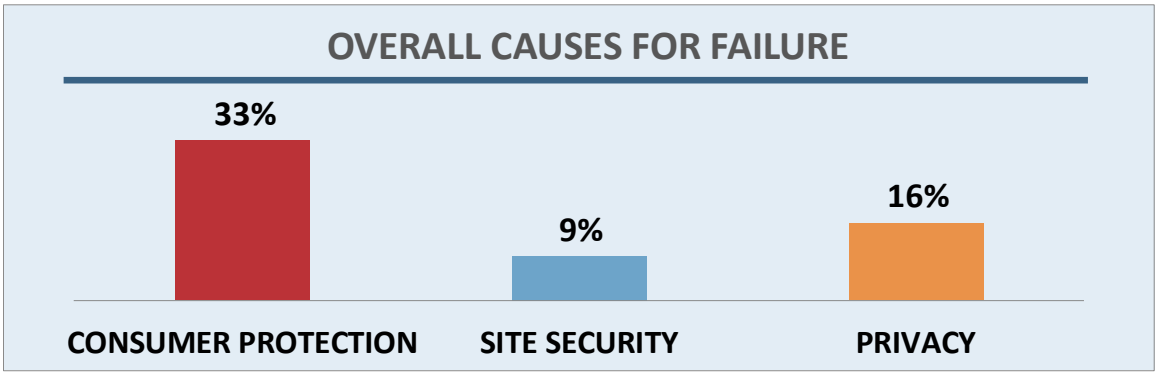


Figure 5- Failures Causes by Audit Category

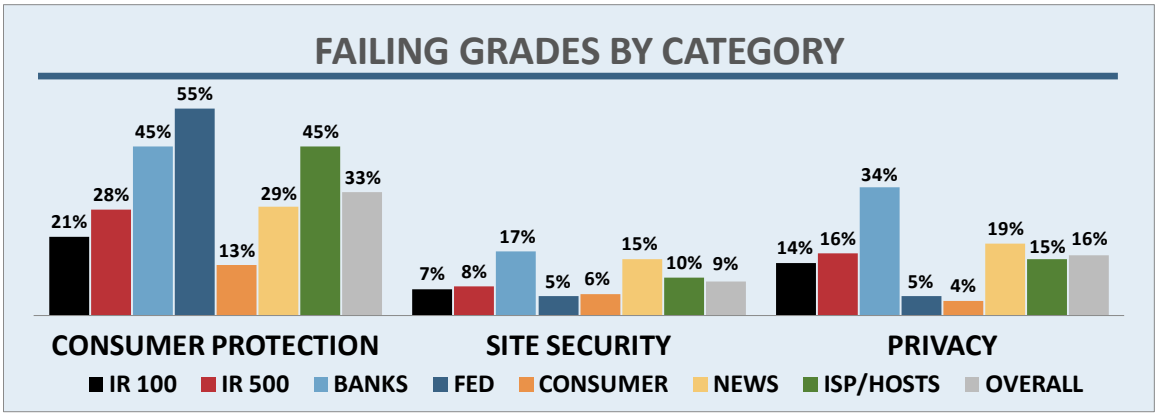


Figure 6 – Percent of Companies with Failing Grade by Sector and Category

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 index across sectors. Figure 7 illustrates how the medians for several sectors sit near the 80% Honor Roll threshold, meaning many of sites could qualify for the Honor Roll through simple operational changes and adoption or remedy of a single best practice.

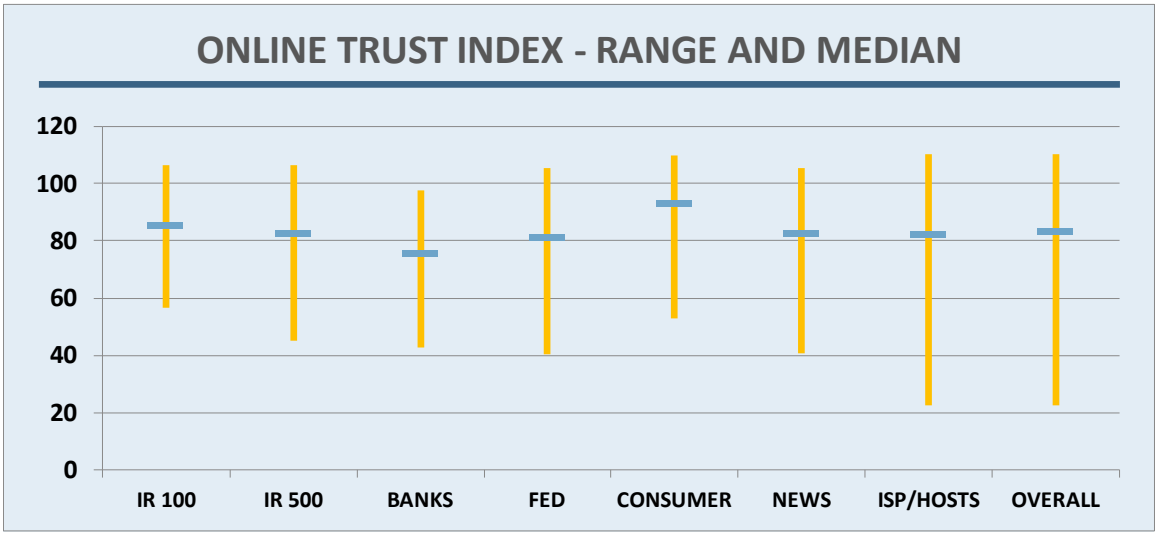


Figure 7 – Range and Median Online Trust Index Scores by Sector

# BEST PRACTICES HIGHLIGHTS

The following is a summary of audited best practices advocated by OTA. Additional details are provided in the respective sections: 1) Domain, Brand and Consumer Protection, 2) Site and Server Security, and 3) Privacy Policy and Practices.

## SERVER SECURITY & CONSUMER PROTECTION

HTTP Strict Transport Security (HSTS), Always on SSL, or HTTPS Everywhere - Adoption surged from 29.8% to 52.2%. Based on direct feedback from several individual sites, this growth is attributed to increased concerns of third party and government spying on web activities and speaks to the success of groups including OTA, the Electronic Frontier Foundation (EFF), the Internet Society and others advocating for encryption as the "norm" for all Internet traffic.[10]

Email Authentication - The 2017 methodology was revised to only recognize Sender Policy Framework (SPF) and Domain-based Message Authentication, Reporting & Conformance (DMARC) records which were in compliance with published specifications. Across all sites, 7.6% had a malformed or invalid SPF record. This underscores the need for sites to continually monitor their records to maximize brand and consumer protection. If left unmonitored, brands may have a false sense of security because some receiving networks and ISPs may disregard such "invalid" records.

- SPF adoption at the top-level domain dropped from 79.9% to 76.6%, which can be directly attributed to the malformed and invalid records cited above.
- Overall adoption of DomainKeys Identified Mail (DKIM) at the corporate top level domain increased from 43.6% to 55.9%, reflecting growing recognition of the standard.
- Use of DMARC records of any type grew from 27.4% to 34.3%, which can be partially attributed to the increase of spear phishing, business email compromise attacks and ransomware being driven by spoofed and forged email.
- Adoption of DMARC reject or quarantine records grew from 5.8% to 14.6% of all sites' domains (top level and subdomains). This growth is positive news and shows confidence by industry in the importance DMARC has in brand and consumer protection.[11]

Domain Name System Security Extensions (DNSSEC) - Adoption nearly doubled, from 6% to 11.6%. This can be attributed to growth within the banking sector from 2% to 9%, inclusion of the ISP/Host segment (6%) and federal government sites, which grew from 88% to 93%. (Bonus Points)

IPv6 – Adoption nearly doubled, from 7.4% to 11.7%, though adoption by Federal sites dropped from 84% to 71%. This drop is due to the expansion of the Federal sector from 50 to 100 sites, which includes "second tier" government agencies. News sites nearly tripled IPv6 use, from 5% to 14%. (Bonus Points)

Secure Socket Layer (SSL) / Transport Layer Security (TLS) Scores - Overall scores increased slightly from 88.3 to 91.3 (out of 100), reflecting sites' adherence to ongoing monitoring of best practices. Sites with failing scores (8.5%) failed to address one of more of the following: weak or insecure cipher suites, use of insecure protocols and incomplete certificate chains. Observed vulnerabilities include: DROWN, POODLE, Open SSL and others. It should be noted that banks scored the lowest in SSL security due to the use of insecure and outdated ciphers, including 64-bit block cipher with modern protocols and use of RC4.

Vulnerability Disclosure Mechanisms / Programs - Added in 2017 and recognized as a best practice by the National Telecommunications and Information Administration (NTIA), National Institute of Standards and Technology (NIST), the Federal Trade Commission (FTC) and OTA. Disappointingly, only 6% of sites overall had a reporting mechanism visible on their site or listed with third party "bug bounty" service providers. While the Consumer Services segment outpaced all categories with 36.2% adoption, it is concerning that only 2% of bank sites have a "discoverable" reporting mechanism. Having such mechanisms is critical to effectively respond to third-party researchers and users and is relatively simple to implement. (Bonus Points)

Web App Firewalls - Adoption increased more than 30%, from 35.8% to 68.1%, due to the recognition of its value in baseline site security, as well as increased telemetry in the 2017 Audit.

Cross Site Scripting (XSS) Vulnerabilities - The presence of these vulnerabilities increased from 26.6% to 50% which is concerning. This increase is largely attributed to enhanced telemetry via access to a public database of reported XSS vulnerabilities.

## PRIVACY TRENDS

Combined scores (privacy policy and use of third-party trackers) improved this year, shifting from 69.2 in 2016 to 72.8 in 2017. This development is extremely positive in light of increased baseline privacy disclosure requirements in the 2017 methodology.

Privacy Policy - Overall privacy policy scores increased from 27.4 to 30.8 from 2016 to 2017, while disclosure of data retention policies jumped from 34.2% to 49.4% from 2016 to 2017. Improvements were observed in Children's Online Privacy Protection Act COPPA compliance, version tracking and multi-lingual offerings. In response to industry support and response to the FTC's recommendations for added disclosure, cross-device tracking disclosure was added as new criteria this year and was observed on 44.3% of sites (bonus points). Do-Not-Track disclosures increased from 32.9% to 36.9% from 2016 to 2017.

Lowlights include the disclosure of vendor / service provider confidentiality, which decreased from 54.8% to 48.4% from 2016 to 2017. Date stamping at the top of the privacy policy page is a new metric for 2017 and was seen on 45.5% of sites. Previously, sites received points for any date stamping on the page. This change was made recognizing the importance of a standardized and discoverable disclosure in light of longer policies and more frequent privacy policy changes. For reference, in 2016, 74.2% of sites had a date stamp somewhere on the page.

Third Party Trackers - Overall the average number of problematic trackers as defined by sharing data with unaffiliated third parties for non-operational purposes decreased from 11.4 to 8.8 per site from 2016 to 2017. These are trackers known to share data with third parties (not including data for anonymous site metrics). The number of unique trackers observed on all sites ranged from 0 to 59. The News/Media sector had the most with an average of 25.4 reflecting their dependence on advertising and re-targeting of site users.

Data Loss Incidents & Breaches - Measured from January 2016 through May 2017, 11.7% of sites had one or more incidents, with a total of over 3.8 billion exposed records. Of all the segments, the Bank 100 had the highest rate (24%) followed by Consumer sites (23.8%). In total, this is a significant jump from 2016, where only 4.8% of the audited sites had an incident. This shift is attributed to three factors: 1) increased telemetry and data fidelity, 2) overall increase in cyber incidents and 3) increased transparency and disclosures of incidents.[12]

Regulatory Fines & Settlements - On the regulatory front, 21 organizations received a penalty for suits or settlements this year (up from 9 last year), with the banking sector having the most (8). This increase is attributed to the inclusion of data from the Consumer Financial Protection Bureau (CFPB) as well as increased data from individual state Attorney General offices. The Audit is focused on consumer protection actions and does not include settlements pertaining to mergers and acquisitions or labor related settlements.

# 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 was added to last year's Audit, recognizing the importance of sites' migration. Early adopters received bonus points for this enhancement in Internet architecture, which expands the number of unique IP addresses supporting the growth of the Internet including demand for new IP addresses driven by IoT.[13] [14]

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
- Optimize SPF records with no more than 10 DNS lookups
- 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
- Mandate the use of DMARC reporting capabilities with RUA and RUF reporting
- Implement inbound email authentication checks and DMARC on all networks to help protect against malicious email and spear phishing 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
- Deploy IPv6
- Implement Distributed Denial of Service (DDoS) mitigation technologies and processes[15]
- Implement multi-factor authentication

## EMAIL AUTHENTICATION

The 2017 Audit included additional telemetry, providing a more precise view of authentication across all sectors. Authentication technologies, namely SPF and DKIM, help prevent phishing and spam. OTA recommends the 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 received increased weighting for the second year in a row.

Figure 8 shows adoption of SPF and DKIM at the corporate top level domain (TLD) and combined use of SPF and DKIM at any level including subdomains. 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.

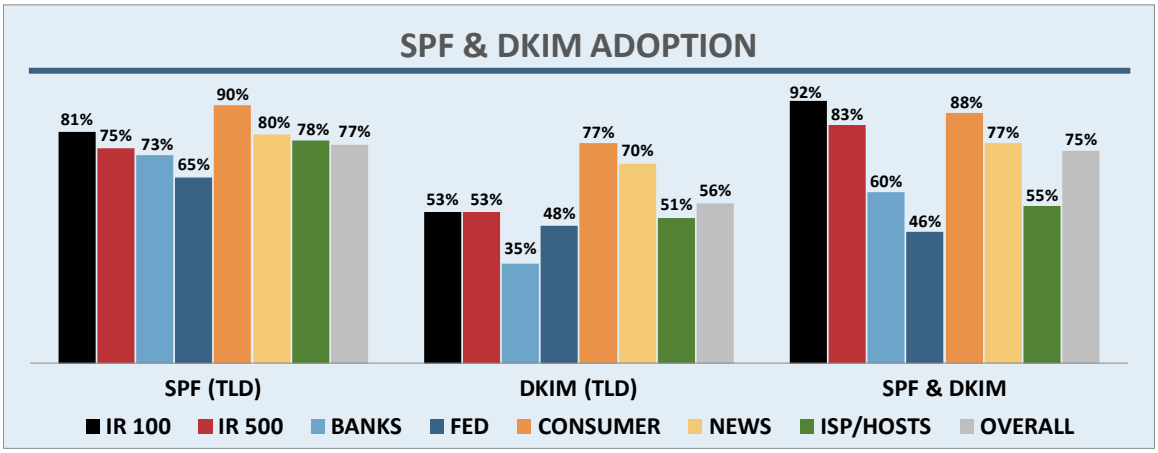


Figure 8 – Email Authentication & DMARC Adoption by Sector

As seen in Figure 9, this year declines were observed primarily due to more stringent criteria disregarding invalid SPF records and non-resolving DKIM signatures. Online retailers and consumer services platforms, which are most heavily reliant on email interaction with their users/customers, continue to outpace all sectors. While on the surface this is encouraging, it is unfortunate that most of the growth occurred via marketing-specific subdomains (note the 10% to 38% gap between "DKIM TLD" and "SPF and DKIM" in Figure 8 above). This gap underscores that additional efforts are needed to drive DKIM implementation to protect top-level and corporate domains from abuse.

SPF records were analyzed more closely this year, and were considered invalid if they contained errors that would cause them to be unusable or ineffective. This impacted 7.6% of sites overall and was most prevalent for retailers (9.8%). The top reasons for being invalid were "include" references to non-existent or invalid SPF records of other domains, use of multiple SPF records and syntax errors rendering the record useless. In addition, the use of a "+all" or "?all" directive was observed, which effectively instructs receivers (ISPs and corporate networks) to allow any IP address to send mail or to ignore the record. Many of these sites may have a false sense of security, not knowing that their records are ineffective in protecting their domain.

This year's analysis also found several SPF records exceeding the 10-lookup parameter of the specification, often via use of daisy-chained "includes." While these were counted as valid for this Audit, some receiving networks may disregard some or part of the result since excessive lookups are out of compliance with the Internet Engineering Task Force (IETF) technical specification, reducing the utility and brand protection value.[16]

While outside the scope or capability of the Audit, all organizations should deploy inbound authentication checks and enforce DMARC policies. As a recommended risk mitigation practice, key vendors, business partners and service providers should be required to deploy end-to-end authentication including SPF, DKIM and DMARC.

| BOTH SPF & DKIM | | | | |
|---|---|---|---|---|
| | 2014 | 2015 | 2016 | 2017 |
| Internet Retailer Top 100 | 88% | 90% | 92% | 92% |
| Internet Retailer Top 500 | 74% | 78% | 85% | 83% |
| Bank 100 | 49% | 63% | 69% | 60% |
| Federal 100 | 22% | 48% | 58% | 46% |
| Consumer 100 | 74% | 76% | 86% | 88% |
| News 100 | 50% | 56% | 75% | 77% |
| ISP/Hosts | - | - | - | 55% |

Figure 9 – 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.

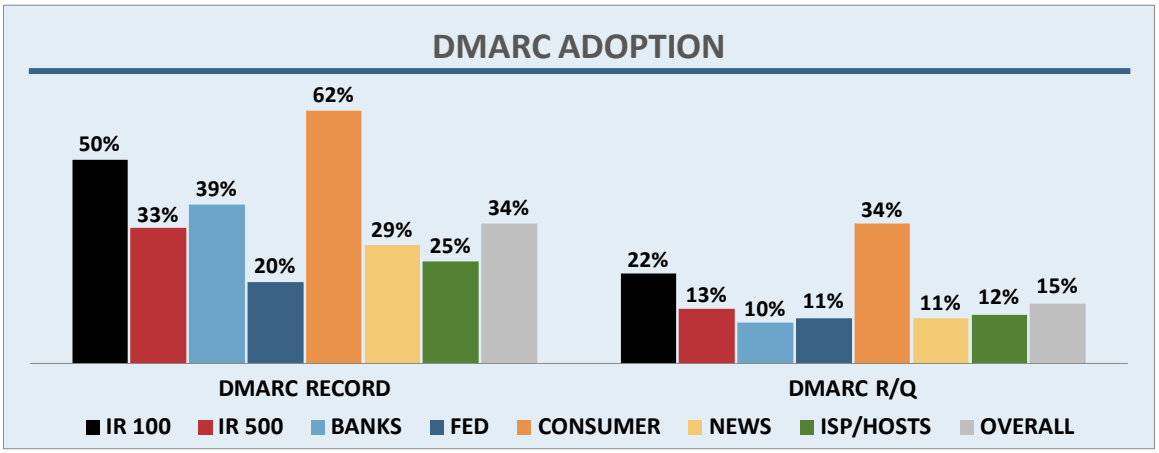


Figure 10 - DMARC Adoption & Policies

Illustrated in Figures 10 and 11, adoption of DMARC grew in most sectors, though due to the in-depth analysis conducted this year, many were considered invalid (compare the "Any Record" results to "Valid Record" to see the impact in each sector). The top reasons to invalidate a record were a "naked" record (p=none and no RUA or RUF reports), pointing reports to domains unable to accept them, syntax errors and placing the "p=" policy directive late in the record. *Note for 2017, DMARC reject "R" or quarantine "Q" is a percent of all sites. In previous years this metric was calculated as a percent of sites publishing any DMARC record.*

| DMARC ADOPTION | | | | | | |
|---|---|---|---|---|---|---|
| | 2014 Record | 2015 Record | 2016 Record | 2017 Any Record | 2017 Valid Record | 2017 R or Q* |
| Internet Retailer Top 100 | 15% | 20% | 30% | 51% | 50% | 22% |
| Internet Retailer Top 500 | 6% | 8% | 21% | 35% | 33% | 13% |
| Bank 100 | 21% | 24% | 33% | 42% | 39% | 10% |
| Federal 100 | 6% | 14% | 20% | 23% | 20% | 11% |
| Consumer 100 | 36% | 48% | 64% | 68% | 62% | 34% |
| News 100 | 10% | 10% | 21% | 35% | 29% | 11% |
| ISP/Hosts | - | - | - | 29% | 25% | 12% |

Figure 11 – DMARC Adoption by Sector. *R = Reject policy / Q = Quarantine policy

## OPPORTUNISTIC TRANSPORT LAYERED SECURITY (TLS) FOR EMAIL

Tracking of Opportunistic TLS for email was added in the 2015 Audit to help address mounting privacy concerns regarding spying on email in transit. TLS encrypts messages in transit from one server to another, seamlessly decrypting the messages before they are delivered to a user's device. TLS adoption grew dramatically from 21% in 2015 to 65.4% in 2017. Adoption ranged from 46% (Federal sites) to 91% (Top 100 Internet Retailers). Growth is attributed to an overall call for encryption by dozens of organizations including OTA and the Internet Society. Another factor influencing adoption is that some email providers such as Gmail, now flag warnings in the user interface for non-TLS compliant email with an unlocked red padlock.[17]

## 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 95% of organizations across all sectors lock their domains. Government sites lead with 100% adoption followed closely by Consumer sites at 99%. Ironically, ISPs & Hosters who should be most familiar with this issue, scored the lowest of all segments lagging at 90%.

## 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, .net and over 135 other TLD's, potentially supporting more than 90 million domain name registrations worldwide in the .com domain alone.[18] DNSSEC adoption nearly doubled to 11.6% from 6% in last year, with the Government sector leading with 93% adoption. Additionally, the banking sector jumped 4-fold to 9% recognizing the criticality of DNS security and resiliency. Surprisingly, ISPs and Hosters lagged at 6%. Broader implementation of DNSSEC continues to be hampered by legacy systems and lack of ecosystem infrastructure.

## 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, significantly expanding the number of available addresses. OTA supports broader deployment, awarding bonus points for early adopters. Adoption worldwide is growing with 24% of the Alexa Top 1000 websites currently reachable over IPv6.[19] Overall adoption in the OTA Audit nearly doubled in 2017 to 14.1%, up from 7.4% in 2016, with Federal sites leading at

71%, followed by ISPs and Hosters at 19%. The high adoption by the Fed 100 is attributed to the 2005 mandate by the Office of Management and Budget (OMB) directing federal agencies to adopt by 2010.[20]

## MULTI-FACTOR AUTHENTICATION (MFA)

Adding another layer of authentication on top of simple username and password is an effective step to help counter unauthorized account access, account takeover and password resets. Multifactor authentication (MFA) requires additional credentials beyond username and password for gaining access to an application, site, or data. In typical 2-factor authentication, a security code or pin is sent to a mobile phone (something the user possesses) to verify account access authorization. This is the first year this has been examined, and overall adoption is at 6%, led by ISPs and Hosters at 25%, and Consumer sites at 18%. While sites with confirmed MFA received bonus points, it is recognized the data may be incomplete (confirmation was available for less than one-fourth of audited sites) and therefore likely significantly understates actual adoption. Future Audits will expand on capabilities for a more comprehensive analysis.

# SITE, SERVER & INFRASTRUCTURE SECURITY

A site's trustworthiness is largely defined by the security of the infrastructure. Users need assurance that the site and its data are secure. Proper implementation of best practices in this category also protects the site itself from attack. The 2017 Audit has been expanded with deeper evaluation of DNS health, IP reputation, application security and patching cadence. In addition, the bar was raised this year in server security scoring by combining results from High-Tech Bridge, Qualys SSL Labs and Security Scorecard. Best practices include:

- Optimize SSL/TLS implementation using information gleaned from public tools, focusing on vulnerabilities that earn a letter grade of "F" or that have failure (60 points or less) in a major subcomponent of the scoring (which normally leads to an overall grade of "C").[21,22] This includes eliminating use of insecure ciphers and older, insecure protocols as well as vulnerabilities to the POODLE and DROWN exploits.[23]
- Use EVSSL certificates 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.
- Review capabilities of certificate authorities, recognizing that support and security resources from free and automated certificate authorities is limited. To maximize brand protection and differentiation, upgrade to EVSSL certificates.
- Implement HTTP Strict Transport Security (HSTS), also referred to as Always on SSL (AOSSL) or HTTPS everywhere, on all pages to maximize data security and online privacy. HSTS helps ensure that all data exchanged between the site and device is encrypted.
- 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.[24]
- 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.
- Plan for implementing Certification Authority Authorization (CAA).[25]
- Provide a discoverable and accessible vulnerability reporting mechanism for site visitors and third parties to report vulnerabilities.

As illustrated in Figure 12, summary security scores are in a relatively narrow range, while the adoption rate of key enhancements varies widely:

- SSL/TLS scores, which represent the baseline score in this category, are tightly concentrated around the overall average of 91.3, with Federal outscoring all segments with a 95-average score.
- EV SSL adoption varies significantly across sectors – it is highest in the Bank 100 (62%, which outpaces all other sectors 2:1) and lowest for News sites (5%) and Federal sites (8%).
- Overall adoption of HSTS grew significantly from 30% in 2016 to 52% in 2017, yet adoption varies widely – from 91% of the Fed 100 to only 26% of News sites. The growth in Federal sites is a continuation of the trend from last year where HSTS grew from 17% to 50%. All sectors nearly doubled in adoption.

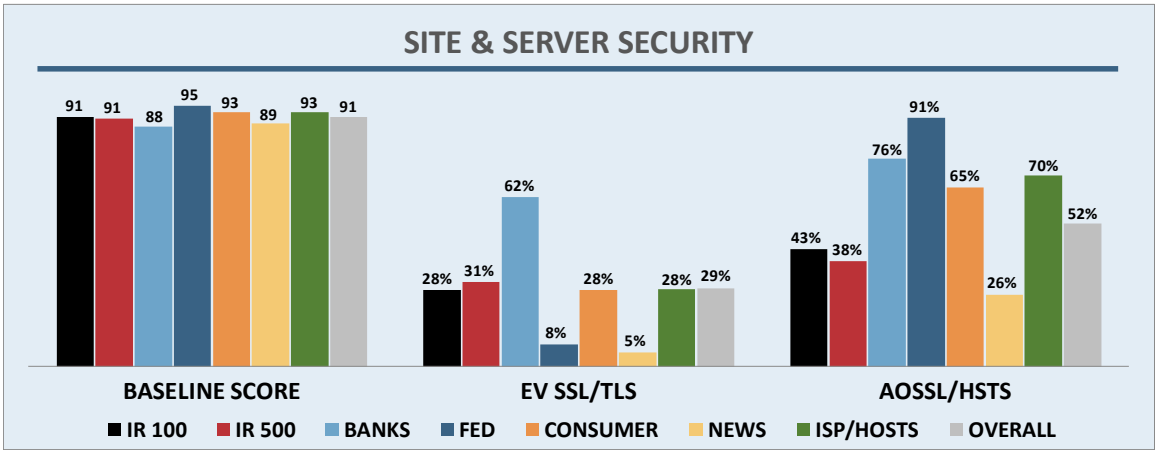


Figure 12 – Site & Server Security Scores/Adoption by Sector

## SERVER IMPLEMENTATION & VULNERABILITY ANALYSIS

Ongoing SSL/TLS configuration monitoring is a fundamental requirement to optimize security and thwart vulnerabilities. The 2017 Audit significantly expands the analysis with the addition of new scanning and diagnostic tools, including those provided by DigiCert, Distil Networks, High-Tech Bridge, SecurityScorecard, SiteLock, Symantec and SSL Labs. 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.

As a reference to the overall state of SSL/TLS security, the June 2, 2017 SSL Pulse report indicated 58% of the 139,154 sites tested were considered secure, a strong increase from the 43% considered secure in June 2016.[26] By comparison, 76% of sites in the OTA Audit are considered secure, indicating the Audit sample significantly outperforms the general population of websites. In the process of analyzing the site security scores, several trends were observed:

- Vulnerable ciphers, which creates moderate risk when used in conjunction with older protocols are high risk when used with current protocols. The common flagged ciphers were RC4 and 64-bit block ciphers.
- Failing to support TLS1.2, the latest, safest protocol (lack of TLS1.2 led to failure of the category), or continued use of SSL3.
- Susceptibility to DROWN, POODLE, Heartbleed and OpenSSL attacks and vulnerabilities.[27]

On a positive note, no malicious links or malware were observed on any site. Unfortunately, XSS/iframe vulnerabilities were observed on nearly 26% of sites, more than a three-fold increase from the 8% observed last year. The XSS growth was primarily due to increased telemetry via access to public information reporting XSS vulnerabilities.[28] The Bank 100 had the lowest presence of XSS/iframe vulnerabilities at 27%, but 80% of News sites, and more than half of Federal and Consumer sites were vulnerable. This increase is concerning reinforcing the need for sites to monitor site development and content management systems.

Increasingly, sites' vulnerabilities, fraudulent form completion and/or account signups are being targeted by bot-orchestrated exploits as cyber criminals leverage computing power for their illicit gain. These can range from completion of contest entries and driving advertising click-fraud to attempting to gain access to banking accounts. 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.

To combat this trend, companies should consider utilizing bot detection and mitigation solutions. Testing for basic anti-bot solutions this year was more rigorous then in previous audits, yielding a drop in overall adoption from 75% to 69%. Three additional levels of anti-bot scans were conducted, demonstrating that only 16% of sites were protected from "simple" bots. Only 7% were protected from bots emulating browsers, and less than 5% were protected from "advanced" bots. Improvements from 2016 were observed in all but the basic level of tests. Banks had the best basic anti-bot protection, while News sites had the least with adoption of 85% and 59% respectively.

**SITE SECURITY SCORES**

| | 2014 | 2015 | 2016 | 2017 |
|---|---|---|---|---|
| Internet Retailer Top 100 | 81.9 | 85.7 | 89.6 | 91.1 |
| Internet Retailer Top 500 | 83.3 | 85.3 | 88.3 | 90.6 |
| Bank 100 | 86.5 | 83.0 | 88.3 | 87.7 |
| Federal 100 | 70.5 | 83.6 | 91.6 | 95.2 |
| Consumer 100 | 86.2 | 86.1 | 89.9 | 93.1 |
| News 100 | 83.2 | 83.0 | 85.0 | 88.8 |
| ISP/Hosts | - | - | - | 92.9 |

Figure 13 – Site Security Score Average by Sector

As shown in Figure 13, despite more stringent criteria, year-to-year security scores rose in every sector, with the exception of banks which show a slight drop of 0.6%. For the second year in a row Federal sites outscored all segments with a score of 95.2. Since new vulnerabilities appear frequently, sites need to monitor continually 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/TLS CERTIFICATE TYPES

Recognizing the importance of trust certificates and increasing concerns about 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 to acquire, but do not verify the identity of the acquiring party. As a result, cybercriminals have moved towards acquiring them for phishing and look-a-like domains.[29] [30]

EV SSL certificates provide 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 display. 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 and other organizations.[31] Overall adoption of EVSSL certificates increased to 168,758 certificates, an increase of 13% over 2016, a continuation of the 20% growth from 2015 to 2016.[32]

*"OTA's Audit continues to drive awareness and recognition on the importance of responsible data security and ethical privacy practices," said Internet Society Chief Internet Technology Officer, Olaf Kolkman. "The increase in sites embracing end-to-end encryption shows it is becoming the norm for all site traffic."*

Figure 14 shows adoption rates for each type of certificate by sector. Note the inclusion of the new ISP/Hosts segment shifts the overall data due to the significantly higher level of DV certificate use. Excluding ISP/Host data, certificate share type would be 19.0% DV, 52.7% OV and 28.7% EV. Other contributing factors include a few commercial sites opting to obtain "free" DV certificates.[33] While DV certificates are the same among all certificate authorities, brand owners should consider the benefits of support and services from commercial certificate authorities and the limitations of an automated certificate service. Based on OTA analysis the decline in percentage of EVSSL certificates is attributed to new brands/sites being added, versus site owners "downgrading" to DV or OV certificates.[34]

**SSL CERTIFICATE TYPE**

| | DV | | OV | | EV | |
|---|---|---|---|---|---|---|
| | 2016 | 2017 | 2016 | 2017 | 2016 | 2017 |
| Internet Retailer Top 100 | 10.0% | 7.0% | 65.0% | 65.0% | 25.0% | 28.0% |
| Internet Retailer Top 500 | 19.2% | 22.4% | 51.0% | 46.8% | 29.8% | 30.8% |
| Bank 100 | 2.0% | 6.0% | 28.0% | 32.0% | 70.0% | 62.0% |
| Federal 100 | 8.0% | 7.1% | 82.0% | 84.8% | 9.5% | 8.1% |
| Consumer 100 | 16.7% | 19.2% | 49.0% | 52.9% | 34.3% | 27.9% |
| News 100 | 19.6% | 26.3% | 74.2% | 68.7% | 6.2% | 5.1% |
| ISP/Hosts | - | 33.3% | - | 38.5% | - | 28.1% |
| **Overall** | **16.3%** | **20.5%** | **52.4%** | **51.1%** | **31.2%** | **28.6%** |

Figure 14 - SSL Certificate Type by Sector

## DDoS MITIGATION

While outside the scope of this year's Audit methodology, organizations need to implement measures to help detect and mitigate the impact of a DDoS attack. Based on data from Q1 2017, the average peak attack size increased to 14.1 Gigabits per second (Gpbs), a 26% increase over Q4 2016. The peak volume recorded was 121 Gbps at a speed of 90 million packets per second. [35] While the metrics show amplification of such targeted attacks, they do not tell the entire story. According to Verisign, nearly 50% of their customers were targeted multiple times during the quarter. Globally these attacks remain unpredictable and persistent, and vary widely

in terms of volume, speed and complexity. To combat these incidents, it is becoming increasingly important to constantly monitor the threats in order to optimize the mitigation strategy. OTA recommends on premise firewalls and dedicated DDoS appliances to help stop malicious traffic. When configured properly, the associated malicious traffic can be effectively blocked and dropped before it reaches the intended servers. Recognizing this importance of DDoS mitigation, OTA anticipates future Audits may apply bonus points for adoption, pending the availability of automated testing capabilities.

## VULNERABILITY REPORTING MECHANISMS

New to the 2017 Audit is awarding bonus points for sites/companies that have a mechanism to submit third-party bug or vulnerability reports. It was added in part because it is recognized as a best practice by NTIA, NIST and the FTC. Only 6% of sites overall had a reporting mechanism visible on their site or listed with third-party "bug bounty" service providers. While the Consumer Services segment outpaced all categories with 36.2% adoption, it is concerning that only 2% of bank sites have a "discoverable" reporting mechanism. Having such a mechanism is recognized as critical to effectively respond to third-party researchers and is relatively simple to implement. OTA advocates for sites to have a vulnerability reporting mechanism either hosted on their site (such as the online form designed by OTA) or by one of the leading third-party "bug bounty" programs.[36]

## MALVERTISING

Cybercriminals have recognized the security vulnerability of the advertising ecosystem and increasingly use its complexity to distribute misleading messages and/or ads with malicious 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 ad supported services. A worrying new trend emerging over the past year is the use of even greater technical customization allowing malvertising campaigns to evade detection. In prior years, significant numbers of malvertising attackers used and reused the same exploit kits, but 2017 saw high-ranked publishers hit with new malvertising campaigns specifically crafted for improved stealth to avoid scanning and monitoring tools. At the same time, the common attacks via lower quality traffic continued to push a mix of malware and scams. Upticks have been seen in fake surveys or sweepstakes requesting personal details and in ads linked to infected landing pages (where the "ad" itself is not malicious, so evades publisher's scanning efforts). In addition, provocative "fake news" linking to unsafe pages or pitching scams continue to put consumers at risk, degrade their experience, and erode trust in publisher and product brands.

# PRIVACY, TRANSPARENCY & DISCLOSURES

The 2017 Audit revealed modest improvements in the transparency and readability of published privacy policies. More policies have moved towards consumer-friendly wording with fewer reading like a contract written for a legal audience. In several cases, privacy policies have made clearer distinctions between PII (Personally Identifiable Information) and non-identified data, and how each is used and shared. Some of this may be the result of increased awareness of and preparation for compliance with the EU's upcoming General Data Protection Regulation (GDPR) requirements.[37]

As the deadline for GDPR is now less than twelve months away, it is more important than ever for organizations to strike the balance between data collection, privacy and data stewardship. In addition, organizations need to be aware of the APEC Cross-Border Privacy Rules. Not unlike Privacy Shield, these are a set of voluntary yet enforceable privacy standards to allow data to flow across the Asia-Pacific region.[38] OTA has been advocating for increased transparency and discoverability of privacy policies since 2009, including recommending disclosure of data collection, usage, sharing and retention practices. Best practices include:

Basic notice/disclosure items

- Make sure privacy policy has a link and is easily discoverable from the home page.
- Place the revision date of the policy at the top of the page.
- Provide access to archived versions of the policy, allowing users to see what has changed.
- Use a simple layered and/or short notice designed to help consumers understand the policy. See OTA short form, linking to the full policy – https://otalliance.org/privacy-policy.
- Use icons to help consumers navigate privacy policies in conjunction with layered/short notices.
- Write policies for the site's target audience and demographics. Consider providing multi-lingual versions supporting non-English-speaking site visitors. See the Spanish version of OTA's privacy policy – https://otalliance.org/politica-de-privacida.

Clearly state key compliance practices

- Compliance with Children's Online Privacy Protection Act (COPPA). [39]
- Disclose whether the site honors Do Not Track (DNT) browser settings and preferably honor users' DNT browser settings.
- Provide a summary of the data retention policy, including how long and for what reason data is retained.

Protect privacy and define protected sharing

- Do not share personal data with any third party except to deliver service to the user. Provide a clear statement including details regarding if, what and for what purposes data is shared.
- Require vendor confidentiality by contract and notify consumers that service providers are prohibited from the use or sharing of their data for any purpose other than providing services on behalf of the site.
- Provide disclosure of cross-device tracking.
- Utilize tag management systems or privacy solutions to manage third-party trackers.
- Make best efforts to notify consumers if their data is requested by third parties' due to legal requirements.

The 2017 Audit has reallocated privacy scoring points with increased weighting on the content, transparency and structure of the privacy policy. Previously equal, this year's Audit is weighted 55% for the privacy policy and 45% for use of tracking. Privacy scores averaged 73, up slightly over 2016, which is a positive highlight considering the more stringent criteria and the revised scoring model. Scores ranged from the Bank 100 at 65 to Consumer sites at 82. This marks the second-year banking sites showed a privacy score decline, largely due to the use of standardized privacy notices which focus on compliance requirements versus embracing stewardship and more restrictive data sharing practices. Overall, fewer sites received failing privacy scores (declining to 16% from 24% in 2016), though banks showed a huge increase in failures (from 5% in 2016 to 34% this year). As represented in Figure 15, scores for the privacy policy component (worth 55 points) varied widely across sectors, from a low of 21 for the Bank 100 to an average of 40 for Consumer sites.

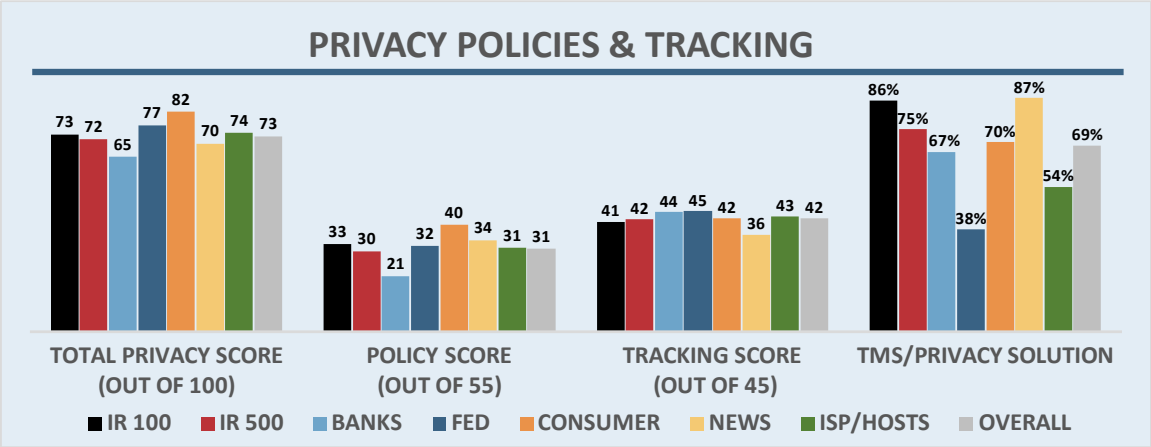


Figure 15 – Privacy Policy Scores and Tracking by Sector

Sites which rely on advertising and third-party analytics are faced with the challenge of managing third-party tracking. A growing challenge for site owners is knowing the respective data sharing practices of partners and the "domino data effect" which may occur with personal data being disclosed. Tag management systems and privacy solutions help monitor third-party data collection and sharing in real time. OTA awarded bonus points if they were present.[40] [41] Overall adoption grew to 69.4%, indicating the likely transition to baseline scoring in future audits. News sites led adoption (87%), with the lowest adoption in Federal sites (38%), attributed to the low number of tags employed and the fact that they do not rely on advertising or data sharing.

## TRANSPARENCY

Meeting consumer expectations by focusing on providing clear affirmative consent action (such as opt-in) versus the "consent by inaction" is an important privacy policy design consideration. Several audited best practices earned bonus points but adoption remains low across most sectors. Providing both a clear notice of policy revisions with a date stamp at the top of the page and a link to archived versions of previous privacy polices helps maximize transparency. The Fed 100 lagged significantly in all areas except honoring of Do Not Track, which is low for all sectors (Figure 16). Version tracking for historical comparison of privacy policies also has relatively low adoption at 6% overall, but saw a jump from 14% to 21% in the Consumer sector. In an effort to maximize transparency, OTA believes linking to archived versions of privacy policies should become a standard practice and likely will shift to baseline scoring in the 2018 Audit.

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 disclose their DNT policy and ideally honor the browser's DNT setting as users visit the site. As shown in Figure 16, overall disclosure of DNT policy continues to rise, now at 37% versus 13% four years ago. Honoring DNT settings, however, remains low with all segments under 5%.

While the precise reason for such low levels of honoring DNT is unclear, some cases appear to be based on the specification not being finalized by the World Wide Web Consortium (W3C), conflicts with monetization objectives, technical limitations or a lack of awareness.[42] Many privacy policies indicated sites were waiting for the formal DNT standard to be approved, while others inappropriately suggest that consumers set opt-out cookie-based mechanisms supported by the Digital Advertising Alliance (DAA). This is concerning because the DAA's opt-out mechanism and the DNT address different issues. The DAA opt-out program only focuses on data used for interest-based advertising; by design it is not privacy enhancing and does not fully address other data collection and sharing.

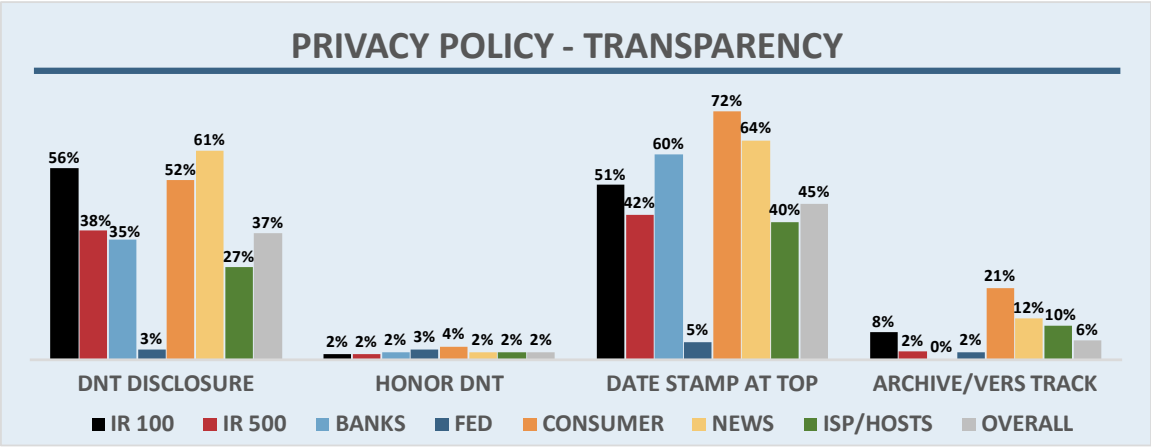

Figure 16 - Privacy Policy Transparency by Sector

## READABILITY & DISCLOSURES

Designing a site's privacy policy for the intended readers versus for the legal audience has been long recognized as a needed shift by privacy professionals. Not only does the language need to be written at the appropriate reading level, but the layout should also maximize readability. Figure 17 outlines results for the baseline requirement of layered short notices, with bonus points awarded for the use of user friendly icons and making the privacy policy available in multiple languages. The only sector other than OTA members with meaningful use of icons is Consumer sites (4%). Support of multi-lingual privacy policies is also in the early stages, growing to 7% overall, led by the ISP/Hosting sector at 19%. OTA believes having the privacy policy in multiple languages helps enhance transparency and readability where English may be a second language.

Maintaining and disclosing data sharing and retention practices is a core component to the privacy policy. Figure 18 outlines the overall trends, with the Bank 100 achieving the lowest overall score in each area, directly impacting their overall score and failure rate. The Fed 100 took top honors in not sharing data while the Consumer segment led with clear data retention policies and requiring vendors to maintain confidentiality.

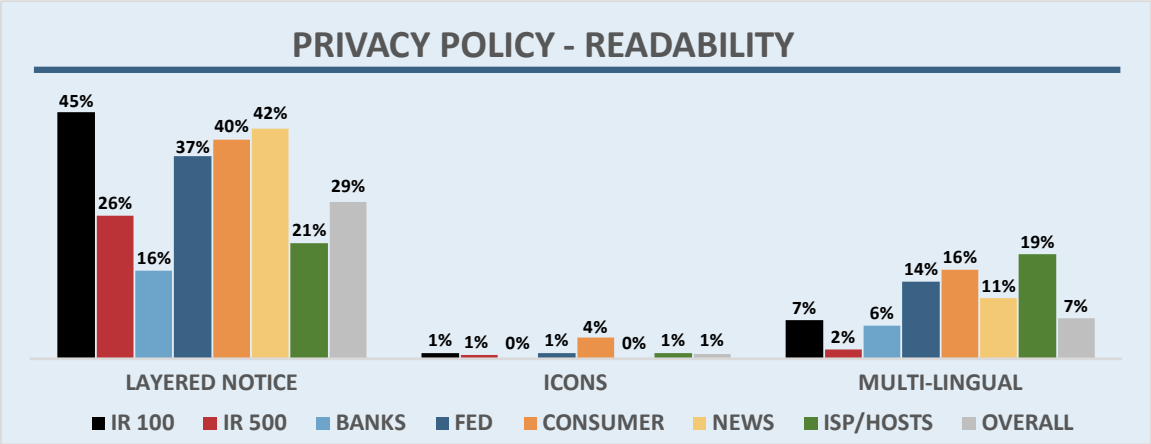


Figure 17 – Privacy Policy Readability by Sector

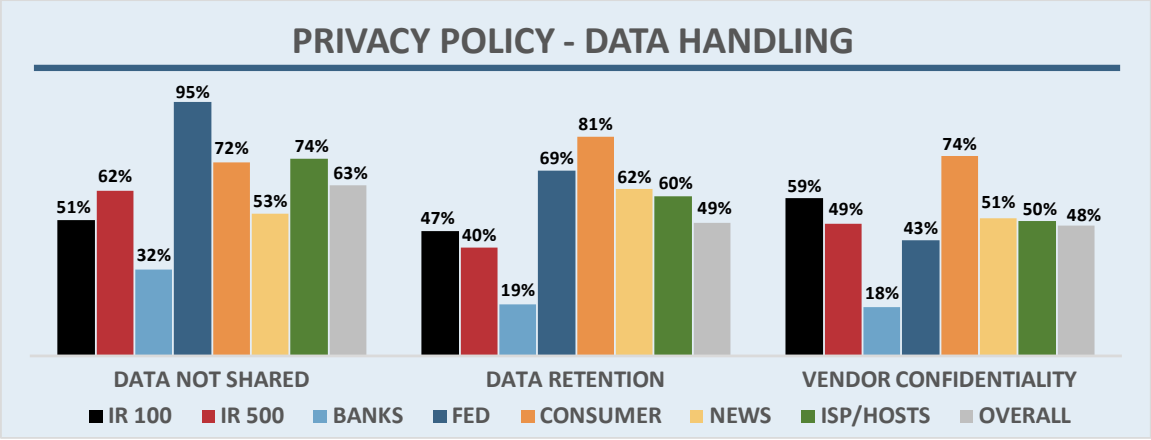


Figure 18 – Privacy Policy Data Handling by Sector

## ADDITIONAL BEST PRACTICES

Responding to the FTC cross-device tracking report released in January 2017, this year's audit reviewed and scored disclosures of tracking across various devices (e.g. desktop, phone, tablet, etc.), finding that 45% of sites make such a disclosure, with variations by sector. It should be noted cross-device tracking has many benefits, including an enhanced user experience when moving between devices and security benefits for users logging in from other devices or IP addresses. Unsurprisingly, the Internet Retailer 100 had the highest level of disclosure at 80%, followed by Consumer sites at 76%. On the other extreme, disclosures within the Fed 100 sector were very low, with only 4% of sites disclosing such tracking. Banks are in the middle with 34% adoption. This may be misleading as the Fed 100 and Bank 100 sites may not enable cross-device tracking as they are not reliant on advertising or tracking, so may perceive less need for it, though they may be missing the related security benefits. As expected, a relatively high percentage (67%) of News/Media sites disclose the use of cross-device tracking. When combined with the relatively high level of third party data sharing, this may raise user concerns about data privacy protection on these ad-supported sites, and without articulating a consumer benefit this may compel users to consider ad blocking and other solutions to obscure their online activities.

## 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 information is posted in the WHOIS database which is available to anyone, providing the registration is not private. This year 87.4% of registrations were public, a slight decline from 89.5% in 2016. Sectors with the largest use of private WHOIS registrations included the Bank 100 (25.0%) and online retailers (14.8%). Private registrations limit consumers' ability to discover who the owner of a site is, impede transparency and may reduce consumer trust, not to mention a third party's ability to contact the site owner regarding an observed vulnerability. Conversely, private registrations are a valid and legitimate practice when registering a domain for a future company, product or marketing effort when in "stealth mode," though they should be made public once launched.

## DATA LOSS INCIDENTS & REGULATORY SETTLEMENTS

Data breaches and regulatory settlements can be indicative of poor data security, privacy and business practices. As such, they can have a major impact on a site's brand reputation and resulting level of consumer trust while placing the privacy and identity of users at risk. At the same time, it is important to recognize there is no perfect security and that a determined adversary with enough time and resources can compromise most any organization. As reported in OTA's 2017 Cyber Incident and Breach Response Guide, there were over 82,000 data loss incidents tracked worldwide in 2016 including 4,149 reported data breaches.[43]

*"Consumer-facing website owners have an important responsibility because their customers entrust them with valuable data," said Roxane Divol, Symantec Executive Vice President and General Manager, Website Security. "The OTA Audit recognizes those who go beyond compliance and demonstrate stewardship of their customers' online security and privacy."*

This year's Audit included advanced telemetry from Risk Based Security and public information from multiple state attorneys general offices. Combined they provide a more comprehensive view of such incidents. OTA's analysis revealed that 132 (13.1%) of the audited organizations experienced one or more incidents, up from 35 organizations last year (4.8%). The number of records lost ranged from a single lost record to over 1.5 billion. Recognizing that all incidents are not equal, organizations who experienced a cumulative loss of 1,000 records or less during the Audit period where excluded from receiving penalty points. This adjustment resulted in a net number of 121 organizations (12.0% of the Audit sample) which experienced one or more incidents. Combined, this equates to 262 incidents exposing over 3.8 billion records containing sensitive or personally identifiable data. Of the sectors, the Bank 100 had the highest incident rate (24%), followed by Consumer sites (23.8%).

On the regulatory front, 21 organizations received a penalty for consumer protection related suits or settlements this year (up from 5 last year), with the Bank 100 having the most (8). This increase is attributed to the inclusion of data from additional agencies and the Consumer Financial Protection Bureau (CFPB). For the Audit, the focus was on settlements related to consumer protection actions and did not include settlements pertaining to mergers and acquisitions and/or labor related settlements. Settlements ranged from agreement to ongoing monitoring by the FTC for twenty years and to curtail any alleged actions, to the record civil fine by the FTC and DOJ awarding $280 million in penalties against Dish Network for Do Not Call violations.[44]

# CONCLUSION

Overall, the 2017 Online Trust Audit results positively surpassed expectations, reaching the tipping point of more than 52% of sites qualifying for the Honor Roll. This increase was significant in light of changes to the methodology, which raised the bar in every core area, and considering that approximately one-quarter of sites audited were new to the Audit. Underscoring the importance of multi-stakeholder initiatives, a record number of organizations not only contributed to the methodology but also downloaded it, watched the OTA webcast and/or contacted OTA directly. Combined, this is evidence that companies are becoming more proactive in their data security, adopting responsible privacy practices and embracing data stewardship moving beyond compliance.

At the same time, the glass remains half-empty in key areas and it is alarming that more than 60% of the largest banks and Federal Government sites received failing grades in one or more category. The security oversights and inadequate privacy policies observed reflect the need to add resources in these areas. These missteps often reflect a lack of ongoing security discipline, failure to take a user-centric view on privacy, and/or organizations not embracing data stewardship and responsible privacy principles.

Increasingly data is the "oil" of the Internet economy. It is fueling innovation, growth and revenue yet if abused or spilled (breached), there is risk of a negative impact to trust and vitality of the Internet. The Audit and failing grades by many sites underscores the urgency to embrace responsible security and privacy practices.

In light of the approaching GDPR implementation deadline (May 25, 2018), organizations of all types and across all sectors would be well advised to develop a "GDPR readiness plan" and use it to revisit their security risks, disclosures and related privacy practices. Moving towards a view of privacy that embraces responsible practices and overall data stewardship will pay long-term dividends. Demonstrating that a company is acting in good faith is critical to the "court of public opinion" and can be equally if not more important than "the court of law".

The 2017 Audit serves three primary objectives:

- Promote best practices to enhance sites' security, data protection and privacy practices
- Recognize excellence in consumer protection, security and responsible privacy practices
- Provide consumer added transparency regarding the security and privacy practices of sites they visit

While the 2017 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 stakeholders seem to be moving in the opposite direction. The shift away from privacy including the reluctance of many within the ad industry to embrace Do Not Track, rescinding of the FCC privacy rules approved in 2016 and current challenges of net neutrality combined may have a negative impact to trust and content access. Left unchecked, the long-term health of the Internet may be at risk.

OTA collaborates with all stakeholders in the public and private sector to work toward improving and enhancing the vitality of the Internet, providing a trusted platform for innovation. For updates visit https://otalliance.org/TrustAudit.

# APPENDIX A - METHODOLOGY & SCORING

The Audit criteria and methodology evolve every year, reflecting the developments in security standards, privacy norms and real-world deployment. Annually, OTA actively solicits input from the Internet at-large through a 60-day call for public comments typically issued in early September, public briefings and hosting of listening sessions with government agencies and NGOS.[45] In addition, several U.S. government agencies and industry standards organizations are consulted. After review, the working group incorporates some of their core security and privacy directives, including Fair Information Practice Principles (FIPPs), NIST standards as well as those supported by the Internet Society's Deploy360 Programme.[46] Reflecting this combined input, weighting and scores are re-examined annually and re-allocated to address the evolving threat landscape, regulatory environment and ease of deployment. The end result focuses on accepted best practices reflecting real-world deployment, bridging the gap between the standards and business communities. The final methodology for this year's Audit was published in January 2017 and promoted via webinars and public briefings with the goal to provide site owners the ability to re-evaluate their practices and optimize their scores. [47]

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

- Consumer Protection (DNS, Domain & Brand Protection)
- Site, Server, Application & Infrastructure Security
- Privacy, Transparency & Disclosures

Sites were eligible to receive 300 base points (up to 100 points in each category), and up to 60 bonus points (20% of the base score) for implementing emerging best practices. This re-weighting of bonus points from upwards of 70 points in previous years recognized the risk that bonus points could mask security and privacy deficiencies. Additionally, organizations could lose up to 60 points for having regulatory settlements, data breaches, observed vulnerabilities and other key deficiencies.

To qualify for the Honor Roll, sites had to receive a composite score of 80% or better *and* a score of at least 60 in each of the three main categories. This reflects a 5-point increase over past years' failure bar, recognizing that "security is only as strong as the weakest link" and sites are built on a "chain of trust".

The 2017 Audit has been powered by technical analysis and data provided from over a dozen organizations. Without their assistance and support, this Audit and telemetry would not be possible. Data sampling was completed over a thirty-day period between April 20, 2017 and May 19, 2017. Industry leading service providers included: Agari, DigiCert, Disconnect, Distil Networks, Ensighten, High-Tech Bridge, Infoblox, Malwarebytes, Microsoft, Risk Based Security, Security Scorecard, SiteLock, SSL Labs, Symantec, The Media Trust, ValiMail and Verisign provided customized research, data and analysis. Additional data was obtained from public data sources including BugCrowd, Google, HackerOne, Open Bug Bounty, Twitter, SSL Labs, Two Factor Auth (2FA) and others. 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.

## CONSUMER PROTECTION (DNS, DOMAIN & BRAND PROTECTION)

Email continues to be the top attack vector of choice, driving business email compromise (BEC), credential and identity theft, bank account takeovers and distribution of malware. The FBI reports that BEC fraud has amounted to $5.3 billion in financial losses since 2013, most of which could have been prevented.[48] For the past decade OTA has advocated for end-to-end email authentication to help detect and block malicious and spoofed email for all domains and subdomains managed by an organization. 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 targeted brand.

- Email authentication (Sender Policy Framework (SPF) and DomainKeys Identified Mail (DKIM)) at top-level ("corporate") domains, and all email subdomains. The 2017 Audit increases weighting on authenticating top level domains (most recognizable to the user and most frequently spoofed), with reduced points for separate delegated sub-domains. In addition, sites with invalid SPF records did not receive credit – *part of base score* [49]
- Domain-based Message Authentication, Reporting & Conformance (DMARC). New for 2017, DMARC records where p=none and have no reporting (RUA or RUF), do not receive any credit. Referred to as "naked DMARC records", they do not provide any consumer or brand protection value since receiving networks not respond to the policy and the brands do not get authentication and abuse reports – *part of base score* [50]
- Implementation of "opportunistic" Transport Layered Security (TLS) for email – *bonus points*[51]
- Domain locking – *penalty if domain not locked*
- Domain Name System Security Extension (DNSSEC) – *bonus points* [52]
- Implementation of Internet Protocol version 6 (IPv6) – *bonus points* [53]
- Multi-factor authentication (new for 2017) – Recognizing the importance to help prevent account takeovers and unauthorized account access, sites are awarded bonus points for implementing any form of multi-factor authentication – *bonus points* [54] [55]

## 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 60. Sites were tested with several tools to look for known vulnerabilities, HSTS configuration and mismatched certificates. [56, 57] New in 2017, server security has expanded to include application security, patching cadence, IP reputation and additional network security elements.[58]

### Bonus / Penalty Points

- Extended Validation SSL Certificates (EV SSL) – *bonus points* [59]
- Adoption of Always On SSL (AOSSL) – *bonus points* [60]
- Web Application Firewall – *bonus points* [61]
- 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 – *penalty if incidents have been observed since January 2017* [62]

- Vulnerability & Bug Reporting Mechanism – New for 2017, sites earn bonus points for reporting mechanisms including online forms and/or using third-party bug bounty reporting. Data was analyzed by online searches using key words, as well as searching third-party bug bounty programs including HackerOne and Bugcrowd [63, 64]

## PRIVACY, TRANSPARENCY & DISCLOSURES

Best practices for all organizations include providing users with clear notice, transparency and control of the data being collected, tracked and shared with third parties. The privacy score is comprised of up to 100 points covering: inclusion of appropriate disclosures; structure of the privacy policy itself (including adoption of generally accepted Fair Information Practice Principles (FIPPS)); and tracking and third-party data collection.[65]

Privacy Policy – 55 points possible (increased from 50 points in 2016), to include added criteria and the importance of policy transparency and disclosures. Sites can receive maximum scores by adhering to the following guidelines:

- Link / discoverability from the home page
- Date stamping of privacy policy on the top of the page
- Designed as a layered and/or short notice
- Compliance with Children's Online Privacy Protection Act [66]
- Disclosure and response on handling of a browser Do Not Track (DNT) setting
- Provide a data retention policy statement
- 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

Third-Party Tracking on Site – 45 points possible (decreased from 50 points in 2016) for sites with no third-party trackers (with the exception of anonymous analytics). Observed trackers known to share data with third parties resulted in reduced points.[67]

### Bonus Points

- Version tracking, including posting of revision mark-ups or archived versions
- Use of consumer-friendly icons to assist navigation
- Localized/multi-lingual policy where English may be a "second language"
- Honoring of a user's Do Not Track browser (DNT) setting
- Cross device Tracking Disclosures (added in 2017) [68]
- Implementation of tag management systems or privacy solutions to manage third party tags

### Penalty Points

- Data breaches – *penalty if incident since January 2016*
- Regulatory settlements with the Federal Trade Commission (FTC), Federal Communications Commission (FCC), Consumer Financial Protection Bureau (CFPB)[69] and/or State – *penalty if settlement since January 2016.*
- Public vs. Private WHOIS registration – *penalty if private* [70]

# APPENDIX B – 2017 "TOP 50" HONOR ROLL

| Sector | Site | Sector | Site |
|---|---|---|---|
| C | Airbnb | C, O | Identity Guard |
| R, O | American Greetings Corp. | C | Indeed |
| C | Blogger | C | Instagram |
| C | Booking.com | C, O | LifeLock |
| C | Box | C, O | LinkedIn |
| R | BuildDirect Technologies Inc. | R | LivingSocial Inc. |
| G | Census Bureau | C | Meetup |
| R | Chewy Inc. | I, O | Microsoft Azure |
| R | Costco | I, O | Microsoft Outlook.com |
| G | Health & Human Services (Healthcare.gov) | N, O | MSN |
| I | Digital Ocean | C, O | OneDrive |
| C | Dropbox | C | Pinterest |
| R | Etsy Inc. | C, O | Publishers Clearing House |
| G | Federal Communications Comm. (FCC) | C, N | Reddit |
| G | Federal Deposit Insurance Corp. (FDIC) | C | Snapchat |
| R | Fitbit Inc. | C | Spotify |
| C | Foursquare | I | Squarespace |
| R, O | Gap Inc. | R | The RealReal |
| C | Glassdoor | C, O | Twitter |
| C | Google Docs | G | U.S. Dept. of Education |
| I | Google Gmail | G | U.S. Postal Service |
| N | Google News | R | Under Armour Inc. |
| C | Google Play | C | UpWork |
| I | Google Sites | C | YouTube |
| C, I | iCloud | C | Zynga |

Sector Codes: C – Consumer Services, F – Bank 100, G – Government, I – ISP/Hosters, N – News/Media, O – OTA / Internet Society Member, R – Retailers. As noted brands (sites) can be in multiple segments.

Note the Top 50 reflects the top 50 consumer facing sites and does not include OTA members. Expanding the ranking to all sites in the Audit, the following additional OTA members would be in the top 50: Constant Contact, DigiCert, Distil Networks, Intelius, Kromtech Alliance Corp., MacKeeper, Malwarebytes, Marketo, People Connect, Symantec, ValiMail, Verisign and ZEDO. The addition of OTA members shifts the achievement in the Top 50 by sector would include; OTA members tied with Consumer Services at 40% of the overall 50 sites. Internet Retailers and ISPs/Hosters score at 12% each, and Gov and News/Media at 6%.

# APPENDIX C – 2017 HONOR ROLL RECIPIENTS

## 2017 Internet Retailer 500 – Honor Roll

51% Honor Roll - 42% Failing - 2% "Top of Class"

1-800 Contacts Inc.
2 A/X Armani Exchange
3 AAFES
Abercrombie & Fitch Co.
AC Lens
Adore Me
Albertsons Inc. (was Safeway)
Aleva Stores
2 Alex and Ani LLC
6 Alibris Inc.
6 Amazon.com Inc.
American Apparel Inc.
2 American Eagle
3 American Girl LLC
6 **American Greetings**
3 Amway
3 APMEX Inc.
2 Apple Inc.
AppliancePartsPros.com Inc.
2 Ashford.com
Ashley Stewart Inc.
AutoZone Inc.
3 Avon Products Inc.
B&H Photo-Video
Backcountry.com
Barnes & Noble Booksellers Inc.
BaubleBar Inc.
3 BCBG Max Azria Group LLC
2 Bealls Inc.
5 Best Buy Co. Inc.
Better World Books
Beyond the Rack
6 BikeBandit.com
3 BJ's Wholesale Club
2 BlissWorld LLC
2 Blue Apron Inc.
Blue Nile Inc.
2 Bluefly Inc.
3 Bonobos
2 Bookbyte
Boscov's Department Store LLC
2 Boxed Wholesale
5 Build.com Inc.
5 BuildASign.com
3 **BuildDirect Technologies Inc.**
3 Burberry Ltd.
6 Cabela's Inc.
Callaway Golf Co.
Carter's Inc.
Casper
2 Cat5 Commerce
Charlotte Russe Inc.
**Chewy Inc.**
2 Chico's FAS Inc.
Christopher & Banks Corp.
2 ClickBank
2 Code42 Software Inc.
3 **Costco Wholesale Corp.**
CPO Commerce LLC
Crate and Barrel
3 Crutchfield Corp.
CustomInk
CVS Caremark Corp.
2 Cymax Stores Inc.
DeepDiscount.com
Dell Inc.
Destination Maternity Corp.
Diamond Nexus
Dick's Sporting Goods
Diesel
Dillard's Inc.
Directron.com
3 Discount Dance Supply
5 DiscountRamps.com LLC
3 Dollar Shave Club
Dolls Kill
4 DoMyOwnPestControl.com
Dover Saddlery Inc.
DSW Inc.
3 eBags Inc.
3 Eddie Bauer LLC
eImprovement LLC
3 Entertainment Earth Inc.
3 eSalon.com LLC
5 **Etsy Inc.** ◆
5 evo
4 Express Inc.
Fanatics Inc.
6 Fathead LLC
2 **Fitbit Inc.**
2 Follett Higher Education
Foot Locker Inc.
3 Forever 21
3 Fossil Inc.
2 Gaiam Inc.
5 GameFly Inc.
6 GameStop Corp.
3 **Gap Inc.**
2 GiftCardLab.com
Godiva Chocolatier Inc.
2 Google Play
2 GoPro Inc.
2 Groupon Goods
H&M
2 Harry's Inc.
2 hhgregg Appliances Inc.
Home Chef
Hot Topic Inc.

**Bold** – Top 50 Consumer Facing ◆ – Top score in sector ❷ ❸ ❹ ❺ ❻ – Consecutive years as Honor Roll recipient

# 2017 Internet Retailer 500 – Honor Roll, continued

- ❻ HSN Inc.
- ❷ Hugo Boss AG
- ❸ iHerb Inc.
- ❸ IKEA.com
- Indigo Books & Music Inc.
- ❷ Indochino Inc.
- IS3 Inc.
- J. Hilburn Inc.
- J.C. Penney Co. Inc.
- ❺ JackThreads Inc.
- JamesAllen.com
- ❸ Jimmy Jazz
- ❸ Joann.com
- ❸ K&L Wine Merchants
- ❸ Kate Spade
- Keurig Green Mountain Inc.
- Kohl's Corp.
- Lakeshore Learning
- ❷ Lands' End
- Leesa Sleep LLC
- Lenovo Group Ltd.
- ❸ LifeWay Christian Resources
- LightIntheBox Ltd.
- Living Spaces
- ❺ **LivingSocial Inc.**
- ❷ Lowe's Cos. Inc.
- LuLu's Fashion Lounge Inc.
- Macy's Inc.
- Mattress Firm Inc.
- ❸ MEC
- MeUndies
- Michael Kors Holdings Ltd.
- ❻ Microsoft Corp.
- MidwayUSA Inc.
- ❺ Minted LLC
- Monkey Sports Inc.
- ❸ Monoprice Inc.
- Moosejaw
- ❷ Motorsport Aftermarket Group
- MotoSport LLC
- ❸ Musician's Friend Inc.
- MVMT Watches
- ❷ NakedWines.com Inc.
- National Business Furniture LLC
- National Football League
- National Geographic Society
- ❸ National Hockey League
- ❷ NatureBox Inc.
- ❸ NBTY Inc.
- Nebraska Furniture Mart
- New Balance Athletics Inc.
- ❹ Newegg Inc.
- ❹ Nike Inc.
- Nine West Holdings Inc.
- ❹ Nordstrom Inc.
- ❸ Nuts.com
- Office Depot Inc.
- ❸ OmahaSteaks.com Inc.
- ❸ Online Stores LLC
- ❷ O'Reilly Auto Parts
- Organize-It
- ❻ Overstock.com Inc.
- Panasonic Corp.
- ❸ Parts Express International Inc.
- Patagonia
- ❻ Payless ShoeSource Inc.
- ❷ Pep Boys
- ❸ Petco Animal Supplies Inc.
- ❷ PetFlow
- PetSmart Inc.
- ❸ Pier 1 Imports Inc.
- Poppin
- ❷ Power Equipment Direct Inc.
- ❹ PromGirl LLC
- ❷ PropertyRoom.com Inc.
- ❸ Purchasing Power LLC
- ❸ PureFormulas.com
- Purple
- QVC Group
- ❺ Ralph Lauren Media LLC
- ❸ RealTruck Inc.
- ❸ REI
- Reitmans (Canada) Ltd.
- Renegade Furniture Group
- Replacements Ltd.
- ❷ Restoration Hardware
- Richline Digital (was Gemvara)
- ❷ Ritani LLC
- ❸ Rock Bottom Golf
- ❺ RockAuto LLC
- rue21 Inc.
- ❷ Saatva Inc.
- Sears Holdings Corp.
- ❷ Sheet Music Plus LLC
- ❸ Shindigz
- Shinola
- ❸ Shoebuy
- ShopLadder
- SmartSign.com LLC
- ❷ Softchoice Corp.
- Spanx Inc.
- ❺ Spiraledge (was SwimOutlet)
- ❹ Spreadshirt Inc.
- ❷ Stage Stores Inc.
- Staples Inc.
- Starbucks Corp.
- ❷ Summit Racing Equipment
- Sur La Table Inc.
- ❹ Sweetwater
- Target Corp.
- Team Express Distributing LLC
- ❷ Tech for Less LLC
- Tempur-Pedic
- Tennis Warehouse
- Textbooks.com
- The Buckle Inc.
- ❸ The Clymb
- The Great Courses
- ❸ The Grommet
- ❻ The Gymboree Corp.

**Bold** – Top 50 Consumer Facing ◆ – Top score in sector ❷ ❸ ❹ ❺ ❻ – Consecutive years as Honor Roll recipient

## 2017 Internet Retailer 500 – Honor Roll, continued

- ❷ The Home Depot Inc.
- ❸ The Honest Company Inc.
- The Kroger Co.
- The Lakeside Collection
- ❸ The Orvis Co. Inc.
- ❷ **The RealReal Inc.**
- Thrift Books Global LLC
- Thrive Market
- Tiffany & Co.
- ❸ Tilly's Inc.
- ❸ Tire Rack Inc.
- Title Nine
- ❸ TJX Cos. Inc.
- ❸ TOMS Shoes Inc.
- Tractor Supply Co.
- Trina Turk
- Tuft & Needle
- ❹ **Under Armour Inc.**
- V2
- Wal-Mart Stores Inc.
- ❸ Warby Parker
- ❺ Wayfair Inc.
- ❺ Weight Watchers
- Wine Library
- ❷ Wine.com Inc.
- Wolverine Worldwide Inc.
- ❸ Zazzle Inc.
- ❸ Zumiez Inc.

## 2017 Top 100 Banks – Honor Roll

### 27% Honor Roll - 65% Failing – 0% "Top of Class"

- ❷ Ally Bank
- ❹ Arvest Bank
- ❻ Bank of America
- ❷ Bank of Hawaii
- ❷ Bank of the West
- ❹ BBT (Branch Bank & Trust)
- ❸ Capital One
- Chemical Bank
- CIT Bank
- ❹ City National Bank
- ❸ Discover
- ❸ First Republic Bank
- ❻ Frost Bank
- Great Western Bank
- ❸ Huntington Bancshares, Inc
- ❸ IBERIA Bank
- ❷ Key Bank
- ❺ Morgan Stanley
- ❹ Regions Financial Group
- ❷ Sun Trust
- Synovus Financial Corp
- ❷ The Private Bank
- ❷ Umpaqua Bank
- ❸ Union Bank (MUFG Union Bank, NA)
- ❻ US Bank NA ◆
- ❻ Wells Fargo
- ❷ Whitney Bank

**Bold** – Top 50 Consumer Facing ◆ – Top score in sector ❷ ❸ ❹ ❺ ❻ – Consecutive years as Honor Roll recipient

# 2017 U.S. Federal Government 100 – Honor Roll

## 39% Honor Roll - 60% Failing - 6% "Top of Class"

- ❸ **Census Bureau**
- Dept of Agriculture
- Dept of Commerce (NIST)
- Dept of Commerce (NTIA)
- ❸ Dept of Education
- **Dept of Education (Grants & Aid)**
- ❸ Dept of Energy
- Dept of Energy (Energy Star)
- ❷ **Dept of Health & Human Svcs (Healthcare.gov)** ◆
- Dept of Health and Human Services (HHS)
- Dept of Homeland Security (DHS)
- ❸ Dept of Interior
- Dept of Interior (US Geological Survey)
- ❷ Dept of Justice (DOJ)
- Dept of Labor
- ❸ Federal Bureau of Investigation (FBI)
- **Federal Communications Commission (FCC)**
- **Federal Deposit Insurance Corporation (FDIC)**
- Federal Emergency Management Agency (FEMA)
- Federal Trade Commission (Consumer Info)
- Federal Trade Commission (Do Not Call)
- ❸ Federal Trade Commission (FTC)
- ❸ First Gov (USA.gov)
- Government Printing Office (GPO)
- ❷ Library of Congress (LOC)
- ❸ National Aeronautics and Space Admin (NASA)
- ❸ National Institutes of Health (NIH)
- National Oceanic and Atmospheric Admin (NOAA)
- ❸ National Park Service (NPS)
- National Science Foundation (NSF)
- Small Business Administration
- ❸ Social Security Administration (SSA)
- ❸ US Government Jobs
- ❸ US Postal Service
- **US Postal Service (Store)**
- US Postal Service (Tools)
- ❷ US Senate
- ❸ White House
- White House (Petitions)

**Bold -** Top 50 Consumer Facing ◆ – Top score in sector ❷ ❸ ❹ ❺ ❻ – Consecutive years as Honor Roll recipient

# 2017 Consumer 100 – Honor Roll

## 76% Honor Roll - 20% Failing - 25% "Top of Class"

- ❷ 1040.com
- ❷ 1040NOW
- ❷ **Airbnb**
- ❷ All Clear ID
- ❷ Ancestry
- AOL
- ❻ Badoo.com
- BigFishGames
- **Blogger**
- ❷ **Booking.com**
- ❹ **Box**
- ❷ CareerBuilder
- Classmates
- Craigslist
- DeviantArt
- ❷ DocuSign
- ❹ **Dropbox**
- ❺ eHarmony
- Equifax
- ❸ eSmart (Liberty Tax)
- ❷ Expedia
- ❸ ezTaxReturn.com
- ❻ Facebook
- ❷ FileYourTaxes
- ❺ Fiverr
- ❸ Flickr
- ❺ **Foursquare**
- ❷ Free Tax Return.com
- ❸ FreeTaxUSA
- ❷ **Glassdoor**
- Goodreads
- ❸ **Google Docs**
- ❷ **Google Play Music**
- ❸ H&R Block
- Hotels.com
- ❹ **iCloud**
- ❷ **Identity Guard**
- IdentityForce
- IMDb
- ❷ Imgur
- ❷ **Indeed**
- ❺ **Instagram**
- ❷ KAYAK
- ❷ **LifeLock** ◆
- ❻ **LinkedIn**
- ❷ Lyft
- ❸ Match.com
- ❷ MediaFire
- ❷ **Meetup**
- ❷ Miniclip
- ❷ Monster
- ❷ MyHeritage
- ❷ OkCupid
- **OneDrive**
- ❷ Orbitz
- ❷ Pandora
- ❺ **Pinterest**
- PlentyofFish
- ❷ Priceline
- ❻ **Publishers Clearing House**
- ❷ **Reddit**
- ❷ Rotten Tomatoes
- ❷ **Snapchat**
- ❷ SoundCloud
- ❷ **Spotify**
- Tagged
- ❸ TaxACT
- ❸ TaxSlayer
- ❷ TripAdvisor
- ❻ Tumblr
- ❻ **Twitter**
- ❷ Uber
- **UpWork**
- ❷ VK
- Wikipedia
- ❺ Wordpress
- ❹ Yahoo!
- ❺ **YouTube**
- ❷ Zoosk
- ❻ **Zynga**

**Bold** – Top 50 Consumer Facing ◆ – Top score in sector ❷ ❸ ❹ ❺ ❻ – Consecutive years as Honor Roll recipient

## 2017 News/Media 100 – Honor Roll

48% Honor Roll - 49% Failing - 3% "Top of Class"

About.com
② American City Business Journals
AOL News
Boston.com
Bostonglobe.com Sites
② Business Insider
② BuzzFeed
CNET
Dallas Morning News
② Disney Interactive
Edmunds.com
Elite Daily
② Engadget
Everyday Health
Financial Times
Forbes
② Fortune
② Gizmodo
④ **Google News** ◆
Huffington Post
Jezebel
LifeHacker
Mashable
② Mic
Mirror Online
② **MSN News**
National Geographic
NBC News
④ New York Times
Politico
② **Reddit**
Refinery29
Rolling Stone
Slate
TechCrunch
② The Atlantic
The Daily Beast
② The Guardian
The New Republic
The Onion
The Street
TMZ
② Vice
Vox
② WebMD
Wired
② Yahoo News
ZDNet

## 2017 ISPs, Carriers & Hosters – Honor Roll

47% Honor Roll - 51% Failing - 3% "Top of Class"

1&1
AOL Mail
Automattic
BlueHost
Bright House Networks
C Spire Wireless
CenturyLink
Charter Communications
Consolidated Communications
Cox Communications
**Digital Ocean**
Enom Inc
Frontier Communications
GMX Email
**Google Gmail**
**Google Sites**
HostGator
HostWay
**iCloud Mail**
Incapsula Inc
KnownHost, LLC
Lightower Fiber Networks
Linode
LiquidWeb
Mail.com
Media Temple
MetroPCS
**Microsoft Azure** ◆
**Microsoft Outlook.com**
Name.com
Namecheap
New Dream Network, LLC
Peer 1 Network (USA) Inc
ProtonMail
SingleHop
Skyriver Communications
SoftLayer
**Squarespace**
Time Warner Cable
T-Mobile
Verizon
Verizon Wireless
Weebly
Windstream
Yahoo Mail
Zoho Mail

**Bold** – Top 50 Consumer Facing ◆ – Top score in sector ② ③ ④ ⑤ ⑥ – Consecutive years as Honor Roll recipient

# 2017 OTA Members – Honor Roll

## 97% Honor Roll - 3% Failing – 34% "Top of Class"

- ❺ ACT, The App Association
- ❹ Act-On Software
- ❷ AdBlock Plus
- ❸ ADT
- ❻ **American Greetings**
- ❻ Agari
- ❸ Brand Protect
- Classmates
- ❹ Coles
- ❻ **Constant Contact**
- ❷ Device Authority
- ❻ **DigiCert**
- Digital Content Next
- ❹ **Distil Networks**
- ❷ Dmarcian Inc.
- ❻ Ensighten
- ❻ Epsilon
- ❷ Eyeo
- ❹ Flybuys
- ❸ **Gap**
- ❻ GetResponse
- Global Cyber Alliance
- Guardian Life
- ❻ Harland Clarke Digital
- ❻ High-Tech Bridge SA
- ❻ IBM/Silverpop
- ❻ Iconix
- ❻ **Identity Guard**
- Identity Theft Council
- ❷ Infoblox
- **Intelius**
- Internet Society
- ❻ **Intersections**
- ❸ **Kromtech Alliance Corp.**
- ❹ LashBack
- ❸ **LifeLock**
- ❸ **MacKeeper**
- ❸ **Malwarebytes**
- ❻ **Marketo**
- ❻ **Microsoft**
- ❷ National Assoc. of REALTORS
- Norton
- ❻ **Online Trust Alliance** ◆
- OpenX
- ❹ Optizmo
- **People Connect**
- ❻ **Publishers Clearing House**
- ❻ Sailthru
- Security Scorecard
- ❸ Simpli.Fi
- ❺ SiteLock
- ❻ **Symantec**
- ❹ The Media Trust
- ❻ TRUSTe
- ❻ TrustSphere
- ❻ **Twitter**
- ❸ UnsubCentral
- ❷ **ValiMail**
- ❺ **VeriSign**
- ❷ Yes Lifecycle Marketing
- ❺ **ZEDO**
- ❷ Zeta Interactive

**Bold** – Top 50 Overall ◆ – Top score in sector ❷ ❸ ❹ ❺ ❻ – Consecutive years as Honor Roll recipient

# APPENDIX D - SAMPLE PRIVACY LANGUAGE

The following draft language has been provided to help organizations consider how to enhance the transparency and notice of key measured criteria. It is recognized these are optional, yet are part of the focus of the Audit to encourage organizations to responsible privacy practices and enhanced disclosures. Readers are encouraged to review these with their legal counsel for applicable regulatory requirements.

1. Control of your Personal Information - Do Not Track Disclosure (DNT)
   For a site to maximize their base privacy score they must have a DNT disclosure in their privacy policy. It should be noted that pointing to the Digital Advertising Alliance (DAA) or Network Advertising Initiative (NAI) opt-out mechanism may not meet the disclosure requirements of the California Online Privacy Protection Act for allowing consumer choice about the collection of personal information across sites and over time.[71]

   Honor DNT:
   "[Company] respects enhanced user privacy controls. We support the development and implementation of a standard "Do Not Track" (DNT) browser feature, which has been designed to provide users control over the collection, sharing and use of information by third parties regarding their web-browsing activities. [Company] respects a user's DNT setting and will not share any information with third parties with the exception of those providing services on our behalf as outlined in this policy and for security and fraud detection services."

   Or, if you do **not** Honor DNT:
   "At this time, we do not respond to "Do Not Track" signals sent from Web browsers or other mechanisms that provide users the ability to exercise choice regarding the collection of personally identifiable information about a user's online activities over time and across third party Internet services. You also may opt-out through blocking third party cookies and other tracking technologies through your browser settings.

   Or, if you are waiting for the W3C spec to be finalized:
   [Company] respects enhanced user privacy controls. We support the development and implementation of a standard "Do Not Track" (DNT) browser feature, which is being designed to provide customers with control over the collection and use of information by third parties. At this time [Company] does not respond to DNT mechanisms. Once a standardized "Do Not Track" feature is released, [Company] intends to adhere to the browser settings accordingly.

2. Data retention
   "We will retain your information for [x months / year(s) or] as long as your account is active or as needed to provide you with services. If you wish to cancel your account or request that we no longer use your information to provide you services, contact us at [company email address]. We will retain and use your information as necessary to comply with legal obligations, resolve disputes, and enforce our agreements."

3. Children's Online Privacy Protection Act (COPPA) [72]
   "This Site is not directed to children. We do not knowingly collect personally identifiable information from children under age 13 [or other age]. If we become aware that a child under 13 [age] has provided us with Personal Information, we will delete such information from our files."

Alternative - “We do not knowingly collect personal information from individuals under age 13 [or other age]. If you are under the age of 13, [age] please do not submit any personal information through the Site. If you have reason to believe that we may have accidentally received personal information from an individual under age 13, [age] please contact us immediately at _____.”

4. Data sharing with vendors

   “We may provide third-parties [vendors and/or contractors] access to your personal information in the course of assisting in operating our business and providing products or services to you. These third-parties may include vendors and suppliers that provide us with technology, services and/or content for the operation and maintenance of our Site or Service. Access to your personal information by these third-parties is limited to the information reasonably necessary for them to perform their limited functions. We require our third-parties to keep the personal information they are provided confidential and to comply with the terms of this Privacy Policy.”

   Alternative - “We may use third parties as necessary to perform functions in connection with the Site or Service. We may share information about you that they need to perform their functions and in accordance with our agreements which prohibits data usage for any other purpose.”

5. Notification to users where and when legally permitted

   “Regardless of the choices you make regarding your information (as described herein) and to the extent permitted by applicable law, we may disclose information about you to third parties pursuant to a request from law enforcement or pursuant to other legal or regulatory process, or as otherwise required by law, or, at our sole discretion, to protect our rights, property or interests, including to enforce this Privacy Policy or our Terms of Service. In the event that we are legally compelled to disclose your personal information to a third party, we will make reasonable efforts to notify you unless doing so would violate the law or court order.”

6. Social network integration

   “We integrate services from social networks on our site. These services may use cookies, web beacons, and other technologies to provide measurement services, target ads, or to help you share content. The information social networks collect may personally identify you to the social network. To control this behavior, you can block cookies in your browser while browsing our site. To learn more about the privacy practices of the social networks to which you belong, you should consult their privacy disclosures.”

7. Cross device tracking

   “Some of our ad partners use information about your logged-in status on different devices, as well as other data regarding the technical characteristics about your devices, to associate these devices with you and to target ads to you across devices. You can opt of out of this category of advertising by using the opt-out options we provide for interest-based advertising.”

# APPENDIX E – BEST PRACTICE CHECKLIST

| | | |
|---|---|---|
| **DNS, Domain, Brand & Consumer Protection** | | |
| ❑ | SPF records & DKIM at the corporate and sub domains | Base Score |
| ❑ | DMARC records with reject/quarantine policy | Base Score |
| ❑ | Naked DMARC records (p=none and no RUA or RUF) | Invalid |
| ❑ | Opportunistic TLS for email | Bonus Points |
| ❑ | Implement DNSSEC | Bonus Points |
| ❑ | IPv6 Adoption | Bonus Points |
| ❑ | Multi-Factor Authentication | Bonus Points |
| ❑ | Domain locked | Penalty for not locking |
| ❑ | Inbound email authentication and DMARC checking | Not scored; recommended |
| **Site, Server & Infrastructure Security** | | |
| ❑ | Server Security & Configuration | Base Score – aggregate, multiple tests |
| ❑ | SSL/TLS Certificate, Protocol, Key Exchange, Ciphers | Base Score – aggregate, multiple tests |
| ❑ | Server Patching Cadence | Base Score |
| ❑ | Certification Authority Authorization (CAA) | Not scored, recommended (planned for 2018) |
| ❑ | Certificate Type (EV SSL) | Bonus Points |
| ❑ | Always on SSL (https by default) | Bonus Points |
| ❑ | Web Application Firewall | Bonus Points |
| ❑ | Malware, malicious links, malvertising incident | Penalty |
| ❑ | Anti-Bot Protection | Penalty for failure to have protection |
| ❑ | XSS / iFrame Vulnerability | Penalty |
| ❑ | Vulnerability / Bug Reporting Mechanism | Bonus Points |
| ❑ | DDoS Mitigation Mechanisms | Not scored, recommended (planned for 2018) |
| **Privacy Policy, Tracking, Transparency & Disclosures** | | |
| ❑ | Link to privacy policy on home page | Base Score |
| ❑ | Privacy policy date stamp at top of page | Base Score |
| ❑ | Layered short notice design (links/expand sections) | Base Score |
| ❑ | Children's Online Privacy Protection Act (COPPA) | Base Score |
| ❑ | "Do Not Track" (DNT) disclosure | Base Score |
| ❑ | Data retention statement | Base Score |
| ❑ | Personal data not shared without permission | Base Score |
| ❑ | Vendors contractually held to privacy policy | Base Score |
| ❑ | Archived/prior version of privacy policy available | Bonus Points |
| ❑ | Icons used to clearly identify sections | Bonus Points |
| ❑ | Multi-lingual policy option clearly linked | Bonus Points |
| ❑ | Honor DNT browser setting | Bonus Points |
| ❑ | Disclosure of cross-device tracking | Bonus Points |
| ❑ | Tag Management System (TMS) in place | Bonus Points |
| ❑ | Notify if personal data is requested by 3rd party | Bonus Points |
| ❑ | Presence of 3rd Party tracking tags | Penalty, number of trackers |
| ❑ | Data breach reported | Penalty, number of incidents |
| ❑ | FTC/FCC/CFPB/State enforcement action | Penalty, number of settlements |
| ❑ | Is your WHOIS record Private? | Penalty |

# APPENDIX F – IMPLEMENTATION RESOURCES

2017 Online Trust Audit https://otalliance.org/TrustAudit

2017 Audit Methodology https://otalliance.org/2017Methodology

2017 Trust Audit Virtual Press Room https://otalliance.org/2017AuditVPR

2017 Trust Audit Press Release https://otalliance.org/2017TrustAudit

## Best Practices

Always on SSL https://otalliance.org/AOSSL

Certification Authority Authorization (CAA) https://cabforum.org/

DMARC https://otalliance.org/DMARC

DNSSEC https://otalliance.org/DNSSEC

DNSSEC Test Tool https://dnssec-debugger.verisignlabs.com/

SSL Certificate best practices https://otalliance.org/SSL

Email Authentication https://otalliance.org/Eauth

Extended Validations SSL Certificates Brand Benefits https://otalliance.org/EVSSL

IPv6 https://internetsociety.org/IPv6

Malvertising https://otalliance.org/Malvertising

SPF / DMARC Record Checker https://otalliance.org/EauthTool

SSL Server Test Tool https://ota.ssllabs.com/

SSL/TLS Server Test Tools https://www.htbridge.com/ssl/

Web Server Security Test https://www.htbridge.com/websec/

SecurityScorecard Test Tool https://instant.securityscorecard.com/

Transport Layered Security (TLS) for email https://otalliance.org/TLS

Vulnerability / Bug Report Form https://otalliance.org/VulnerabilityReports

## Related Resources

Cyber Incident & Breach Response Readiness Guide https://otalliance.org/Incident

IoT Trust Framework https://otalliance.org/IoT

Smart Home Resources https://otalliance.org/SmartHome

Email Marketing Unsubscribe Practices https://otalliance.org/unsub

Native Advertising Transparency Audit https://otalliance.org/Native

Vision of Trust White Papers https://otalliance.org/vision-trust

Internet Society – Deploy360 Programme https://www.internetsociety.org/deploy360/

Internet Society; Global Internet Report http://www.internetsociety.org/globalinternetreport/

# ACKNOWLEDGEMENTS

Data and analysis assistance has been provided in part by Agari, DigiCert, Disconnect, Distil Networks, Ensighten, Google, High-Tech Bridge, Infoblox, Malwarebytes, Microsoft, Risk Based Security, SecurityScorecard, SiteLock, SSL Labs, Symantec, The Media Trust, Twitter, Two Factor Auth (2FA), ValiMail and Verisign. In addition, special thanks to report editors and contributors including Matt Ford (Internet Society), Olaf Kolkman (Internet Society), Melissa Krasnow, (VLP Law Group LLP), Steven Roosa (Holland & Knight LLP), Liz Shambaugh-Spiezle, Madelon Smith, Craig Spiezle and Jeff Wilbur of the Online Trust Alliance. Special thanks for *Internet Retailer Magazine* and Vertical Web Media for data from the Top 500 Guide®.

## ABOUT THE OTA

OTA is an initiative within the Internet Society (ISOC), a 501c3 charitable non-profit with the mission to promote the open development, evolution, and use of the Internet for the benefit of all people throughout the world. OTA's mission is to enhance online trust, user empowerment and innovation through convening multi-stakeholder initiatives, developing and promoting best practices, responsible privacy practices and data stewardship. Updates to the Audit and related resources are posted at https://otalliance.org/TrustAudit.

To learn more about OTA visit https://otalliance.org and the Internet Society at https://www.internetsociety.org.

*Sponsored in part by*





# ENDNOTES

[1] 2017 Global Survey on Internet Security & Trust https://www.cigionline.org/internet-survey

[2] OTA IoT Trust Framework https://otalliance.org/IoT.

[3] 2016 Online Trust Audit – Virtual Press Room https://otalliance.org/2016-online-trust-honor-roll-virtual-press-room-vpr

[4] While sector definitions and criteria for inclusion have remained constant, individual companies may be change due to reported revenues, site traffic ranking and the impact of market consolidation. 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.

[5] 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.

[6] Bank 100 is based on assets as reported by the Federal Reserve as of September 30, 2016 https://www.federalreserve.gov/releases/lbr/current/

[7] Top ranked consumer sites or edge providers based on site traffic for which the provider requires the user to subscribe or establish an account in order to use the service and are neither financial services or ecommerce focused.

[8] Data does not include results of the OTA Member sector due to their high level of achievement and would distort the chart axis.

[9] Board of Governors of the Federal Reserve System, Regulation P: Compliance Guide. https://www.federalreserve.gov/bankinforeg/regpcg.htm

[10] EFF Electronic Frontier Foundation https://www.eff.org/

[11] DMARC is currently not an IETF standard, but this is an example where industry drives adoption ahead of standards bodies, creating "de facto" standard.

[12] Includes both electronic and physical data loss incidents.

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

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

[15] Verisign DDoS https://www.verisign.com/en_US/security-services/ddos-protection/index.xhtml

[16] IETF RFC 4408 https://www.ietf.org/rfc/rfc4408.txt

[17] Gmail TLS for email warning https://arstechnica.com/information-technology/2016/02/gmail-to-warn-you-if-your-friends-arent-using-secure-email/

[18] ICANN DNSSEC Report http://stats.research.icann.org/dns/tld_report/

[19] IPv6 adoption http://www.worldipv6launch.org/measurements/

[20] USG IPv6 & DNSSEC deployment status https://usgv6-deploymon.antd.nist.gov/cgi-bin/generate-gov

[21] High-Tech Bridge SA https://www.htbridge.com/ssl/

[22] Qualys SSL Labs https://www.ssllabs.com/projects/documentation/

[23] DROWN (Decrypting RSA with Obsolete and Weakened eNcryption) https://drownattack.com/

[24] https://otalliance.org/resources/type/advertising-integrity-fraud

[25] CAA Overview https://blog.qualys.com/ssllabs/2017/03/13/caa-mandated-by-cabrowser-forum

[26] Source: Trustworthy Internet Movement SSL Pulse Report https://www.trustworthyinternet.org/ssl-pulse

[27] See SSL Pulse report for summary data https://www.trustworthyinternet.org/ssl-pulse/

[28] Open Bug Bounty https://www.openbugbounty.org/report/

[29] Let's Encrypt https://letsencrypt.org/

[30] See SSL overview https://otalliance.org/SSL

[31] 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

[32] April 2017 data from Netcraft https://www.netcraft.com/

[33] Let's Encrypt free and automated certificate service https://letsencrypt.org/

[34] Note that approximately one-fourth of the sites in 2017 are new to the Audit, making a direct year-to-year comparison difficult.

[35] Verisign DDoS Trends Report https://www.verisign.com/en_US/security-services/ddos-protection/ddos-report/index.xhtml

[36] OTA Vulnerability Reporting Form https://otalliance.org/VulnerabilityReports

[37] GDPR https://en.wikipedia.org/wiki/General_Data_Protection_Regulation

[38] APEC Cross-Border Privacy Rules http://www.cbprs.org/

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

[40] Scanning capabilities provided by OTA member Ensighten, www.ensighten.com .

[41] Note while the presence of such solutions was verified, it is possible sites may not use the solutions or data.

[42] W3C Tracking Protection Working Group http://www.w3.org/2011/tracking-protection/

[43] OTA 2017 Incident Response Guide https://otalliance.org/Incident

[44] FTC Dish Networks Settlement https://www.ftc.gov/news-events/press-releases/2017/06/ftc-doj-case-results-historic-decision-awarding-280-million-civil?utm_source=govdelivery

[45] Call for comments press release https://otalliance.org/2017auditCFC

[46] Internet Society Deploy360 Programme https://www.internetsociety.org/deploy360/

[47] January 31, 2017 methodology press release https://otalliance.org/news-events/press-releases/ota-announces-methodology-ninth-annual-online-trust-audit

[48] BEC Fraud http://www.eweek.com/security/business-email-compromise-scams-continue-to-grow-with-5.3b-in-losses

[49] OTA email authentication overview, resources and tools https://otalliance.org/eauth

[50] OTA overview of DMARC and resoruceshttps://otalliance.org/DMARC

[51] SSL/TLS security and deployment best practices https://otalliance.org/best-practices/TLS

[52] DNSSEC https://en.wikipedia.org/wiki/Domain_Name_System_Security_Extensions

[53] IPv6 https://en.wikipedia.org/wiki/IPv6

[54] White House Lock Down Your Login September 2016 - https://obamawhitehouse.archives.gov/the-press-office/2016/09/28/fact-sheet-launch-lock-down-your-login-public-awareness-campaign

[55] May 8, 2017 U.S. Social Security Administration requires two-factor authentication http://www.healthcareinfosecurity.com/social-security-to-try-two-factor-authentication-again-a-9900

[56] Qualys SSL Labshttps://ota.ssllabs.com/

[57] High-Tech Bridge SA https://www.htbridge.com/ssl/

[58] SecurityScorecard https://securityscorecard.com/

[59] EVSSL https://otalliance.org/resources/extended-validation-certificates-evssl

[60] AOSSL https://otalliance.org/AOSSL

[61] 2017 telemetry enhanced with data using https://nmap.org/nsedoc/scripts/http-waf-detect.html

[62] Malvertising https://otalliance.org/malvertising

[63] NTIA Vulnerability Reporting Guidelines and practices https://www.ntia.doc.gov/other-publication/2016/multistakeholder-process-cybersecurity-vulnerabilities

[64] OTA Vulnerability Reporting Form https://otalliance.org/VulnerabilityReports

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

[66] COPPA https://www.ftc.gov/tips-advice/business-center/privacy-and-security/children's-privacy

[67] Third party tracking data – Primary source includes data from https://disconnect.me/trackerprotection/blocked netting out https://disconnect.me/trackerprotection/unblocked

[68] FTC Cross Device Tracking Recommendations https://www.ftc.gov/system/files/documents/reports/cross-device-tracking-federal-trade-commission-staff-report-january-2017/ftc_cross-device_tracking_report_1-23-17.pdf

[69] CFPB https://www.consumerfinance.gov/

[70] January 31, 2017 methodology press release https://otalliance.org/news-events/press-releases/ota-announces-methodology-ninth-annual-online-trust-audit

[71] CADOJ https://www.oag.ca.gov/sites/all/files/agweb/pdfs/cybersecurity/making_your_privacy_practices_public.pdf

[72] https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/childrens-online-privacy-protection-rule




Rev621