2014
ONLINE TRUST AUDIT & HONOR ROLL

Independent Audit of Best Practices In:

- Domain, Brand & Consumer Protection
- Site, Server & Infrastructure Security
- Data Protection, Privacy & Transparency

OTA
Online Trust Alliance

released June 17, 2014

TABLE OF CONTENTS

OVERVIEW AND BACKGROUND

As society and businesses increase their dependency on the Internet, consumers are faced with perplexing choices due to growing data security and privacy threats. In an effort to enhance online trust and recognize companies who have demonstrated a holistic approach to consumer protection, data security and privacy, the OTA has developed the Online Trust Audit and Honor Roll.

Since being introduced in 2010, the OTA Online Trust Audit continues to set the standard for independent review and analysis of best practices and controls. This report serves as the foundation for business and technical decision makers as they bring new products and services to the market. The Audit underscores the imperative that data security, protection and privacy need to be keystones of every online service, web site and mobile application.

The development of this report and the respective methodology represents OTA's commitment to open and transparent multi-stakeholder initiatives. A public call for comments was issued in November 2013 in parallel with meetings with trade organizations, consumer advocates and leaders in the private and public sector. The feedback and recommendations were incorporated into the methodology released in March 2014. OTA then hosted webinars and workshops in April 2014 prior to the start of data collection. This process represents OTA's commitment to providing businesses prescriptive advice to optimize their security, brand protection, data and privacy practices. Organizations that have followed suit are to be commended for their commitment to their customers, employees and stockholders.

Consumers, regulators and the media should recognize organizations that have demonstrated a pattern of leadership and stewardship of their online properties. Conversely, one should question and consider organizations that have been conspicuously absent from the Honor Roll year after year. A cursory look points to a strong correlation between brands who have failed to qualify for the Honor Roll and those that have subsequently experienced data breach incidents. Businesses that fail to adopt a security and privacy by design culture and a data stewardship mindset risk disenfranchising consumers, validating the need for increased regulatory oversight and inviting lawsuits.

It is important to recognize that this analysis is limited to a slice of time. Based on the dynamic nature of site and application configuration and the evolving threat landscape, sites' scoring and qualifications for the Honor Roll may have changed. All analysis was done anonymously without the participation of the sites being analyzed.

Sites tested were selected based on their ranking within their individual sectors (or membership in OTA) and at no time has any organization been able to solicit its inclusion or attempt to impact the scoring. In instances where a significant vulnerability or risk was identified, OTA attempted to contact the "at-risk" entity. With the exception of organizations where OTA had a pre-existing contact, most efforts to engage these companies were not successful.

Supplemental reports will be issued over the next six months. These will include a review of mobile application security and privacy best practices, mapping to the respective web sites of the Internet Retailer 100. In addition, an in-depth analysis of email authentication practices used to counter the rise of malicious email will be published.

SECTORS EVALUATED

The 2014 Honor Roll examined the brand protection, security and privacy protection practices of approximately 800 websites across the following sectors:

- 2014 Internet Retailer top 100 (IR 100)
- 2014 Internet Retailer top 500 (IR 500)[1]
- FDIC top 100 banks (FDIC 100)
- Top 50 federal government sites (Federal 50)
- Top 50 social networking and sharing sites (Social 50)
- Top 50 news and media sites (News 50) – new in 2014
- OTA member companies (OTA Members)

With the exception of the News 50, all sectors have been evaluated for the past several years. Though sector definitions and criteria for inclusion have remained constant, individual companies may be added or removed from sector lists due to revenue/traffic ranking and the impact of market consolidation and acquisitions. This consistency allows year-over-year analysis within a sector. Segmenting the Internet Retailer top 100 from the top 500 based on 2013 revenues allows comparison of best practice implementation between large and small companies, and the newly added News 50 gives insight into practices of sites used daily by hundreds of millions of consumers.

[1] Raw data is from the Internet Retailer Top 500 Guide (http://www.internetretailer.com/top500/), a ranking of the largest North American e-retailers by online sales, produced by Vertical Web Media, publisher of Internet Retailer magazine.

METHODOLOGY AND SCORING

The criteria used in the Honor Roll are highly relevant to the security and privacy practices companies must implement to maximize online trust. The 2014 Online Trust Audit includes a composite analysis focusing on three major categories:

- Domain, Brand & Consumer Protection
- Site, Server & Infrastructure Security
- Data Protection, Privacy & Transparency

The criteria for this year's report are indicative of the most current best practices supported by industries, standards bodies and government agencies.

Sites were eligible to receive 300 total base points, including up to 100 points in each category, and up to 30 total bonus points for implementing emerging best practices. As in previous years, the specific scoring criteria continue to evolve with best practices supported by OTA, other organizations and government agencies. The criteria are adjusted to address the constantly evolving threat environment and the need for all sites to continually monitor their security and privacy practices, in essence "raising the bar" for Honor Roll qualification. To qualify for the Honor Roll, sites had to receive a composite score of 80% or better ***and*** a score of at least 55% in each of the three main categories. The minimum scoring requirement was instituted in 2013 recognizing that sites are built on a "chain of trust" that is only as strong as its weakest link.

Data sampling was completed between April 15 and May 23, 2014. In total, more than 300 million email headers and approximately 8,500 web pages were reviewed. 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. We also recognize that the sites examined might be using other technologies (which our tools or research did not detect) to authenticate domains or subdomains, secure their infrastructures, track users on their sites, etc.

A complete list of criteria, along with notes regarding scoring changes from previous reports, is shown below. The 2014 methodology is posted at https://otalliance.org/initiatives/2014-methodology.

DOMAIN, BRAND & CONSUMER PROTECTION

- Email Authentication (Sender Policy Framework and DomainKeys Identified Mail) – *part of base score, maximized by implementing both methods at top-level and subdomains*
- Domain-based Message Authentication, Reporting & Conformance (DMARC) – *part of base score, increased weighting in 2014*
- Domain Locking – *penalty if domain not locked*

SITE, SERVER & INFRASTRUCTURE SECURITY

- Secure Sockets Layer (SSL) Server Configuration – *base score of 100, with increased granularity and requirement levels in 2014*
- Extended Validation SSL Certificates (EV SSL) – *bonus points*
- Testing for XSS, iframe exploits, malware, malicious links – *penalty if these threats exist (new in 2014)*
- Always On SSL (AOSSL) – *bonus points*
- Domain Name System Security Extension (DNSSEC) – *bonus points*

DATA PROTECTION, PRIVACY & TRANSPARENCY

- Privacy Policy – *part of base score*
- Third Party Tracking on Site – *part of base score*
- Layered Privacy Policy – *bonus points (new in 2014)*
- Do Not Track Privacy Policy disclosure – *bonus points (new in 2014)*
- Honoring of Do Not Track Browser Settings (DNT) – *bonus points*
- Implementation of Tag or Privacy Management Systems – *bonus points (new in 2014)*
- Public vs. Private WHOIS registration – *penalty if private*
- Data Breach & Loss Incidents – *penalty if incident in last 2 years*
- FTC / State Legal Settlements – *penalty if settlement in last 2 years*

The factors are weighted and scored based on the impact they have on email safety, brand protection, website security, consumer transparency, and overall best practices that will distinguish an organization and brand from a business and consumer perspective. Results are used to assess each organization's qualifications for the OTA Honor Roll as well as to compare sectors via an Online Trust Index (OTI) which tracks key sectors' adoption of best practices on a normalized scale.

Since the release of the 2014 criteria, several dozen companies including leading banks, retailers and OTA members have contacted OTA asking for guidance. Due to the sensitivity of this data and risk of disclosing vulnerabilities, individual organizations' scores and data are not publicly available, nor are they shared with any third party or OTA member. Information will be provided to site owners upon written request and verification. For details, including reporting fees, please email editor @ otalliance.org.

ONLINE TRUST HONOR ROLL HIGHLIGHTS

The primary goal for this report is to highlight and recognize companies demonstrating their commitment to online trust and consumer protection. A secondary goal is to promote best practices and provide prescriptive tools and resources to aid companies in enhancing their security, data protection and privacy practices.

Twitter, for the second year in a row, received the highest score across all sectors, followed by American Greetings who outscored all online retailers and e-commerce sites. These companies have demonstrated a consistent commitment to collaboration and data sharing including participation in multiple working groups, the standards community and industry associations.

In addition, OTA recognized the top 10 scores among the Internet Retailer 500. Joining American Greetings, the 2014 recipients include Ancestry.com, Big Fish, Books-A-Million, ChristianBooks.com, JackThreads, Netflix, Newegg, Sony Electronics, Walmart.com and Zulily. These companies represent a broad range of revenues from Walmart.com, ranked number 4, to Books-A-Million (BAM), ranked 476 by Internet Retailer Magazine. Similar findings were observed in 2013, validating that the best practices advocated by OTA are achievable by companies of any size.

As shown in Figure 1, of the organizations evaluated for the Honor Roll, 30.2% qualified for the Honor Roll this year (vs. 32.2% last year). Netting out the News 50 sector provides a direct comparison, yielding an adjusted 2014 Honor Roll rate of 32.1%. It is encouraging the 2014 results are on par with 2013, considering the addition of new criteria and enhanced scoring granularity raised the bar this year. More than one-third of qualifiers (88) achieved Honor Roll status for the third year in a row, and nearly another third (77) qualified for the second year in a row. 69 Companies made the Honor Roll for the first time, highlighting that security and privacy practices are not a static process – sites need to continually monitor, update, evolve and innovate to keep pace with evolving threats. A complete list of Honor Roll recipients by sector can be found in Appendix A.[2]

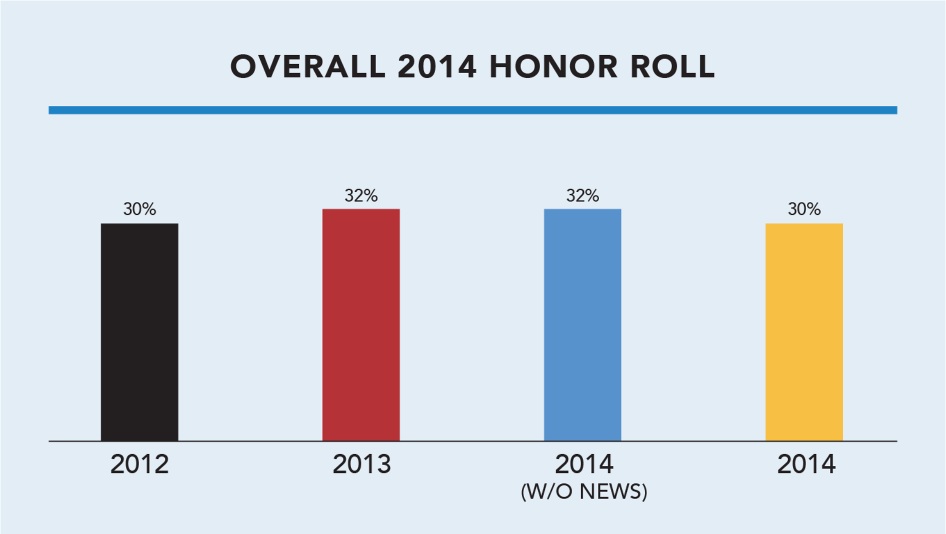

Figure 1 – Overall Honor Roll Achievement by Year

[2] Due to scoring ties, the 2014 Top 10 Internet Retailers includes 11 individual companies.

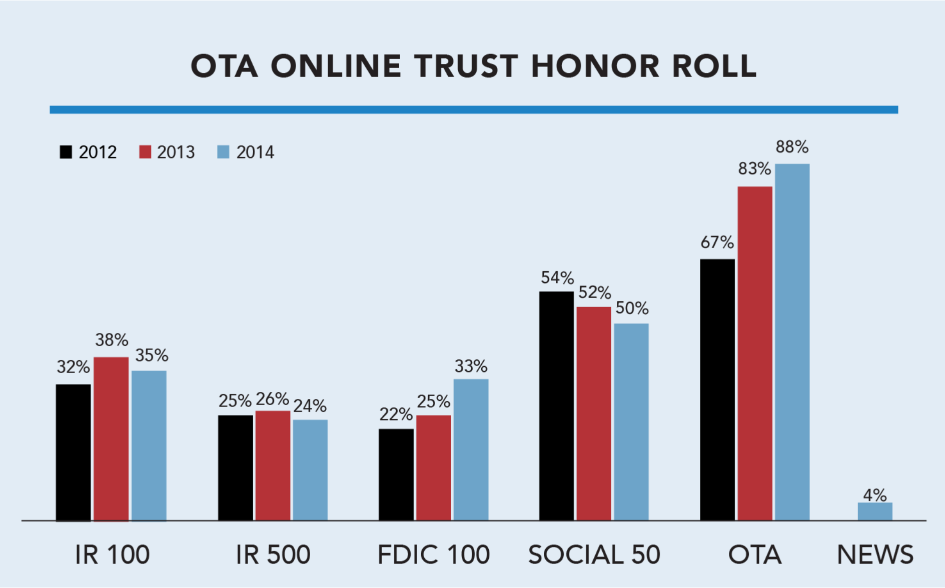

Figure 2 – Percentage Achieving 2014 Honor Roll Status by Sector

Figure 2 shows the percentage of organizations in each sector achieving Honor Roll status. Not surprisingly, OTA members lead with 88% of members qualifying. It is recognized that results may be somewhat biased since companies self-select by becoming OTA members/sponsors and these companies are also active participants in development of best practices.

Outside OTA, the Social 50 outpaced all other sectors. Their high scores are in part a reflection of system architectures that are much more homogeneous and integrated. Somewhat surprising was that only 4% of the News 50 made the Honor Roll, highlighting a significant need to improve practices. While it is recognized companies in this sector are not generally conducting financial or commerce transactions, their lack of adoption of best practices is cause for alarm. For example, 34% of the sites sampled do not encrypt their registration or log-in screens, leaving such personal data exposed and ripe for abuse.

Examining year-over-year results, there was solid growth in the OTA member and FDIC 100 sectors, and slight dips in the Social 50 and IR 100/500 sectors. These dips are attributed to more stringent scoring requirements, not deprioritizing of security and privacy-enhancing practices by the organizations evaluated. These changes were incorporated due to the combination of the escalating threat landscape, evolving technical standards and global privacy regulatory requirements.

It is also useful to examine the reasons why organizations did not achieve Honor Roll status. Figure 3 shows the percentage of each sector that had a failing grade (<55%) in one or more of the three main categories. Figure 4 breaks that down a step further to show which categories caused the failures.

Failures were most prominent in the FDIC 100 and News 50 sectors, and least prominent in OTA members. The IR 100 fared better than the IR 500, as they have the past three years. This can be attributed to the fact that larger companies have been more frequently targeted by cyber criminals, have deeper security and privacy staffing, and in the wake of highly-publicized breaches are more conscious of the risk to their brand image and reputation. These factors have led them to more likely be early adopters of the outlined best practices.

Inadequate domain and brand protection was the primary cause for failures in all but the IR 100/500, mostly due to the shift in scoring that placed increased emphasis on comprehensive implementation of email authentication standards and practices. This area was especially damaging to the FDIC 100 and News 50 sectors, with nearly half of the companies receiving failing scores.

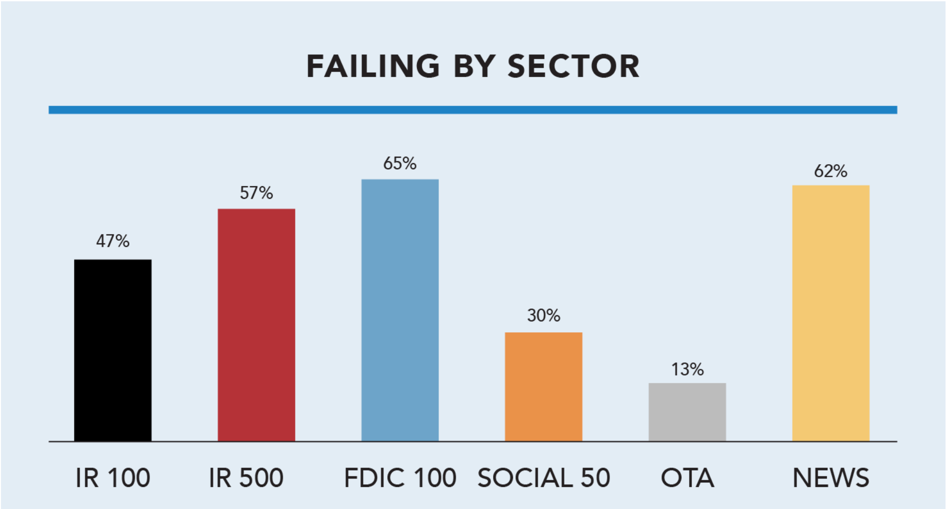

Figure 3 – Percent of Companies with Failing Grade by Sector

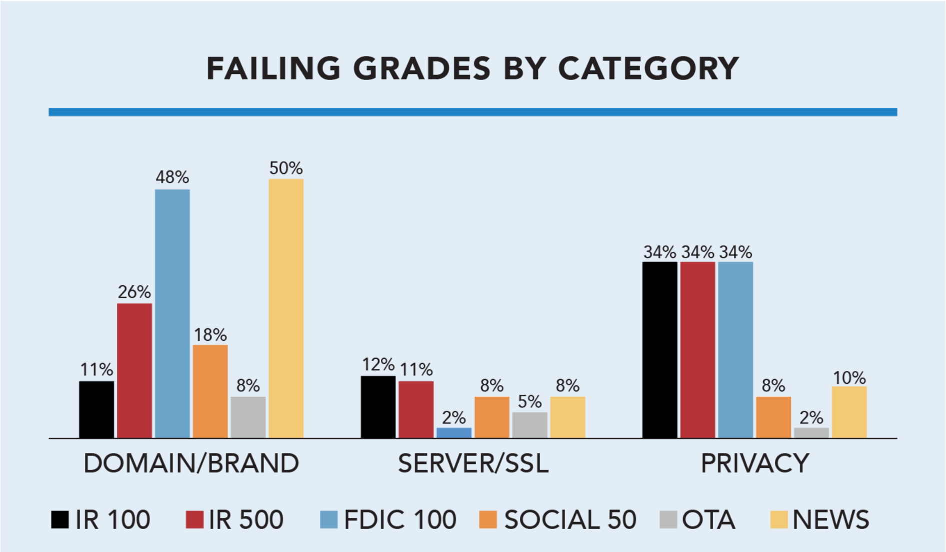

Figure 4 – Percent of Companies with Failing Grade by Sector and Category

Insufficient privacy practices constituted the next largest cause of failures, with one-third of the IR 100/500 and FDIC 100 receiving failing scores. Though it continues to be a high cause of failure, it should be noted the FDIC sector made notable improvements in their privacy policies with increased disclosure and reduced data sharing with unaffiliated third parties. Site security was the lowest cause of failure, showing that the vast majority of organizations across all sectors have implemented at least the minimum recommended level.

The Online Trust Index (OTI), introduced in 2012, provides a normalized view of scoring among sectors. The OTI is calculated as an average composite score across all methodology categories, using a normalized score of 1 to 100.

Figure 5 shows the year-to-year results, while Figure 6 shows the breakdown by major category. Despite the more rigid criteria, OTI scores remain relatively consistent. The News 50 sector had the lowest OTI score, driven by very low scores in email authentication and privacy a lack of SSL usage on sites requiring user registration.

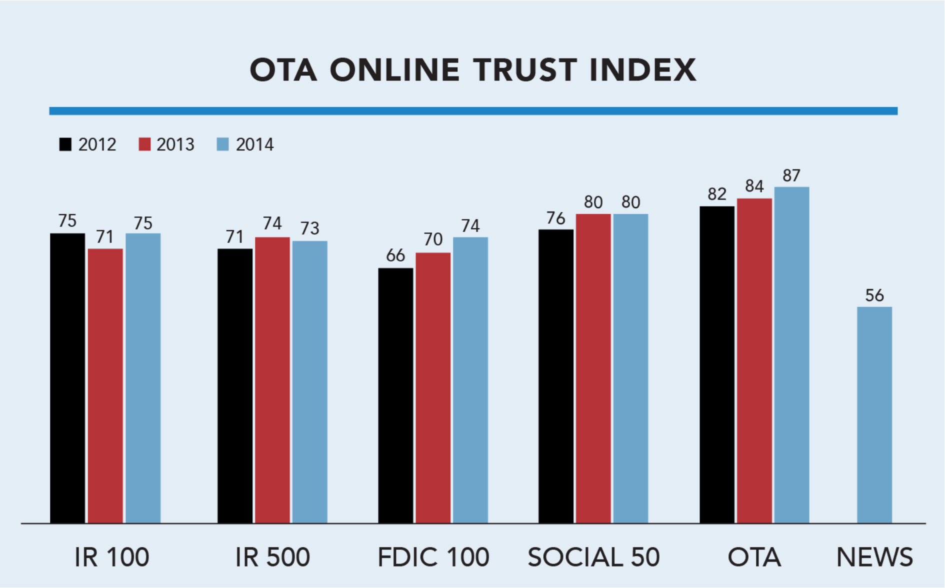

Figure 5 - Online Trust Index by Sector

Reviewing the OTI category scores in Figure 6, it can be seen that the Domain/Brand protection and Privacy areas have the highest variability, while the Server/SSL category scores were tightly clustered. The Domain/Brand scores are primarily based on the thoroughness of email authentication, and the main reasons for low scores are the lack of support for SPF and DKIM at top-level domains. While marketers have been quick to adopt at the delegated sub-domain level, this offers little or no protection from the spoofing and malicious email purporting to come from the main corporate domains. A secondary cause for low scores is lack of DMARC records – the email community and respective trade organizations need to engage their customers to optimize their brand and consumer protection efforts.

In the Privacy category, low scores are due to lack of clear notice in privacy policies, incomplete and outdated privacy policies, and use of website trackers that share information with other entities. Other contributing factors are the lack of layered privacy notices and "Do Not Track" disclosures. It is important to note these shortfalls can be remedied in a straightforward manner within the site's privacy policy and by a re-evaluation of who they share data with.

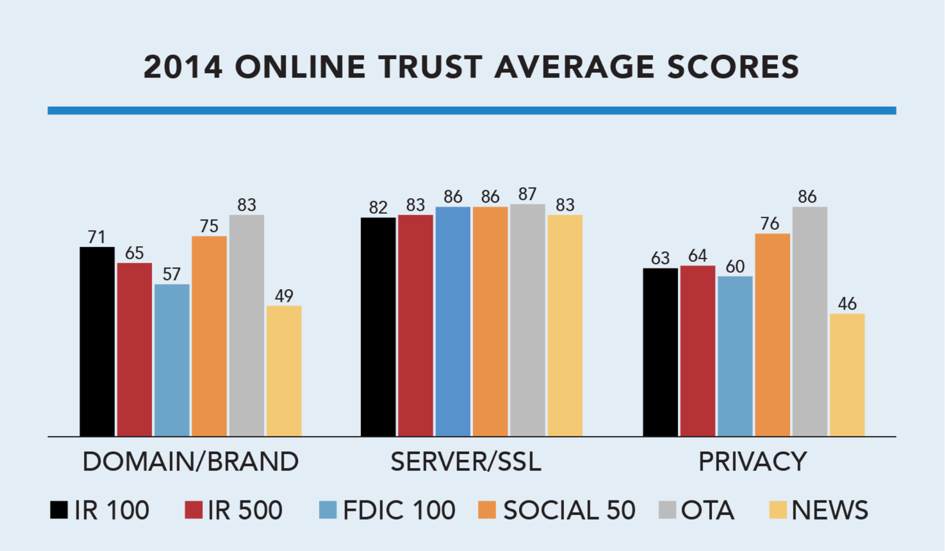

Figure 6 – Major Category Scores by Sector

INDIVIDUAL BEST PRACTICES HIGHLIGHTS

DOMAIN, BRAND & CONSUMER PROTECTION

- Email Authentication (SPF & DKIM) – Adoption continues to rise across all sectors, especially in use of both SPF and DKIM (e.g., IR 500 adoption rose from 56% to 74%, and the IR 100 leads all sectors with 88% of companies supporting both). Adoption of either SPF or DKIM is being led by the Social 50 and OTA with each scoring nearly 100%.
- Domain-based Message Authentication, Reporting & Conformance (DMARC) – Adoption continues to rise in all sectors, yet remains disappointingly low considering the ease of implementation and proven technical and brand protection benefits. There remains significant room for improvement, especially in the Fed 50, FDIC 100, and IR 100/500 sectors.

SITE, SERVER & INFRASTRUCTURE SECURITY

- SSL Server Configuration – Reflecting more rigorous criteria and increased scoring granularity, overall scores dipped from 85.0 to 83.4. Only the FDIC 100 and Social 50 had increased scores.
- Extended Validation SSL Certificates (EV SSL) – Worldwide use grew more than 39% to more than 103,000 deployed certificates. Adoption is led by the FDIC 100 (64%).
- Always On SSL (AOSSL) – Recognizing the need to encrypt entire user sessions to optimize security and privacy, the FDIC 100 leads all sectors with 78% adoption.
- Domain Name System Security Extension (DNSSEC) – Only the Fed 50 has significant adoption (92%). DNSSEC continues to struggle as an IT priority in spite of its technical value.

DATA PROTECTION, PRIVACY & TRANSPARENCY

- Privacy Policy & Third Party Tracking – All sectors but the Fed 50 were evaluated, and the overall average was 64.7, a slight dip from the 66.5 average in 2013. This was primarily due to the low score in the News 50 sector (45.9). The IR 100 showed a large increase (80.1 vs. 63.0 last year).
- Layered Notice – New in 2014, 10.5% of sampled sites were found to have layered privacy policies. The clear leader is the FDIC 100 (44%), followed by OTA members (17.2%). The IR 500 lagged at only 3.2%. This is an emerging best practice that will require attention in all sectors and is expected to be incorporated into base scoring in future audits.
- Do Not Track (DNT) Disclosure – New in 2014, this tracks whether the privacy policy specifies support of DNT. Overall 13.1% of sites meet California's disclosure requirements, led by the News 50 (22%).[3]
- Honoring of Do Not Track (DNT) Browser Settings – Added in 2013, this category had only one adopter last year, but has grown to 8 across all sectors, led by the Social 50 (8% adoption).
- Support of Tag Management/Privacy Solution – New in 2014, this metric tracks whether the site utilizes a tag management system or privacy solution. This element was added to recognize sites that are addressing the complexity and difficulty of managing third-party data collection. Overall, 41.8% of sampled sites have adopted such a solution, indicating that it is quickly becoming recognized as a best practice. The News 50 leads adoption with 88%, followed by the IR 100/500 (62%/44% respectively). The Social 50 lags in adoption at 16%.
- Data Breach & Loss Incidents – 7.1% had a breach incident in the last two years. The FDIC 100 (15%) and Social 50 (18%) had the highest rate. It is recognized there is no absolute security and that breaches and data loss incidents can impact any organization.

[3] http://oag.ca.gov/privacy/business-privacy

SECTOR HIGHLIGHTS

Internet Retailer 500

- Strong growth in email authentication, especially for both SPF and DKIM (IR 100 leads all sectors at 88%). Also strong support of tag management/privacy solutions (44.2%).
- Privacy policies need improvement – resulted in failing scores for more than one-third of the sector.

FDIC 100

- Continues to lead all sectors by far in EV SSL adoption (64%) and AOSSL adoption (78%).
- Highest failure rate across all sectors, caused by lack of email authentication support (especially DKIM at top-level domains), which caused nearly half the sector to fail, and privacy policies, which caused more than one-third of the sector to fail.
- DMARC adoption grew to 21% outpacing Internet Retailers, led by JPMorgan Chase who has led the financial services sectors by being one of the first sites to publish a "reject" or "quarantine" policy.

Social 50

- Top consumer-facing sector for percent of companies making the Honor Roll (50%), OTI average score (80), and DMARC adoption (36%).

Federal Government 50 (not part of Honor Roll calculation due to lack of Privacy scores)

- Lags all sectors in all aspects of email authentication, especially support of DKIM. Also lagging in SSL scores (averaged 70.5 vs. cross-industry average of 83.4).
- Primary adopter of DNSSEC (92%, the next highest sector is 5%), reflecting White House Office of Management and Budget (OMB) directive.
- Of significant concern is that 26% of Fed 50 sites tested received failing SSL grades with one or more vulnerabilities or at risk server mis-configuration(s).

News/Media 50 (new in 2014)

- Lowest Honor Roll achievement (4% vs. overall average of 30%) due to poor email authentication (caused failing scores for 50% of the sector) and low privacy scores (not failing scores, but too low to allow Honor Roll achievement).
- Highest adoption of tag management/privacy solutions (88%), reflecting sites' reliance on funding via third-party advertising. While they also led in publishing Do Not Track disclosure (22%), they realized the lowest privacy score (average of 45.9 vs. cross-industry average of 64.7) as a result of the third party data collection and tracking, indefinite data retention policies and related factors. Of concern are many sites that have logins and collect user profiles without SSL (36% have no SSL support), resulting in private information being transmitted "in the clear."

DOMAIN, BRAND & CONSUMER PROTECTION

By utilizing email authentication (SPF and DKIM), organizations can help protect their brands and 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. Domain locking ensures that domain ownership cannot be transferred without the owner's permission, further helping to protect a site's brand from abuse.

An accompanying report will be issued later this year providing in-depth review and discussion of email authentication. This report will include a deep dive of DMARC, including an analysis of the adoption of reject or quarantine policies. Such policies are recommended best practices to maximize brand and consumer protection by providing receiving networks and ISPs direction to reject email which fails email authentication verification.

Best practices include:

- Implement both SPF and DKIM for top-level domains, "parked" domains (not used for email) and any major subdomains seen on websites or used for email.
- Implement DMARC for all appropriate domains, initially in "monitor" mode to get receiver feedback and verify accuracy of email authentication, and eventually to assert a "reject" or "quarantine" policy to receivers.
- Implement inbound email authentication and DMARC support to protect employees and corporate data from spear phishing exploits.
- Ensure that domains are locked to prevent domain takeovers.

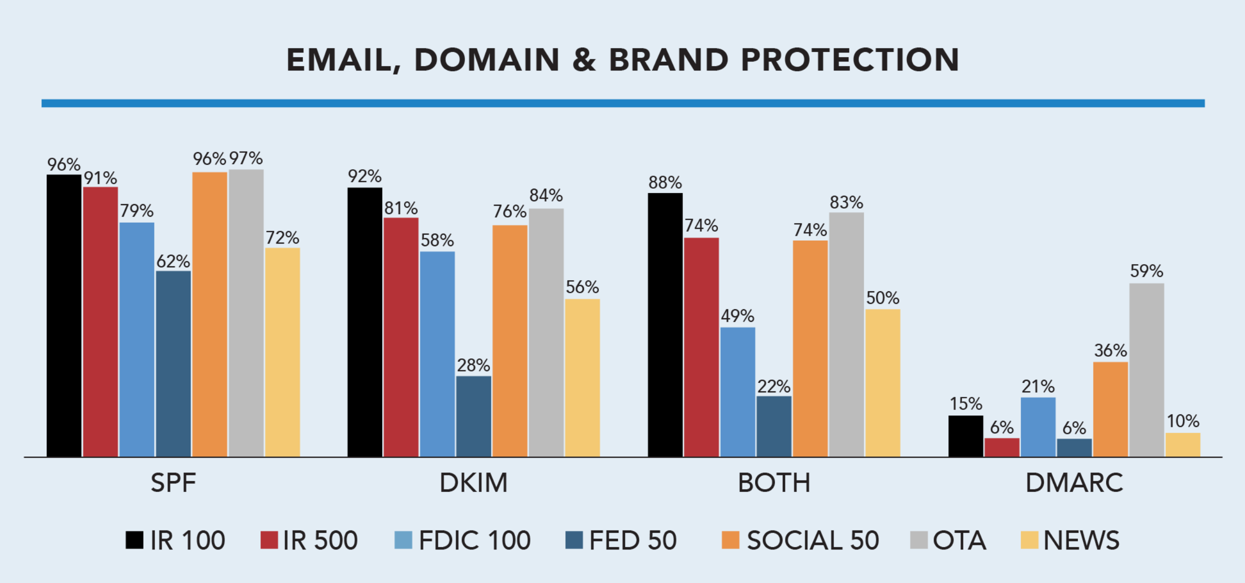

Figure 7 – Email Authentication & DMARC by Sector

EMAIL AUTHENTICATION

Email authentication technologies, namely Sender Policy Framework (SPF) and DomainKeys Identified Mail (DKIM), help prevent phishing and spam. OTA has tracked the progress of email authentication technologies, best practices and adoption since 2005, has offered training and resources to help companies implement best practices and continues to communicate their value to enhance brand and consumer protection. As shown in the summary chart in Figure 7, email authentication adoption varies across sectors, led by Internet retailers, social networks and OTA members, while the federal government sites continue to lag despite training offered through the Department of Homeland Security. This low adoption rate impedes receiving networks and ISPs from accurately detecting and blocking malicious and fraudulent email purporting to come from government agencies. SPF adoption is higher than DKIM adoption by 15-25% across all sectors, primarily due to its ease of implementation, whereas DKIM requires additional configuration and updates to outbound mail servers.

Organizations worldwide have found that adoption of **both** SPF **and** DKIM best enables receivers to detect and block forged and malicious email, while reducing the risk of false positives from mail that is forwarded or sent from mailing lists.

As seen in Figure 8, use of both SPF and DKIM grew in nearly all sectors, most notably in the IR 100 and IR 500. Some of this growth can be attributed to more thorough analysis of sending domains and subdomains in the retail sector. It is evident that online retailers and social platforms, which are most heavily reliant on email interaction with their users/customers, have recognized the brand value of email authentication. Conversely, more efforts are needed at the top level or corporate domains to maximize protection.

2014 DOMAIN & BRAND PROTECTION

BOTH DKIM AND SPF

	2010	2011	2012	2013	2014
IR 100	24.0%	42.0%	56.0%	76.0%	88.0%
IR 500	14.0%	23.0%	43.0%	56.0%	74.0%
FDIC 100	22.0%	23.0%	34.0%	49.0%	49.0%
Fed 50	2.0%	4.0%	10.0%	20.0%	22.0%
Social 50	-	28.0%	63.0%	72.0%	74.0%
OTA Members	36.0%	44.0%	59.0%	69.0%	83.0%
News 50					50.0%

Figure 8 – Adoption of Both SPF and DKIM by Sector, 2010-2014

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

Introduced in early 2012, DMARC creates consistency by leveraging the best of SPF and DKIM; visibility by reporting on how receivers process inbound email; and policy so senders can declare how to process unauthenticated email. As a result, DMARC became a baseline scoring component in 2013 and received increased weighting for the 2014 report.

Figure 9 shows the year-to-year growth in adoption of DMARC. With the exception of the Fed 50, which added only one DMARC-adopting agency, all sectors showed solid growth in adoption, with many sectors showing absolute growth of 10% or more.

DMARC ADOPTION

	2012	2013	2014
IR 100	2.0%	5.0%	15.0%
IR 500	1.5%	3.0%	6.2%
FDIC 100	1.0%	13.0%	21.0%
Fed 50	0.0%	4.0%	6.0%
Social 50	18.5%	22.0%	36.0%
OTA Members	34.3%	43.8%	59.4%
News 50			10.0%

Figure 9 – DMARC Adoption by Sector, 2012-2014

INBOUND ADOPTION OF EMAIL AUTHENTICATION

With the rise in spear phishing and associated attempts to compromise business user passwords and system access (as evidenced in the attack on Target Corporation's HVAC vendor [4]), it is critically important that all organizations – both public and private sector – implement email authentication verification on **inbound** messages to help protect employees and internal systems from attacks.

While the focus of this report is a company's **outbound** adoption of email authentication for brand and consumer protection, the full value is only realized when both the sender and receiver are participating in the process. While the consumer ISP community has overwhelmingly adopted inbound authentication, corporate and governmental agency adoption remains a serious concern.

DOMAIN LOCKING

Analysis of domain locking was added to the report in 2013 due to its importance in prevention of domain takeovers (a penalty is assigned if the domain is not locked). More than 92% of sampled organizations across all sectors lock their domains (led by the IR 100 at 98%), but this means that 35 of the 813 sites evaluated still need to lock their domains to help protect their brand and users.

[4] http://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/

SITE, SERVER & INFRASTRUCTURE SECURITY

A site's trustworthiness is primarily defined by the security of the infrastructure. Users want to know that they are on the right site and that their data transactions are secure. Proper implementation of best practices in this category also protects the site itself from attack.

Best practices in this category can be summarized as follows:

- Optimize SSL implementation using information gleaned from tools such as Qualys SSL Labs, with specific focus on vulnerabilities that earn a letter grade of "F".
- Use EV SSL on sites that are frequently spoofed and for sites where users need to be assured they are at a legitimate site.
- Implement AOSSL on sites where a high degree of sensitive data transfer occurs or users are apt to use public wireless access points.
- Utilize DNSSEC to further protect a site's DNS infrastructure from attack and exploits.
- Proactively scan sites and third-party content for malicious links, iFrame exploits malware and malvertising.[5]

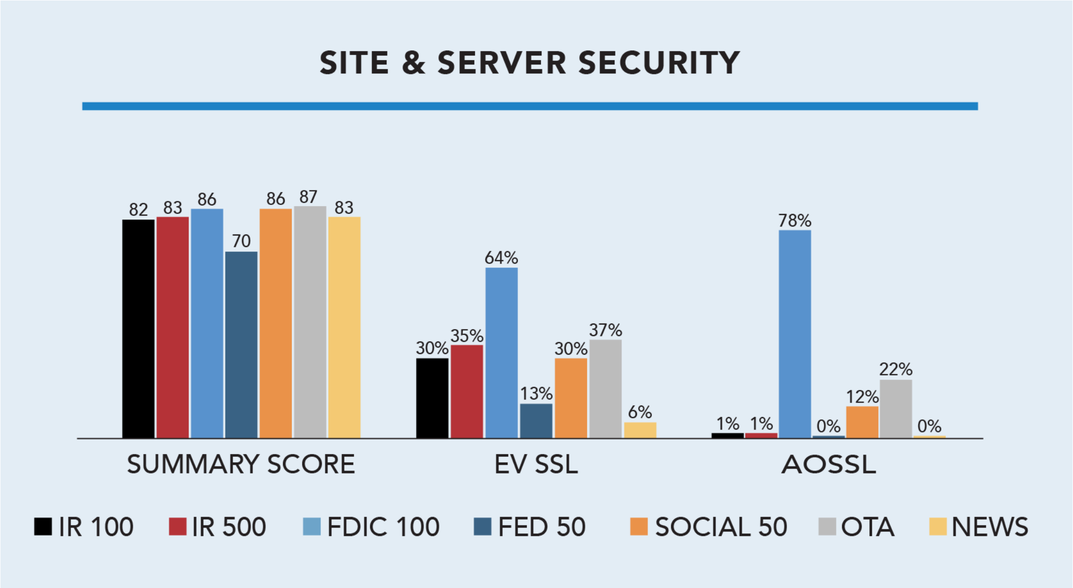

Figure 10 – Site & Server Security Scores/Adoption by Sector

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

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

- SSL scores, which represent the base score in this category, are concentrated around the overall average of 83.4, with the exception of the Fed 50, which trails by 12 points.
- EV SSL adoption varies significantly across sectors – it is highest in the FDIC 100 (64.0%) and lowest in the News 50 (6.1%).
- AOSSL helps ensure that all data exchanged between the site and user is encrypted. Here, too, adoption varies dramatically – from 75% in the FDIC 100 to less than 1% in the IR 500, Fed 50 and News 50.

SSL IMPLEMENTATION & VULNERABILITY ANALYSIS

Proper and ongoing SSL configuration is the primary mechanism sites can use to minimize vulnerabilities. While it is straightforward to obtain and install an SSL or EV SSL certificate, care must be taken to maintain a site properly, with ongoing checks to ensure that the latest protocols and configurations are in use. In a May 2014 report, Qualys SSL Labs found that only 28.4% of the 156,022 sites tested were considered secure.[6]

The SSL scores incorporated data from the Qualys SSL Labs tool, High-Tech Bridge and SiteLock tools as well as tools provided by Symantec and Microsoft. Collectively these tools were used to evaluate sites' SSL implementation, EV SSL adoption, and vulnerability to cross-site scripting, iframe exploits, malware and malicious links.

In addition to incorporating additional data attributes for the 2014 Audit, including testing for HeartBleed vulnerabilities, Qualys upgraded its testing methodology to provide additional granularity. These enhancements allow the 2014 report to better evaluate server configurations against the current threat environment.[7] [8] It is important to recognize that this analysis does not scan for every server attribute or possible combination of vulnerabilities. Secondly, in instances where more than one SSL server was found, the analysis focused on the highest scoring server.

As in previous years, OTA's 2014 analysis found numerous cases of mis-configured servers. Where possible, OTA made efforts to contact the server administrators to help them protect their site from the visible exploits by sending email to the contact address at the respective domains. Several sites were able to reconfigure servers to reduce vulnerabilities, and while notification may have resulted in a favorable impact on a site's scores, OTA felt responsible to notify the sites immediately to help protect the organizations and their customers from harm. Unfortunately more than one-third of these efforts failed, highlighting the need for enhanced sharing of threat intelligence data and ability to engage proper contacts at the respective companies.

Presence of site vulnerabilities including iframes, XSS and malicious links were observed in less than 5% of all sites. This reflects increased diligence of site owners regarding scanning and securing their server configuration. Sites which accept third-party content and advertising are encouraged to hold their ad partners accountable to security best practices.

[6] Source: Qualys 2014 report https://www.trustworthyinternet.org/ssl-pulse/

[7] https://community.qualys.com/blogs/securitylabs/2014/01/21/ssl-labs-stricter-security-requirements-for-2014

[8] http://heartbleed.com

As shown in Figure 11, SSL scores dipped modestly in most sectors due to increased granularity and the more rigorous requirements imposed in the 2014 report. Exceptions were the Social 50 and FDIC 100 which posted modest gains.

Site administrators are encouraged to review the SSL Server Rating Guide[9], updated in January 2014, which provides an overview of the assessment methodology and addresses common configuration issues. A useful companion document is the "SSL/TLS Deployment Best Practices" published by Qualys[10]. OTA's experience with these resources and tools has shown that changes can usually be made quickly and inexpensively once technical decision makers are engaged and issues are identified.

2014 SITE & SERVER SECURITY
SSL IMPLEMENTATION SCORES

	2012	2013	2014
IR 100	75.9	85.3	81.9
IR 500	76.8	85.1	83.3
FDIC 100	75.8	85.0	86.5
Fed 50	67.7	73.2	70.5
Social 50	77.7	82.1	86.2
OTA Members	79.8	87.1	86.8
News 50			83.2

Figure 11 – SSL Site Averages by Sector

EXTENDED VALIDATION SSL CERTIFICATES

Extended Validation SSL Certificates (EV SSL) were introduced in the 2006 report to help address lookalike and phishing sites as well as the issue of fraudulently obtained SSL Certificates. EV SSL requires a thorough verification and audit process that helps prevent deceptive and illicit entities from obtaining a certificate on behalf of a legitimate brand.

EV SSL provides differentiation and recognition for sites by displaying a green identifier as a visual trust indicator in the address bar or browser chrome.

As illustrated in Figure 12, worldwide adoption of EV SSL certificates continues to increase, growing more than 39% to exceed 103,000 deployed certificates.[11] Growth has been attributed to brands' desire to instill consumer trust and increased differentiation, amplified by increased cybercriminal activities and deceptive websites.[12]

[9] https://www.ssllabs.com/downloads/SSL_Server_Rating_Guide_2009e.pdf

[10] https://www.ssllabs.com/downloads/SSL_TLS_Deployment_Best_Practices_1.3.pdf

[11] www.netcraft.com

[12] Note the actual number of certificates issued by Certificate Authorities is greater due to lags in deployment.

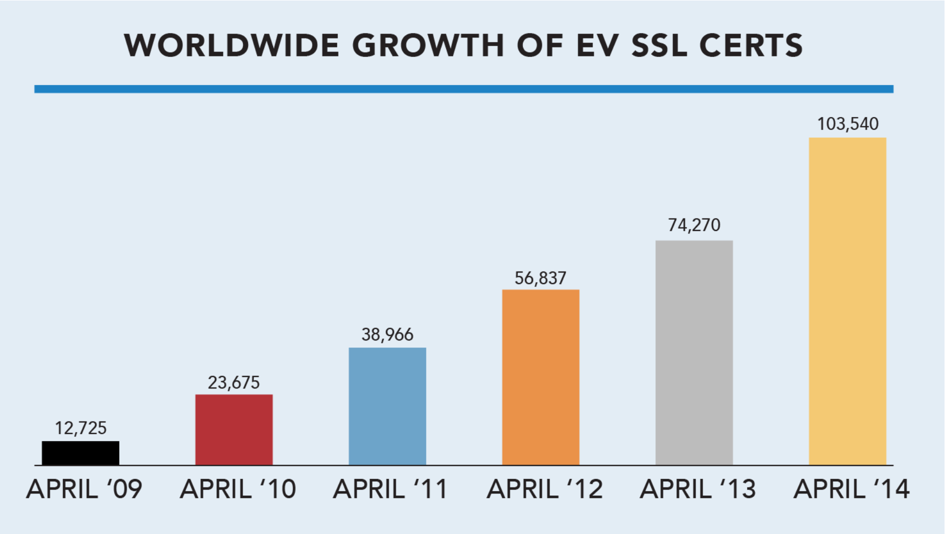

Figure 12 – Worldwide EV SSL Certs, 2009-2014 (Netcraft, 2014)

Figure 13 below shows the year-to-year growth in EV SSL adoption by sector (calculating EV SSL adoption as a percentage of sites with SSL), and most sectors showed modest growth again this year. As in past years, the FDIC 100 leads adoption at 64% (nearly double the next closest sector), which reflects their need to instill consumer trust by differentiating their sites from look-a-like sites used to attack banking customers.

EV SSL CERTIFICATE ADOPTION

	2010	2011	2012	2013	2014
IR 100	18.0%	27.3%	27.2%	28.0%	30.0%
IR 500	26.1%	29.8%	30.7%	33.4%	35.0%
FDIC 100	25.6%	45.6%	55.0%	60.0%	64.0%
Fed 50	11.4%	22.2%	25.9%	15.2%	12.5%
Social 50	-	12.0%	29.6%	24.5%	30.2%
OTA Members	32.5%	35.3%	43.4%	35.0%	36.7%
News 50					6.1%

Figure 13 - EV SSL Certificate Adoption by Sector, 2010-2014

DOMAIN NAME SYSTEM SECURITY EXTENSION (DNSSEC)

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

DNSSEC adoption grew modestly this year, with only the Federal 50 having significant adoption (92% this year vs. 88% last year). The only other sectors with any DNSSEC adoption are OTA members (4.7%) and the News 50 (2%). Broad implementation of DNSSEC continues to be hampered by lack of ecosystem infrastructure (hosting environments, registrars and browsers) as well as competition from higher priority security issues.

DATA PROTECTION, PRIVACY & TRANSPARENCY

As businesses throughout the world are becoming "data driven"marketers, increasingly collecting and appending data through data brokers and collection methods across devices, it is more important than ever for organizations to strike the balance between data collection privacy and data stewardship. OTA has been advocating for increased transparency and discoverability of privacy policies since 2009, including recommending that policies provide clear disclosure of data collection, data usage, sharing and retention practices.

Best practices are summarized as follows:

- Publish discoverable, easy to find, and comprehensible privacy policies.
- Create a layered, concise summary linking to an expanded policy. Provide a clear detailed statement regarding whether personal data is being shared with third parties, what data is being shared and why it is being collected. See OTA short form, linking to the full policy http://otalliance.org/privacy-policy.
- Write policies for the site's target audience and demographics. Consider providing bi-lingual versions representing the diversity of non-English speaking site visitors. See Spanish version of OTA's privacy policy – https://otalliance.org/politica-de-privacida.
- Share details of data retention policies including clarification if such data is retained after the online interaction is terminated.
- Make best efforts to provide notice to consumers if their data is requested by third parties due to legal requirements. Suggested draft copy includes the statement "To the extent we are legally permitted to do so, we will take reasonable steps to notify you in the event that we are required to provide your personal information to third parties as part of legal process." [13]
- Utilize tag management systems or privacy solutions that can manage third-party trackers and ensure they are acting properly.

[13] Sites should conduct a legal review to ensure this draft copy is applicable to their business models and regulatory requirements.

- Disclose whether the site honors Do Not Track (DNT) settings in the site's privacy policy, and preferably honor users' DNT browser settings. While such disclosure is now required for sites with users who reside in California, due to the recent passage of the regulation, this requirement was classified as bonus points for this year's Honor Roll. In subsequent years DNT disclosure is expected to be part of the base privacy score.

  Suggested disclosure draft copy as implemented by OTA;

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

As itemized in the Methodology and Scoring section, several criteria were added as bonus opportunities this year, including the use of layered privacy policies, disclosure of a site's DNT policy, and use of tag management or privacy solutions. These emerging best practices add to the analysis of privacy policies, site tracking, public vs. private WHOIS registrations, honoring of DNT and data loss incidents or FTC privacy-related settlements/judgments evaluated in the 2013 report. By looking comprehensively across these criteria, it is possible to get a complete view of a company's commitment to privacy and their respective business practices.

Figure 14 shows the average scores and adoption of various criteria which varied widely across sectors.

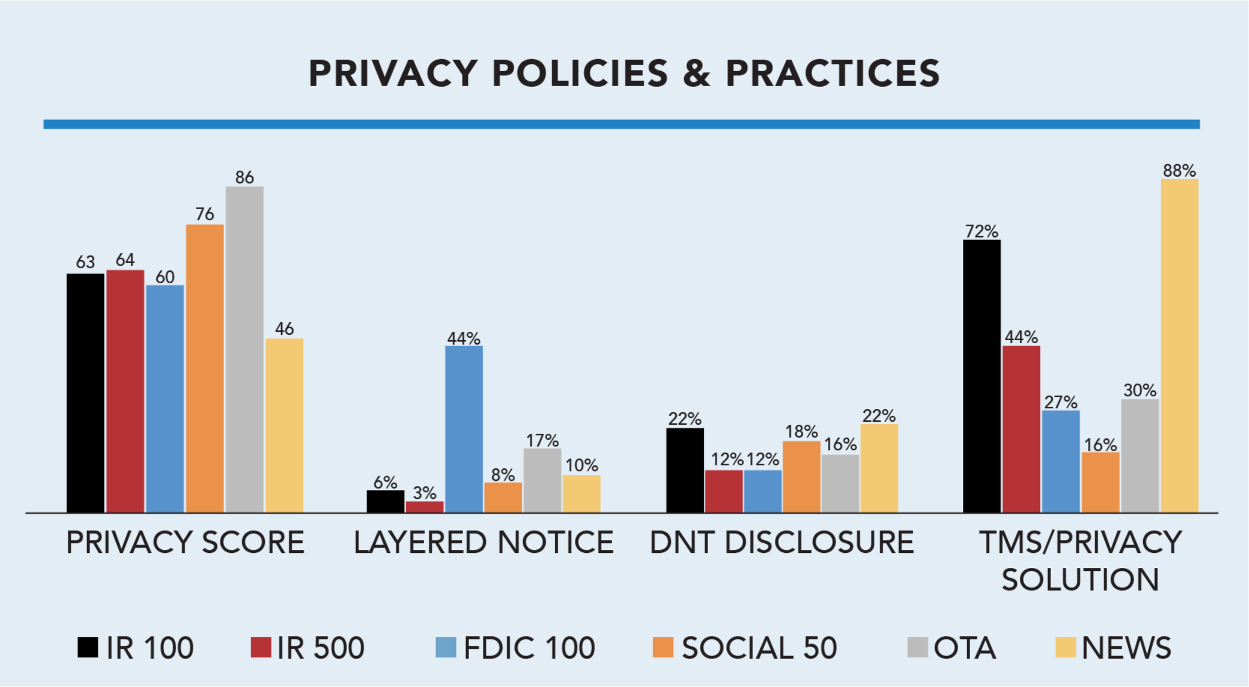

Figure 14 – Privacy Policies and Practices by Sector

PRIVACY POLICIES & THIRD PARTY TRACKING

Privacyscore, a service of AVG Technologies, along with data from TRUSTe and OTA analytics were used to analyze sites' privacy practices. Sites were scored on a scale of 100 points, with 50 points possible for evaluation of the site's privacy policy, and 50 points possible based on the privacy qualifications of third-party trackers seen on the site.[14] OTA staff augmented this tool with its own evaluation across all sectors. It should be noted that sites may have add-ons or apps which collect and share data that may not have been detected in this analysis.

Privacy scores averaged 64.7 across all sectors (vs. 66.5 last year), with the year-to-year dip largely due to the newly added News 50 sector, which had an average score of only 45.9. Scores ranged from OTA members at 86.2 to the News 50 at 45.9. Overall, privacy scores caused more than a third of companies in the IR 500 and FDIC 100 to receive failing scores, indicating the need for significant improvement. Privacyscore and other related third party tools can provide valuable insight into changes that will improve sites' practices.

LAYERED NOTICE

New for 2014, sites' privacy policies were analyzed by OTA tools and staff to determine whether they had implemented a layered privacy notice. Disappointingly, only 10.5% of sites overall offered layered notice, with the FDIC 100 out-pacing all segments more than 2:1 with 44% adoption, followed by OTA members at 17.2%. All other sectors were at 10% or less, indicating there is much room for improvement in this area.

DO NOT TRACK DISCLOSURE

As Do Not Track (DNT) becomes a legal requirement in some jurisdictions and issues regarding implementation are resolved, it becomes increasingly important for sites to both disclose their DNT policy as part of their privacy policy and to honor the browser's DNT setting as users visit the site.

Overall, 13.1% of sites disclosed their DNT policy, led by the News 50 at 22%, with all other sectors in the 12-16% range. As this requirement is now mandated by the State of California for all sites with users who reside in the State, the low adoption reflects a significant compliance concern. By contrast, only 1% of sites overall actually honor the DNT setting, ranging from the Social 50 (8%) to the Internet Retailer 500 and FDIC 100 (0%).

[14] Privacyscore methodology http://www.privacyscore.com/faq

TAG MANAGEMENT SYSTEMS OR PRIVACY SOLUTIONS

Sites which rely on advertising and third-party analytics are faced with a complex and dynamic challenge of managing third-party tracking, which can create conflict with the stated privacy policy and regulatory compliance. Tag management and privacy solutions are becoming a best practice to allow review and monitoring of data collection and sharing in real time. OTA utilized site scanning capabilities to detect such systems and awarded bonus points if they were present.[15] [16]

Analysis revealed such solutions are already a well-adopted practice, with 41.8% of sites overall utilizing these systems. The News 50 led all sectors with 88%, followed by the IR 100/500 (62% and 44.2% respectively). The Social 50 had lowest adoption (16%), possibly due to the fact that they have less third-party activity on their sites.

WHOIS REGISTRATIONS

WHOIS registrations are overwhelmingly public, with all sectors at 95% or higher and an overall average of 96%. Still, 32 organizations (nearly all in the IR 500) have private registrations, which limits transparency.

DATA BREACH INCIDENTS & FTC SETTLEMENTS

Though even organizations with strong practices are not immune to compromise, data breaches and FTC settlements can be indicative of poor data stewardship and privacy practices, impacting a site's brand reputation and trustworthiness. Sites with such incidents or settlements receive a penalty impacting their overall composite score.

Data breach incidents occurred in 58 (7.1%) of the organizations evaluated and impacted all sectors. The News 50 had the lowest rate (2%) of breaches, followed by the IR 500 (4.4%). The highest rate of breaches was in the Social 50 (18%). FTC suits or settlements disclosed by the FTC alone did not prevent any site from qualifying for the Honor Roll, though based on rankings it did prevent one site from qualifying for the Internet Retailer Top 10.

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

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

CONCLUSION

The security and privacy landscape continues to evolve as new and innovative data driven services are being introduced while data breaches and privacy missteps are becoming a common occurrence. As mobile devices and systems become more interconnected, our critical infrastructure, computers, mobile devices and applications are increasingly at risk.

These highly public failures and vulnerabilities have a negative impact on consumer trust. Left unchecked and without a commitment to meaningful self-regulation and enforceable codes of conduct, the reputation of brands and the health of the Internet itself is at risk. As the world economy and society at-large become increasingly reliant on the Internet, it is incumbent on the business community and associated trade organizations to embrace these practices and move from a compliance mindset to one of stewardship.

The OTA Online Trust Audit and Honor Roll works to highlight best practices and identify those companies which have demonstrated a commitment to consumer safety, security and privacy. Companies that earned Honor Roll status are to be commended and serve as a North Star for others to aspire to.

Adoption of the outlined best practices serves as the foundation of meaningful self-regulation. Companies who adopt these and other security controls should be afforded protection from onerous regulatory oversight and receive "safe harbor" from frivolous lawsuits. In the absence of such commitment to consumer protection, Congress is increasing its demand that industry be accountable.[17]

The 2014 report confirms a renewed commitment to stewardship and adoption of best practices. This report serves four primary objectives:

- Recognize leadership and commitment to best practices which aid in the protection of online trust and confidence in online services.
- Promote best practices and provide tools and resources to aid companies in enhancing their security, data protection and privacy practices.
- Raise awareness of the risks, helping businesses to improve their security and privacy practices.
- Aid consumers in making informed decisions about the security and privacy practices of sites they frequent.

To maximize consumer protection, no single company or constituency can work alone. Only with the collaboration of industry, business, NGOs and government stakeholders can we achieve a "trusted Internet" and assure the vitality of online services.

Updates to the report with additional data are posted at https://otalliance.org/HonorRoll. To submit comments or suggestions, email editor @ otalliance.org.

[17] U.S. Senate Hearing Online Advertising & Hidden Hazards to Consumer Security & Data Privacy http://www.hsgac.senate.gov/hearings/online-advertising-and-hidden-hazards-to-consumer-security-and-data-privacy

ACKNOWLEDGEMENTS

Data and analysis has been provided in part by: Agari, AVG Technologies, Bounce.IO, comScore, DigiCert, Ensighten, GlobalSign, High-Tech Bridge SA, IID, InfoTrust, Microsoft, Qualys, Return Path, SiteLock, SSL Labs, Symantec and TRUSTe. Special thanks to OTA members and staff for their strategic input including: David Ader, Tom Bartel, Mark Goldstein, Mike Hammer, Mike Jones, Lauren Millslagle, Ivan Ristic, Liz Shambaugh, Craig Spiezle, Joe St. Sauver, Jeff Wilbur and Ben Wilson.

ABOUT ONLINE TRUST ALLIANCE (OTA)

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

OTA supports collaborative public-private partnerships, benchmark reporting, and meaningful self-regulation and data stewardship. Its members and supporters include leaders spanning public policy, technology, e-commerce, social networking, mobile, email and interactive marketing, financial, service provider, government agency and industry organization sectors.

OTA is a 501(c)(3) tax exempt global non-profit focused on enhancing online trust with a view of the entire ecosystem. OTA is supported by donations and support across multiple industries, representing the private and public sectors. To support OTA visit https://otalliance.org/donate.

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

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

APPENDIX A – 2014 HONOR ROLL RECIPIENTS

2014 Internet Retailer Top 500 - Honor Roll

- AJ Madison Inc.
- ★★ Alibris Inc.
- Allied Electronics
- AMainHobbies.com
- ★★ Amazon.com Inc.
- American Apparel Inc.
- ★★ **American Greetings Corp.**
- ★★ **Ancestry.com Inc.**
- ★★ Apple Inc.
- ★★ Art.com Inc.
- Bare Escentuals Inc.
- ★ Bellacor Inc.
- ★ Best Buy Co. Inc.
- ★ Beyond the Rack
- ★ Bidz.com Inc.
- ★★ **Big Fish Inc.**
- ★★ BikeBandit.com
- ★★ **Books-A-Million Inc.**
- ★ Build.com Inc.
- ★ BuildASign.com
- ★★ Cabela's Inc.
- ★★ CafePress.com
- Calendars.com LLC
- ★ Camping World Inc.
- Cheaper Than Dirt
- **Christianbook.com LLC**
- Coastal Contacts Inc.
- CPA2Biz Inc.
- ★★ Crate and Barrel
- ★★ CustomInk
- Dillard's Inc.
- ★ Discount Ramps.com LLC
- ★ Disney Store USA LLC
- DoMyOwnPestControl.com
- Eastern Mountain Sports Inc.
- ★ Etsy Inc.
- ★ evo
- Express Inc.
- Fab.com
- ★★ Fathead LLC
- Frys.com
- ★ Gaiam Inc.
- ★ GameFly Inc.
- ★★ GameStop Corp.
- ★★ Garmin Ltd.
- ★ Groupon Goods
- ★★ Gymboree Corp., The
- ★★ Hayneedle Inc.
- ★ HP Home & Home Office Store
- ★★ HSN Inc.
- ★ Hulu LLC
- ★ Ice.com Inc.
- ID Wholesaler
- Interline Brands Inc.
- ★ **JackThreads.com**
- Jewelry Television
- ★ Karmaloop.com
- ★★ Kohl's Corp.
- ★★ Lakeshore Learning
- ★ Lakeside Collection
- LeapFrog Enterprises Inc.
- ★ LeatherUp.com
- ★ LEGO Brand Retail Inc.
- ★ Levenger Co.
- ★ Liberty Interactive Corp.
- ★ LivingSocial Inc.
- ★ Lowe's Cos. Inc.
- ★★ Microsoft Corp.
- ★ Minted.com
- ★★ ModCloth Inc.
- Mountain Equipment Co-op
- Nebraska Furniture Mart
- ★★ Net-a-Porter Group LLC
- ★★ **Netflix Inc.**
- ★ New Balance
- **Newegg Inc.**
- Nike Inc.
- ★ NoMoreRack.com Inc.
- Nordstrom Inc.
- OneCall.com
- ★ Onlineshoes.com
- Oriental Trading Co. Inc.
- OvernightPrints.com
- ★★ Overstock.com Inc.
- ★ Pacific Sunwear of California
- ★★ Payless ShoeSource Inc.
- ★★ PersonalizationMall.com
- ★★ Powell's Books Inc.
- PromGirl LLC
- ★ Ralph Lauren Media LLC
- ★ Replacements Ltd.
- ★ RockAuto LLC
- ★ Sephora USA Inc.
- ★ Sheplers Inc.
- Shopping Channel
- Signet Jewelers Ltd.
- Silver Star Brands
- SmoothFitness.com
- ★★ Sonic Electronix
- ★ **Sony Electronics Inc.**
- SparkFun Electronics
- Spreadshirt Inc.
- Sweetwater
- ★ SwimOutlet.com
- Systemax Inc.
- ★★ ThinkGeek Inc.
- ★ Threadless.com
- ★★ Tiffany & Co.
- ★ Tory Burch LLC
- Tumi Inc.
- Under Armour Inc.
- Vintage Tub & Bath
- ★★ Vitacost.com Inc.
- ★★ **Walmart.com**
- ★ Wayfair LLC
- ★ Weight Watchers
- Wet Seal Inc.
- ★ Yankee Candle Co. Inc.
- ★ **zulily Inc.**

★ = Honor Roll 2013 ★★ = Honor Roll 2012 & 2013

Bold = Top 10 Internet Retailer 500 (Includes 11 sites due to scoring ties.)

2014 FDIC Top 100 Banks - Honor Roll

- ★★ American Express Bank, FSB.
- ★★ American Express Centurion Bank
- Arvest Bank
- ★★ Bank of America California, National Association
- ★★ Bank of America, National Association
- Bank of the West
- ★★ BMO Harris Bank National Association
- Branch Banking and Trust Company
- ★★ Charles Schwab Bank
- ★ Citibank, National Association
- Citizens Bank of Pennsylvania
- City National Bank
- ★ E*TRADE Bank
- EverBank
- ★ FIA Card Services, National Association
- Fifth Third Bank
- FirstBank
- ★★ Frost Bank
- JPMorgan Chase Bank, National Association
- KeyBank National Association
- ★ Morgan Stanley Bank, National Association
- ★ Morgan Stanley Private Bank, National Association
- RBS Citizens, National Association
- Regions Bank
- ★★ Scottrade Bank
- ★ SunTrust Bank
- ★★ U.S. Bank National Association
- ★ UBS Bank USA
- ★★ USAA Federal Savings Bank
- ★ USAA Savings Bank
- ★★ Wells Fargo Bank Northwest, National Association
- ★★ Wells Fargo Bank South Central, National Association
- ★★ Wells Fargo Bank, National Association

2014 Social Top 50 - Honor Roll

- ★ AOL
- ★★ Badoo.com
- ★ Blogger
- Box
- ★★ DeviantArt
- Dropbox
- ★ eHarmony
- ★★ Facebook
- ★ FiveRR
- ★ Foursquare
- ★ Goodreads
- iCloud
- ★ ImageShack
- ★ Instagram
- ★★ LinkedIn
- MeetMe
- MySpace
- ★ Pinterest
- ★ PlentyofFish
- ★★ Tumblr
- ★★ **Twitter**
- ★ Wordpress
- Yahoo!
- ★ YouTube
- ★★ Zynga

★= Honor Roll 2013 ★★= Honor Roll 2012 & 2013

Bold = Top score across all sites/sectors.

2014 News/Media Top 50 - Honor Roll

- Google News
- New York Times

2014 OTA Members - Honor Roll

- ACT
- ★ Act-On Software
- ★★ American Greetings Interactive
- ★★ Agari
- AVG
- ★ BounceIO
- Coles
- ★ comScore
- ★★ Constant Contact
- ★★ deviantART
- ★★ DigiCert
- Distil Networks
- ★ eBay Enterprise (formerly e-Dialog)
- ★★ eHarmony
- ★★ Ensighten
- ★★ Epsilon
- ★ eWayDirect
- ★★ Exact Target
- flybuys
- ★★ GetResponse
- ★★ Global Sign
- ★★ GoDaddy
- ★★ Harland Clarke Digital
- ★★ High-Tech Bridge SA
- ★★ Iconix
- ★★ Identity Guard
- ★★ Innovyx
- ★ Interent Identity (IID)
- ★★ Intersections
- LashBack
- ★ Listrak
- ★★ Mark Monitor
- ★★ Marketo
- MeetMe
- ★ Message Systems
- ★★ Microsoft
- ★★ NSS Labs
- ★★ Online Trust Alliance
- Optizmo
- ★★ PayPal
- ★★ Privacy Score
- ★★ Publishers Clearing House
- ★ PWC
- ★★ Return Path
- ★ RiskIQ
- ★★ Sailthru
- ★★ Silverpop
- ★ SiteLock
- ★★ Symantec
- The Media Trust
- ★★ TRUSTe
- ★★ TrustSphere
- ★★ Twitter
- ★ VERISIGN
- ★ VivaKi
- WebMD
- ★★ ZEDO
- ★★ Zynga

OTA members evaluated were limited to private sector companies, not inclusive of NGOs, government agencies or individual professional members.

★= Honor Roll 2013 ★★= Honor Roll 2012 & 2013