ONLINE TRUST AUDIT

2016
Presidential Candidates

Analysis of the adoption of best practices in:

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

OTA
Online Trust Alliance

Released September 18, 2015

TABLE OF CONTENT

PREFACE

The Online Trust Alliance is a 501c3 non-profit organization with the mission to enhance online trust, promoting security, privacy and identity protection best practices. Through the development of best practices and vendor neutral prescriptive guidance OTA works to educate the public and private sectors to help enhance the security and integrity of their data and adopt responsible data privacy practices.

The information and results included in the report is neither an endorsement nor condemnation of any candidate's website and serves solely to help educate voters and candidates of the data security, privacy and consumer protection status of the audited websites.

It is important to note this audit is limited to an analysis of the candidate's websites and posted privacy policy. Outside the scope of the audit are any side data sharing agreements which a candidate may have with other organizations, including their respective national political parties. If such agreements were to exist and conflicted with the candidate's published privacy policy, it would raise several policy and legal issues forcing the candidate to automatically fail the audit. If this were to occur with existing commercial websites it would likely constitute a violation of the Section 5 of the FTC Act and various State consumer protection statutes, [1]

As with making donations to any cause or organization or sign up for any online service, consumers are encouraged to evaluate the website to see if a site's published practices are consistent with their individual expectations regarding the collection, use and sharing of their data. As outlined in this report, the published privacy policies vary significantly, from disallowing any such sharing to broad language enabling candidates to effectively sell or share donors personal information with any third party.

The 2016 Presidential Candidates Website Audit complements the June 2015 Online Trust Audit and Honor Roll report, evaluating nearly 1,000 web sites.[2] The report examined the top online retailers, banks, social/sharing sites, news/media sites, Internet of Things (IoT) companies and consumer-facing federal government sites.

OTA has conducted the Online Trust Audit for seven years, now recognized as a benchmark audit of businesses' and government's commitment to security, privacy and consumer protection best practices. Each year OTA publishes an Honor Roll showing the top results of the Audit. As the cyber threat increases and privacy concerns heighten, the relevancy and timeliness of this report is significant, underscoring the imperative that data security, protection and privacy need to be integrated into every service, business process, web site and mobile application.

Criteria for the Audit are updated annually through a multi-stakeholder process and public call for comments, reflecting input from leading trade organizations, consumer advocates and leaders in the private and public sector. This process ensures that Audit criteria reflect the latest standards and best practices to enhance and maximize consumer protection, site security and privacy.

[1] http://www.federalreserve.gov/boarddocs/supmanual/cch/ftca.pdf

[2] https://otalliance.org/HonorRoll

OVERVIEW & BACKGROUND

2016 PRESIDENTIAL CANDIDATE SITES AUDIT

Today, high-profile breaches in both the public and private sector, including the Internal Revenue Service, the Office of Personnel Management (OPM) and the Pentagon, have increased sensitivity to security and received sharp criticism by the public, Democrats and Republicans on Capitol Hill. In response, OTA initiated this evaluation of the 2016 presidential candidates' websites utilizing the same criteria as the 2015 Online Trust Audit to examine the sites' security, consumer protection and privacy practices (independent of any carve outs provided for political candidates in State and Federal legislation).

The list of sites audited was selected according to the top twenty-three presidential candidates listed on Ballotpedia.org which as of September 14, 2015 included six Democrat candidates, sixteen Republican candidates and one Green Party candidate.[3] Candidates' sites were examined by signing up for email, making donations and using external analysis publically available tools and data provided by more than a dozen technology, security and privacy data sources. Analysis was conducted anonymously without the participation of the sites being analyzed, and it should be recognized that the results reflect a snapshot in time and practices and policies may change in the future or since the analysis was completed. As it is anticipated additional candidates might enter the race over the next few weeks, the report will be updated within the next sixty days. Updates will be posted at https://otalliance.org/2016candidates

OBJECTIVES

This report serves four primary objectives:

- Promote best practices and provide tools and resources to assist the public and private sectors to help enhance their security, data protection and privacy practices.
- Recognize leadership and commitment to best practices which aid in the protection of online trust and confidence in online services.
- Offer assistance to candidates to help improve the consumer protection, security and privacy practices of their respective websites.
- Assist consumers in making informed decisions about the security and privacy practices of sites they frequent.

[3] http://ballotpedia.org/Presidential_candidates,_2016

PRESIDENTIAL CANDIDATE SITES AUDIT HIGHLIGHTS

OTA believes a strong commitment to data stewardship and meaningful self-regulation will benefit organizations in all sectors. We have been impressed with the increased engagement over the years of many types of organizations, along with public support from hundreds of entities, ranging from consumer-facing sites to technology providers. This Audit examines three main categories:

- Privacy – data sharing, retention, notice and third-party restriction policies in the privacy policy, as well as analysis of third-party tracking on the site
- Site Security – server security, use of encryption for web sessions, protections such as firewalls and potential site vulnerabilities
- Consumer Protection – protection of email via authentication and encryption between servers, and protection of domains from hijacking

Each category is worth 100 baseline points, bonus points are available for emerging best practices, and to qualify for the Honor Roll, candidates must achieve a combined score of 80% or higher, yet not fail (score less than 55) in any single category. The detailed methodology and criteria are in Appendix A.

The results of the 2016 Presidential Candidate Sites Audit are shown in Figure 1 below – disappointingly, only 26% (six) of candidates' sites made the Honor Roll (overall achievement of 80% or higher) while 74% failed. There was no middle ground, all sites either made the Honor Roll or received a failing grade.

2016 PRESIDENTIAL CANDIDATE SITES AUDIT RESULTS

Honor Roll	Failed
Jeb Bush (R)	Ben Carson (R)
Lincoln Chafee (D)	Hillary Clinton (D)
Chris Christie (R)	Ted Cruz (R)
Martin O'Malley (D)	Carly Fiorina (R)
Rick Santorum (R)	Jim Gilmore (R)
Scott Walker (R)	Lindsey Graham (R)
	Mike Huckabee (R)
	Bobby Jindal (R)
	John Kasich (R)
	Lawrence Lessig (D)
	George Pataki (R)
	Rand Paul (R)
	Marco Rubio (R)
	Bernie Sanders (D)
	Jill Stein (G)
	Donald Trump (R)
	Jim Webb (D)

Figure 1 – 2016 Presidential Candidate Sites Audit Results

COMPARISON OF CANDIDATE SITES TO OTHER SECTORS

OTA finds the 26% Honor Roll achievement for candidate sites disappointing and it is lower than all but two other sectors audited by OTA in the June 2015 study, as shown in Figure 2 below (the average achievement across other sectors was 44%). The failure rate of 74% is on the high end as shown in Figure 3 (the overall failure rate across other sectors was 46%).

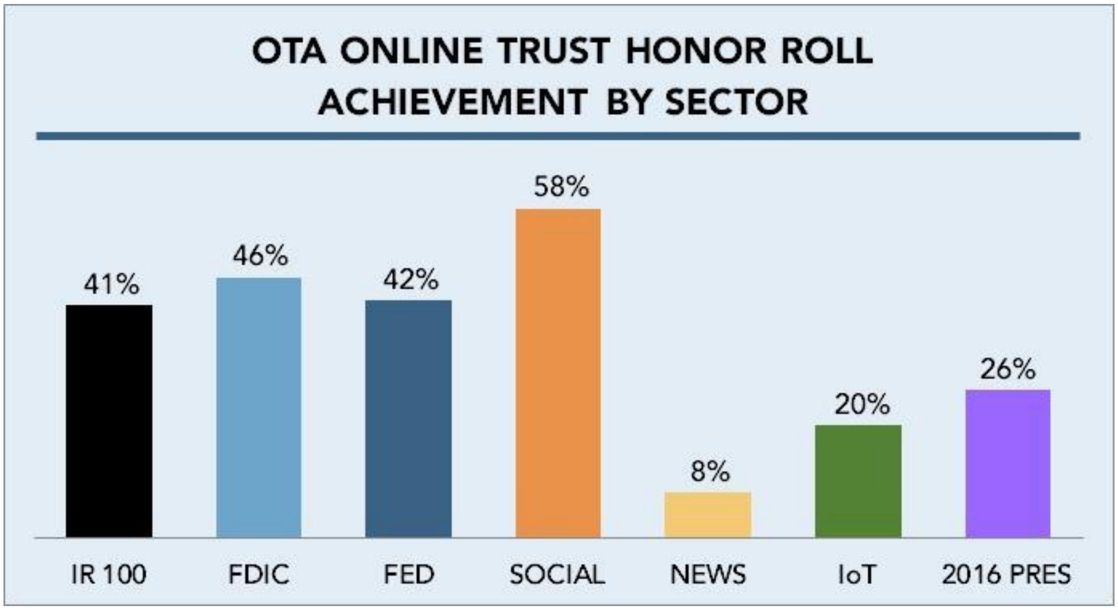

Figure 2 – Honor Roll Achievement by Sector

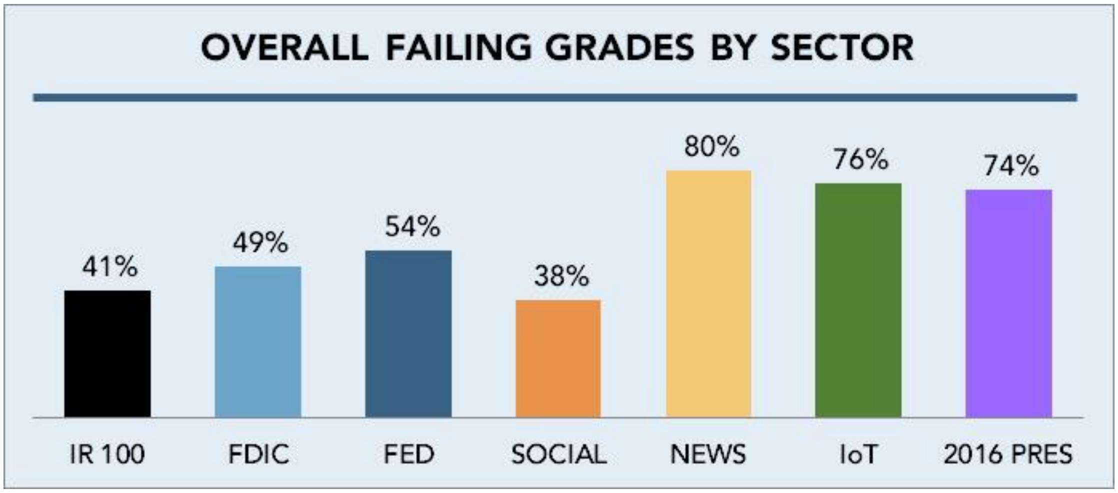

Figure 3 – Percent of Organizations with Failing Grade by Sector

Given the fact that the infrastructure for candidates' websites and email infrastructure is very new and streamlined for their limited purposes (versus e-commerce and banking sites), the adoption of security and privacy best practices should be relatively straightforward. One would expect scores to be quite high across all categories for candidates' sites – so why such a high failure rate?

FAILURE RATES

To answer this question, it is useful to look further inside the data. Figure 4 shows failure rates within each of the three main categories audited. While candidate sites performed well in terms of Site Security and Consumer Protection (no failures in either), the findings for Privacy are distressing. The failure rate of 74% in the Privacy category was the highest of all sectors OTA audits. This high rate of Privacy failure was the leading cause of overall failure for candidate sites which did not achieve Honor Roll status.

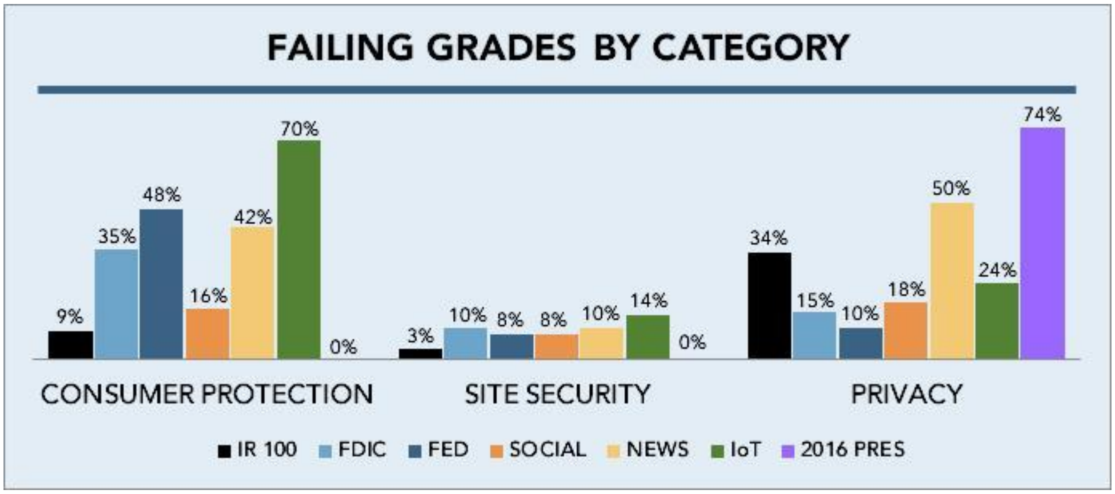

Figure 4 – Percent of Companies with Failing Grade by Sector and Category

AVERAGE BASELINE SCORES

Figure 5 below shows the average baseline score (out of 100) in each main category by sector. As expected, the 2016 candidate sites outpace other sectors in the Consumer Protection and Site Security categories, primarily due to their new and straightforward server infrastructures. But the data reveals Privacy is a serious issue with an average privacy score of 58. By contrast, the average score was 73 across all other sectors sampled. While the News/Media sector average score was lower at 50, unlike the candidate sites this is not due to their privacy policy but driven by use of multiple third-party ad trackers that freely share data with ad networks, data brokers and other unaffiliated third parties.

While none of the candidate sites appear to rely on third-party advertising and associated data collection by ad networks, a score of only 58 is alarming primarily due to the sharing and selling of personal data with unaffiliated third parties.

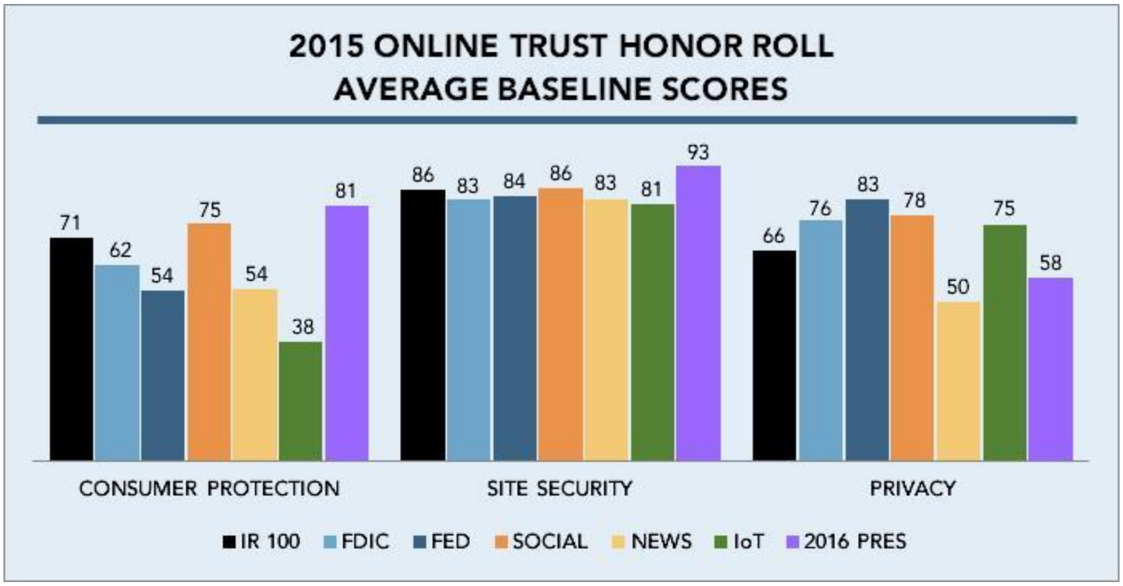

Figure 5 – Major Category Scores by Sector

Privacy and respect for the personal and sensitive information of supporters, donors and volunteers is a significant problem for nearly three-fourths of the candidate sites (the 74% which failed). A detailed analysis with recommended privacy best practices is discussed in the "Data Protection, Privacy & Transparency" section, and highlights are presented here.

PRIVACY PRACTICES

The 100-point baseline score for privacy is divided equally into 50 points for the content of the *privacy policy* (data sharing, data retention, notice of data sharing and binding of third-party vendors' use of data) and 50 points for *third-party tracking* on the site (fewer trackers is better, and points are deducted for third-parties with loose data sharing practices). The average candidate site score for the privacy policy portion was 10 out of 50, by far the lowest of all sectors audited, and the primary driver of failures. The average candidate site score for third-party tracking was 47 out of 50, among the top scores. What caused the low privacy policy scores? The answers varied:

- Lack of Privacy Policy – Four sites had no discoverable policy. This scores a 0 and is an automatic failure. This may be an oversight, but is inexcusable. Fortunately it can be remedied quickly, leveraging related policies of candidate sites which made the Honor Roll.
- Inadequate Policy – Several candidate sites were silent on the issue of data sharing, retention, etc. so did not give clear notice of their policy. Such disclosures are generally accepted practices.
- Promiscuous Policy – Several sites claimed the right to share data with "like-minded entities" or unidentified third parties or anyone, or even to sell the data.

Overall, fifteen sites scored a 0 (four of the fifteen due to no discoverable policy), two had very low scores (mainly due to not addressing shared data or sharing it too broadly), and six had adequate scores (all six made the Honor Roll). These failures were so severe that eight of the twenty-three candidate sites had enough points to qualify for the Honor Roll (despite their lower privacy scores) but were disqualified due to a failing grade for their poor privacy policies. While securing consumer data is important, the very nature of sharing such personal data with any third parties deemed like-minded is in contrast to generally accepted Fair Information Practice Principles (FIPPS).[4]

One other issue was noted in the area of privacy and transparency – nearly half (44%) of sites used a private registration for their domain (discoverable via a WHOIS lookup).[5] In these days of heightened sensitivity to government transparency, OTA encourages candidates to fully disclose who owns these domains. It is understandable that the domains may have originally been registered privately (before the campaign was launched), but this needs to be changed now that the sites are public. It is not uncommon for criminals to set up sites using lookalike domains, so this is an extra step candidates can take to ensure transparency and increase trust.

In general, candidate sites' privacy scores can be significantly improved by implementing a policy (if absent), stating their data sharing practices (if silent), and restricting sharing of the data to only third parties necessary for the operation of their site and services (and requiring those third parties to hold all information as confidential). Key excerpts from all candidate sites' policies are shown in Appendix C, with links to each site's privacy policy.

[4] https://en.wikipedia.org/wiki/FTC_Fair_Information_Practice

[5] The Who Is database can be accessed from multiple domain tools and domain registers. https://who.godaddy.com/

SITE SECURITY AND CONSUMER PROTECTION FINDINGS

Following are the key findings from the other scoring categories:

- Site Security – This category scores the use of server security, data encryption for website sessions as well as other site protections and discovery of known site vulnerabilities. Overall scores were excellent (highest of all sectors). The adoption of Always On SSL, which fully encrypts all traffic between the client devices and the server, thereby maximizing protection from snooping by fraudulent businesses, criminals as well as the NSA, was high (70% – only banks were higher).

  The missed opportunity here is use of Extended Validation (EV) SSL certificates, which helps website visitors know they're on the right site via a trust indicator, green browser bar, thus distinguishing them from fraudulent web sites. Only one site has adopted EV SSL, yielding an adoption rate of 4%, which is far below other sectors (21% for Social, 24% for online retailers and 67% for banks). Since citizens are providing personal information and donating on these sites, OTA would expect an EV SSL adoption rate closer to that of the banks. This need is heightened due to the fact that OTA has observed several lookalike sites and domain registrations. Adoption of EVSSL is a simple and cost-effective solution to enhance trust and protect both consumers and the candidate's brand. OTA encourages all candidates to implement it immediately.

- Consumer Protection – This category scores the adoption of email authentication and associated technologies to help protect consumers from receiving fraudulent email purporting to come from candidates, their PACs or political parties. These protocols include Sender Policy Framework (SPF) and DomainKeys Identified Mail (DKIM), which allow recipients to verify the sender. In addition, Domain-Based Authentication, Reporting and Conformance (DMARC) allows senders to receive feedback on their authentication status and instruct ISPs and mail systems to reject or quarantine forged email. Finally, opportunistic Transport Layer Security (TLS) encrypts sessions between mail servers to prevent fraud and eavesdropping. Overall adoption was excellent (100% of sites support both SPF and DKIM, the recommended best practice), and use of opportunistic TLS is the highest of all sectors (57%).

  However, there's a missed opportunity with DMARC (only one candidate's email supports it). OTA encourages all candidates to add this support as soon as possible since the absence of DMARC support invites the campaign to be targeted by cybercriminals and spearphishing campaigns, and this vulnerability is fully disclosed when examining a site's Domain Name System files (DNS). As there is no cost or impact to server performance and DMARC can be implemented in minutes, there is no excuse for candidates not to implement it, whereas failing to do so puts consumers at unnecessary risk.

CONCLUSION

The privacy and data security landscape is rapidly evolving with new threat vectors emerging daily threatening consumer's data, privacy and identity as well as risking the reputations of candidates and sites worldwide. Left unchecked the impact can drive identity theft, financial account take-overs as well as disclosure of personal and sensitive information impacting one's employability, and financial stability.

On the whole candidates' sites audited have excellent security configurations today, but candidates should not rest on their laurels and become complacent. We believe such sites are breaches waiting to happen as they are prime targets for people motivated by the commercial value of the data or politics and hacktivism. As we have observed with commercial sites, servers may be configured correctly "out of the box" but within thirty-to-ninety days can become vulnerable to new exploits and fall behind current security standards.

Focusing on consumer and candidates' brand protection, the inconsistent use of mailing domains and lack of comprehensive implementation of email authentication raises significant risks. In spite of otherwise good marks, as of today the majority of candidates' email systems are still exposed to the possibility of email being spoofed or forged. Typically such exploits are used to deliver malware and ransomware to unsuspecting users of both desktop and mobile devices. OTA encourages all candidates to fully adopt email authentication protocols and implement rejection policies for mail which fails authentication. Failing to do so not only puts consumers at risk but also impacts the deliverability and in-box placement of legitimate email communications.

As outlined in the report, the candidate sites' published privacy policies (and for some the lack of a policy) are concerning. While the broad disclosure of sharing of personal information with like-minded organizations may historically be "an accepted practice", it is concerning in light of the depth of information being collected, including date of birth, personal interests and even passport numbers and related data. OTA calls on all candidates to review and consider updating their policies to better reflect consumer concerns pertaining to the collection, use, retention and sharing of their personal information. OTA is prepared to provide advice to help.

Last but not least, all candidates need to be prepared for a breach and develop a comprehensive breach readiness plan.[6] Such plans need to include mechanisms and procedures to help prevent, detect, mitigate and remediate any such data loss incidents, including timely notification to consumers, law enforcement and State regulators. As several states require commercial sites to have such plans, consumers' data collected by candidate sites should be afforded the same level of protection.

The following sections detail the methodology and scoring used in the Audit and then examine each major audit category in more detail, including adoption rates of key criteria, comparison to best practices of other sectors, and insights, observations and recommendations for the candidates.

[6] OTA Data Breach Readiness Guide https://otalliance.org/Breach

DATA PROTECTION, PRIVACY & TRANSPARENCY

RECOMMENDED BEST PRACTICES

Best practices can be summarized as follows:

- Publish discoverable, easy to find, and comprehensible privacy policies.
- 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.*"[7]
- Create a layered, concise summary linking to an expanded policy. Use icons to help consumers navigate the policy elements more easily. Provide a clear statement including details if, what and for what purposes personal data is being shared with third parties. 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 and the importance of the Hispanic voting community (this is a lost opportunity for many of the candidates, sending a message to this voting block). See Spanish version of OTA's privacy policy – https://otalliance.org/politica-de-privacida.
- Disclose whether the site honors Do Not Track (DNT) settings in the site's privacy policy, and preferably honor users' DNT browser settings as required by the State of California. Suggested copy –

  > *XYZ site 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 XYZ does not respond to DNT mechanisms. Once a standardized "do not track" feature is released, XYZ intends to adhere to the browser settings accordingly.*

- Utilize tag management systems or privacy solutions that can manage third-party trackers and ensure they are acting properly.

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

CANDIDATE SITES RESULTS

As outlined in the "2016 Presidential Candidate Sites Audit Highlights" section, the Privacy category is the cause for failure (and concern) for nearly three-fourths of candidate sites. Figure 6 below shows the breakdown of the 100 baseline points into its two 50-point components – the policy score and the tracking score. The policy score assesses the privacy policy content regarding clear notice, data sharing/retention/notice practices and vendor confidentiality. The tracking score reflects the number and type of third-party trackers on the site, with maximum points possible for a low number of trackers and those that have restrictive (or no) data sharing practices. 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.

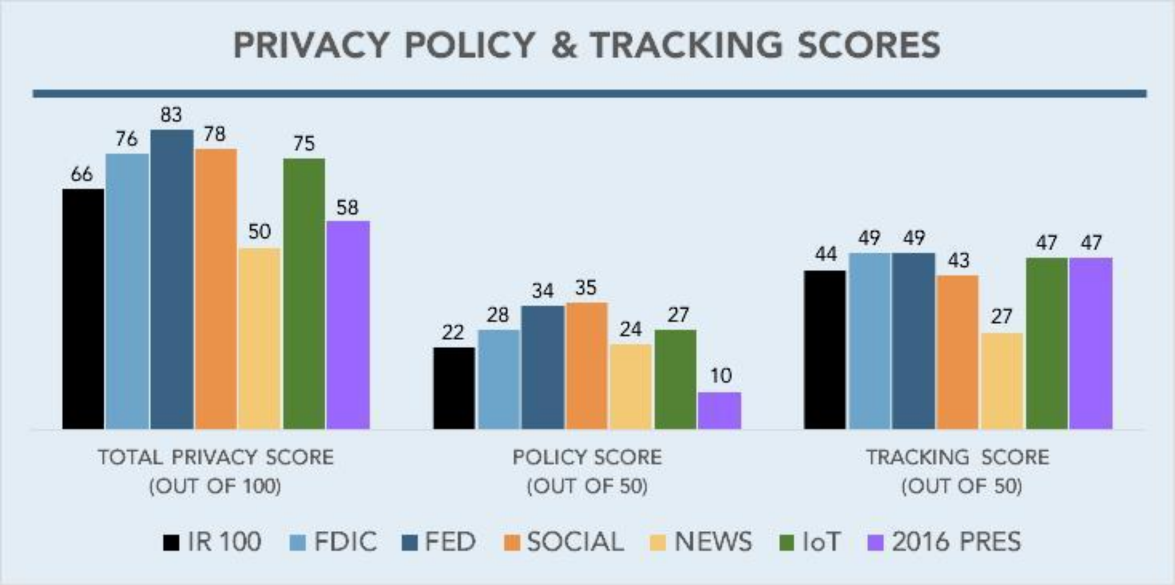

Figure 6 – Privacy Policy and Tracking Scores by Sector

As noted previously, the candidate sites' tracking score is near the top, which is to be expected since there are no ads on the sites. The area of concern is the policy score, which at an average of 10 out of 50 is significantly lower than all other sectors (and well under half the overall average of 28). Policies failed because they were absent, silent or promiscuous about data sharing, retention and user notice as well as third-party use of data. It is recognized that widespread sharing of voter data is common within political parties, but candidates should recognize that voters may not want their information shared in such a manner, and possibly provide an "opt-in" to such sharing versus claiming that right in the default policy.

An interesting side note – the length of the sites' privacy policies ranged from 278 words (Graham) to 3,354 words (Bush) and averaged 1,439 words. OTA believes that a well-constructed concise 500-word short layered policy linking to a longer policy strikes the balance between brevity and adequate disclosure. See OTA's privacy policy as example of using a short layered notice https://otalliance.org/privacy-policy.

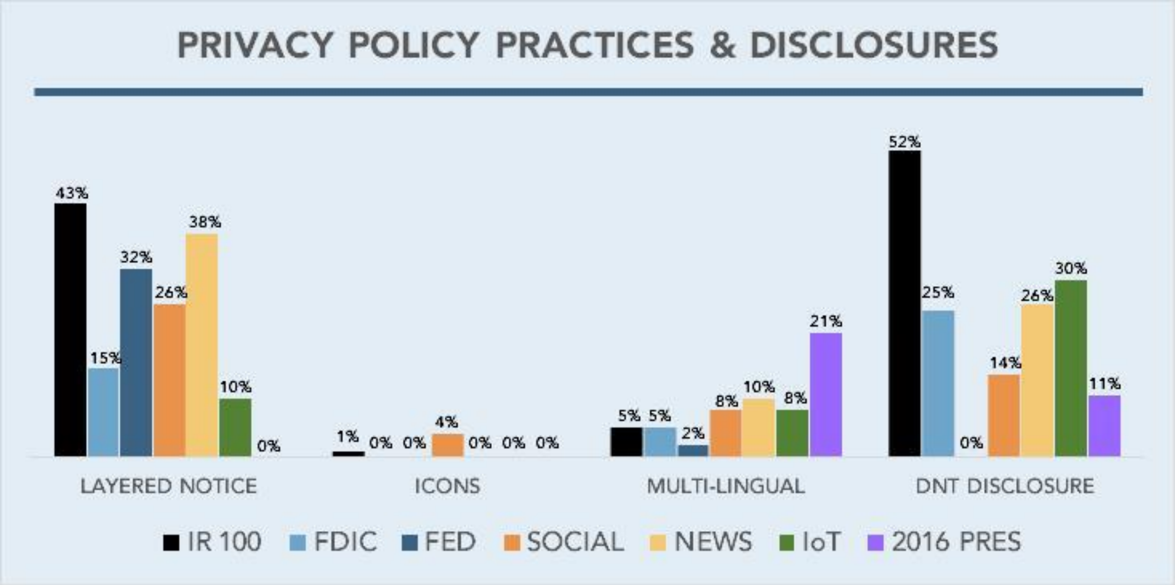

Figure 7 – Privacy Policy Implementation and Disclosure by Sector

Figure 7 above shows additional analysis of the content and implementation of candidate sites' privacy policies which qualify for "bonus" points. Observations regarding these criteria are as follows:

- **Layered Notice** – Disappointingly, no sites had a layered notice, which makes the policy easier to read, comprehend and navigate (the average for other sectors is 21%). This is becoming an established practice that will likely be incorporated into base line scoring in future audits.
- **Policy Icons** – No sites used icons in their privacy policy, which further aids user navigation, though no other sectors have implemented this in a meaningful way. See leading example from Publishers Clearing House.[8]
- **Multi-Lingual Policies** – Candidate sites lead all other sectors 2:1 or more in use of multi-lingual policies (all Spanish), which makes sense given their need to reach all possible voters. Considering the efforts by several candidates to court this voting block, this might be a lost opportunity to demonstrate interest.
- **Do Not Track** – Only two sites address Do Not Track in their policy (lagging nearly all other sectors), and only one said they would honor the Do Not Track setting. This requirement is mandated by the State of California for all sites with users who reside in the State.

[8] http://privacy.pch.com/

Additional privacy observations:

- Tag Management Systems/Privacy Solutions (TMS/PS) – Though candidates' sites would not be expected to have a significant number of third-party trackers, TMS/PS can help sites better manage, review and monitor data sharing in real time. In reality many sites had a surprising number of trackers, ranging from 9 to 212 and averaging 69. Nearly half (48%) of the sites utilize a TMS/PS, which is slightly lower than the overall average of 55% for all other sectors evaluated.[9]
- Private WHOIS Registrations – As noted in the Highlights section, this is an area of concern due to the transparency issue of domain ownership. Forty-four percent of candidate sites have a private registration, a whopping four times higher than other sectors, which range from 2%-11% and average 9%. Even if these domains were registered privately prior to use, now that sites are public the domain ownership should be made public as well. Voters want to see transparency in government and candidates can lead by example. Public registration enhances voter trust and makes it easier to discern fraudulent lookalike sites that may be using private registrations.

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

SITE, SERVER & INFRASTRUCTURE SECURITY

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

RECOMMENDED BEST PRACTICES

Best practices in this category can be summarized as follows:

- Optimize server SSL implementation using information gleaned from tools such as OTA-Qualys SSL Labs,[10] with specific focus on vulnerabilities that earn a letter grade of "F".
- Use EV SSL certificates for domains and sites which are frequently spoofed and for sites where users need to be assured they are visiting and browsing a legitimate site.
- Implement AOSSL or HTTPS on all pages to maximize data security and online privacy.
- Implement a Web Application Firewall to monitor HTTP conversations and block common attacks such as cross-site scripting (XSS) and SQL injections.
- Proactively scan sites and third-party content for malicious links, iFrame exploits, malware and malvertising.[11]
- 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.

CANDIDATE SITES RESULTS

As illustrated in the middle set of bars in Figure 5, candidate sites outperformed all other sectors in the baseline scoring for this category, again not surprising given their simple and newly formed infrastructure.

Specific results for each of the best practice recommendations were as follows. For detailed comparisons by sector, see the table in Appendix B.

- Optimized SSL/TLS – With few exceptions (one "C" and a few "B's"), candidate sites scored very well, and their average score was significantly higher than any other sector. Of note, one site supported encryption via a frame not visible to the user, so it was unclear whether data was encrypted, even while donating to the campaign. This should be corrected to make it clear. Consumers trained to look for "https://..." in the browser bar may hesitate to donate and lack of clear notice invites spoofing and confusion.

[10] https://ota.ssllabs.com/
[11] https://otalliance.org/resources/type/advertising-integrity-fraud

- **EV SSL Certificates** – Only one candidate's site has taken advantage of this simple yet powerful trust-enhancing practice (users see a green indicator in the browser bar). This adoption rate (4%) is on the low end of key sectors (Fed at 11%, Social at 21%, online retailers at 24% and banks at 67%). Given the ease of implementation and low cost of EV SSL, this is a missed opportunity to enhance trust.
- **AOSSL** – Adoption of this key best practice was high (70%), outpacing all but the banks (78%) more than 2:1. Given that citizens are submitting personal information and making donations on candidate sites, this level of adoption is encouraging, though not surprising. Additional incentives include the Federal government itself, which has mandated use of AOSSL for all government sites by December 31, 2016, and Google, whose search results and rendering in Chrome are enhanced for sites supporting AOSSL.
- **Web App Firewall** – 35% of candidate sites have implemented a web app firewall, which is near the overall average for other sectors, but lags the leaders significantly (online retailers at 47%, federal government sites at 46%). Given that these sites are new, adoption should be higher.
- **Site Vulnerabilities** – 4% (one site) has a XSS/iFrame vulnerability, which is lower than all sectors but banks (1%). No sites were found to have malware or malicious links. Considering the simplicity of candidates' site architecture the one anomaly was disappointing. To date, efforts to reach the site and provide responsible disclosure have not been responded to.

CONSUMER PROTECTION

By utilizing the email authentication standards Sender Policy Framework (SPF) and Domain Keys Identified Mail (DKIM), organizations can help protect their brand 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, Domain-based Message Authentication, Reporting, and Conformance (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 sender and consumer. Domain locking ensures that domain ownership cannot be transferred without the owner's permission, further helping to protect a site's brand from abuse. Domain Name System Security Extension (DNSSEC) adds security and integrity to the DNS lookup, helping to prevent "Man-in-the-Middle" (MitM) attacks, cache poisoning and related DNS attacks.

RECOMMENDED BEST PRACTICES

Best practices include:

- Implement both SPF and DKIM for top-level domains (most recognizable to the recipient / consumer), "parked" domains (not used) and any major subdomains seen on websites or used for email, including those managed by third party email service providers.
- 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 workers and volunteers as well as organizational data from spearphishing exploits.
- Implement opportunistic TLS to help protect and enhance the privacy of email in transit between mail servers.
- Ensure that domains are locked to prevent unauthorized domain takeovers.
- Implement DNSSEC to further protect a site's DNS infrastructure from attack and exploits, including man-in-the middle exploits.

CANDIDATE SITES RESULTS

As seen in Figure 5, candidate sites outperformed all other sectors in the baseline scoring for this category, which is not surprising given the straightforward nature of their email infrastructure and associated ability to utilize the latest services for email. Specific results for each of the best practice recommendations were as follows. For detailed comparisons by sector, see the table in Appendix B.

- SPF and DKIM – Adoption of the recommended best practice of using both SPF and DKIM was 100% (the highest of all sectors). Use of SPF at the top-level domain (the domain of the website) was near the highest (91%) while use of DKIM at the top-level domain far outpaced all sectors (78% - next closest was 56%). Though somewhat expected since these sites have one primary purpose, email should be coming from the primary domain to reduce consumer confusion.
- DMARC – This area was a big disappointment, since only one candidate's email uses a DMARC record, and it makes no policy assertion. Given the streamlined nature of candidates' infrastructure and the ease of implementing DMARC (a simple text record in the DNS), there is no reason all candidates' systems should not have a DMARC record asserting a "Reject" policy, allowing receiving systems to discard spoof messages and protect citizens. Even sectors with much larger and more complex infrastructures have implemented DMARC records (48% for Social, 24% for banks and 20% for online retailers) and many have made policy assertions. If all candidates' systems added DMARC with a reject policy, the scoring in this category would be nearly perfect.
- Opportunistic TLS – Candidates' email significantly led other sectors with 57% adoption.
- Domain Locking – All but one has locked their domain. This is a simple issue that should be addressed immediately to help prevent unauthorized domain transfer.
- DNSSEC – No candidate sites have implemented DNSSEC, which is disappointing since OMB has issued a mandate for all Federal Government sites to implement it and the simplicity of candidates' site architecture makes such implementation straightforward and simple to manage.

One additional observation in this category was the varied use of different domains to send email. While most candidates' systems (~60%) send email from the same domain as their website (and therefore the most recognizable to the consumer or voter), some only send from a separate but related domain, which could confuse recipients, make them suspicious ("Is this really from the candidate?") or desensitize them to accept spoof messages from other lookalike domains.

OTA encourages candidates to align email domains with website domains as closely as possible to avoid voter confusion, suspicion or exposure.

CONCLUSION

As campaigns ramp up for candidates, political parties and super PACs, it is time for politicians, their staff and vendors to review the privacy, security and sensitivity of the information their donors and constituents entrust to them. The nation has been alarmed by data collection practices in the public and private sector, including those of the NSA. Now candidates must examine their own practices.

As the world economy and society at-large become increasingly reliant on the Internet, it is incumbent on politicians as well as the business community to embrace these practices and move from a compliance mindset to one of responsible privacy practices and data stewardship. Digital data is the lifeblood of the economy but it is being exploited daily by cyber-criminals and state sponsored actors, placing America at the crossroads of a trust meltdown, underscoring the need for candidates to walk the talk and put voters and their privacy ahead of their own interests.

While politicians have been successful in obtaining "carve outs" from anti-spam, privacy and related legislation, OTA believes most consumers would be alarmed at the broad liberties being taken with their data when they donate or volunteer to help a candidate. Donors are paying once with the bank accounts and in perpetuity with their personal data. Even though the language of many candidate sites' privacy policies may disclose they share personal information broadly with others (other candidates, organizations, campaigns, groups or causes that THEY believe have similar political viewpoints, principles or objectives), the reality is a consumer should not have to read a 3,000 word privacy policy to discover this. Instead, by default they should be able to trust the candidate with their data. Second, policies should be discoverable from every page of a candidate's site with clear and concise disclosures written for the consumer versus by attorneys for attorneys.

The OTA Online Trust Audit and Honor Roll highlights best practices, identifying organizations that have demonstrated a commitment to consumer safety, security and privacy. Disappointingly only six candidates' sites made the grade, while the balance (74%) received failing grades. The sites earning high grades, reflecting a commitment to consumer protection, data security and respect for privacy, in alphabetical order include; Jeb Bush (R), Lincoln Chafee (D), Chris Christie (R), Martin O'Malley (D), Rick Santorum (R) and Scott Walker (R).

In this post-Snowden era with its increased anxiety regarding industry privacy practices, OTA calls for greater disclosure on collection, use, retention and sharing as well as the ability for consumers to opt out (or ideally opt in) of all such sharing with third parties.

It is each candidate's duty to protect and be a steward of the data and personally identifiable information voters entrust to them and the recommended fixes are simple and straightforward. OTA has resources, tools and guidance available to help candidates understand and implement best practices to help keep their sites, messaging and data safe.

Let's work together in a bi-partisan effort to enhance online security and privacy.

ACKNOWLEDGEMENTS

The Audit has been powered in part by leading organizations, including: Agari, Disconnect, Distil Networks, Ensighten, GlobalSign, High-Tech Bridge SA, IID, Qualys, Return Path, SiteLock, SSL Labs, ThreatWave, TRUSTe and VERISIGN.

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. For updates visit No part of this publication may be reproduced or distributed in any form or by any means, or stored in a database, web site or retrieval without the written consent of OTA.

APPENDIX A – METHODOLOGY & SCORING CRITERIA

The criteria used in the annual Online Trust Audit are highly relevant to the security and privacy practices organizations must implement to maximize online trust and consumer protection and are indicative of the most current best practices supported by industry, standards bodies and government agencies. This Audit of 2016 Presidential Candidate Sites uses the same methodology and scoring as the 2015 Online Trust Audit, and includes a composite weighted analysis focusing on three major categories:

- Data Protection, Privacy & Transparency – includes analysis of privacy policy for disclosure and data protection, use of layered notice, icons and multi-lingual policies, acknowledgement of Do Not Track, analysis of data trackers (and their known policies) on the site, use of tag management systems, and private versus public WHOIS registrations.
- Site, Server & Infrastructure Security – includes implementation of secure protocols for web traffic (SSL, TLS, EVSSL, AOSSL, implementation of web application firewalls, resistance to cross-site scripting (XSS) and bot attacks and presence of malware or malicious links on the site. [12, 13, 14, 15]
- Domain, Brand & Consumer Protection – includes protection of email via email authentication and related technologies (SPF, DKIM, DMARC and TLS) as well as protection of DNS (DNSSEC) and domains (domain locking). [16]

Sites were eligible to receive 300 total base points (up to 100 points in each category), and up to 70 total bonus points for implementing emerging best practices. Additionally, organizations could lose up to 65 points for having observed vulnerabilities and other key deficiencies. The audit criteria are adjusted annually to address the evolving threat environment, responsible privacy practices and the need for all sites to continually monitor their security and privacy practices, thus "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 recognizing that sites are built on a "chain of trust" that is only as strong as its weakest link.

Data sampling was completed between August 15 and September 7, 2015. It is important to note that a site's configuration, privacy practices and published privacy policies 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 is shown in Appendix A. The methodology is posted at https://otalliance.org/initiatives/2015-honor-roll-methodology.

[12] https://otalliance.org/resources/ssl-best-practices
[13] https://otalliance.org/resources/always-ssl-aossl
[14] https://otalliance.org/best-practices/transport-layered-security-tls-email
[15] https://otalliance.org/resources/extended-validation-certificates-evssl
[16] https://otalliance.org/resources/email-security

DATA PROTECTION, PRIVACY & TRANSPARENCY

Best practices providing users clear notice and control of the data being collected, tracked and shared with third parties.

- Privacy Policy – *50 points of 100 point base score*
- Third Party Tracking on Site – *50 points of 100 point base score*
- Layered Privacy Policy – *bonus points*
- Use of Consumer-Friendly Icons – *bonus points*
- Localized/Multi-lingual Policy – *bonus points*
- Do Not Track (DNT) Privacy Policy disclosure – *bonus points*
- Honoring of Do Not Track Browser Settings – *bonus points*
- Implementation of Tag or Privacy Management Systems – *bonus points*
- Public versus Private WHOIS registration – *penalty if private*
- Data Breach & Loss Incidents – *penalty if incident since January 2014*

SITE, SERVER & INFRASTRUCTURE SECURITY

Best practices to secure data in transit and collected by websites and prevent malicious exploits running against clients' devices including desktop, mobile and IoT devices.

- Secure Sockets Layer (SSL) Server Configuration – *part of base score, with increased granularity and requirement levels in 2015, including RC4, SHA1 and Forward Secrecy* [17]
- Evaluation of SSL Certificate type (Domain Validation [DV] or Organization Validation [OV]) – *part of base score*
- Extended Validation SSL Certificates (EV SSL) – *bonus points*
- Always On SSL (AOSSL) – *bonus points*
- Bot detection and mitigation - *part of base score*
- Web Application Firewall – *bonus points*
- Testing for XSS, iframe exploits, malware, malicious links – *penalty if these threats exist*

[17] https://ota.ssllabs.com/

DOMAIN, BRAND & CONSUMER PROTECTION

Best practices to help detect and prevent malicious and spoofed email and protect corporate domains.

- Email Authentication (Sender Policy Framework and DomainKeys Identified Mail) – *part of base score, maximized by implementing both methods at top-level and subdomains*[18]
- Domain-based Message Authentication, Reporting & Conformance (DMARC) – *part of base score*
- Implementation of "opportunistic" Transport Layered Security (TLS) for email[19] – *bonus points*
- Domain Name System Security Extension (DNSSEC) – *bonus points*
- Domain Locking – *penalty if domain not locked*

The Audit factors were weighted and scored based on the impact they have on email integrity and risks, consumer protection, website security, consumer transparency and overall best practices that will distinguish an organization and brand from the consumer's perspective.

[18] https://otalliance.org/eauth

[19] https://otalliance.org/best-practices/transport-layered-security-tls-email

APPENDIX B – DETAILED SECTOR COMPARISON

The following tables summarize adoption of specific criteria evaluated in the Consumer Protection and Site Security categories and allow a comparison of adoption by 2016 Presidential Candidate Sites to other key sectors.

2015 AUDIT RESULTS BY SECTOR
CONSUMER PROTECTION ADOPTION

	IR100	FDIC	FED	SOCIAL	NEWS	IoT	2016 PRES
SPF (any)	94%	87%	80%	92%	80%	62%	100%
SPF (TLD)	85%	73%	70%	92%	62%	52%	91%
DKIM (any)	93%	68%	50%	78%	64%	30%	100%
DKIM (TLD)	31%	30%	28%	56%	16%	14%	78%
SPF and DKIM	90%	63%	48%	76%	56%	30%	100%
DMARC Record	20%	24%	14%	48%	10%	2%	4%
DMARC (R or Q)*	15%	21%	14%	58%	20%	0%	0%
TLS	42%	38%	38%	36%	14%	24%	57%
DNSSEC	0%	1%	90%	0%	4%	4%	0%
Domain Lock	100%	97%	100%	94%	92%	88%	96%

* Based on organizations with a DMARC record

2015 AUDIT RESULTS BY SECTOR
SITE SECURITY ADOPTION

	IR100	FDIC	FED	SOCIAL	NEWS	IoT	2016 PRES
EV SSL	24%	67%	11%	21%	8%	4%	4%
Always On SSL	15%	78%	17%	35%	14%	20%	70%
Web App Firewall	47%	32%	46%	12%	28%	36%	35%
XSS/iFrame Vulnerability	10%	1%	20%	16%	48%	6%	4%

APPENDIX C – PRIVACY POLICY EXCERPTS

The following paragraphs provide links to the privacy policies evaluated (if present), the date the policy was last updated (if available) and excerpts of key language from each candidate's privacy policy. To see the full context of the excerpts, readers are encouraged to review the complete privacy policies via the provided links.

1. **Jeb Bush** – Use of Personal Information: If we do receive your personal information, we will only use it for the purposes described where it is collected or otherwise described in this Privacy Policy. We may share this information outside of Jeb 2016, Inc. if: (1) you authorize us to do so; (2) it is necessary to allow our service providers or agents to provide products or services for us; (3) it is necessary in order to provide our products or services to you (and contacting you when necessary); (4) subject to applicable contractual or legal restrictions, it is necessary to disclose to entities that perform marketing services on our behalf or to other entities with whom we have joint marketing agreements; (5) subject to applicable contractual or legal restrictions, it is necessary in connection with a sale of all or substantially all of the assets of Jeb 2016, Inc. or the merger of Jeb 2016, Inc. into another entity or any consolidation, share exchange, combination, reorganization, or like transaction in which Jeb 2016, Inc. is not the survivor"
   https://jeb2016.com/privacy Updated June 15, 2015

2. **Ben Carson** – Carson America may share information that you voluntarily provide us with like-minded organizations committed to the principles or candidates of the Republican Party, Republican State Party organizations and local Republican groups. Carson America may provide your email address or other personal information to authorized This Privacy Policy does not cover the collection methods or use of the information collected by vendors of Carson America.
   https://www.bencarson.com/privacy-policy/ Updated June 26, 2015

3. **Lincoln Chafee** – Other than to our agents, contractors and affiliates, as described above, we disclose personal information only in response to a subpoena, court order or other governmental request, or when we believe in good faith that disclosure is reasonably necessary to protect our property or rights. We take all measures reasonably necessary to protect against the unauthorized access, use, alteration or destruction of personal information.
   http://www.chafee2016.com/privacy-policy/ No date posted

4. **Chris Christie** – If you choose to identify yourself (or otherwise provide us with personal information) when you use our online forms: We will collect (and may retain) any personally identifying information, such as your name, street address, email address, and phone number, and any other information you provide. We will use this information to try to fulfill your request and may use it to provide you with additional information at a later time. We may share your information with third parties. If you request information, services, or assistance, we may disclose your personal information to those third parties that (in our judgment) are appropriate in order to fulfill your request. If, when you provide us with such information, you specify that you do not want us to disclose the information to third parties, we will honor your request.)
   https://www.chrischristie.com/privacy-policy Updated June 27, 2015

5. **Hillary Clinton** – We may share information about you as follows or as otherwise described in this Privacy Policy: With vendors, consultants and other service providers or volunteers who need access to such information to carry out work on our behalf; With candidates, organizations, campaigns, groups or causes that we believe have similar political viewpoints, principles or objectives or share similar goals and with organizations that facilitate communications and information sharing among such groups;; In connection with, or during negotiations of, any reorganization, formation of new committee or successor organization, asset sale or transfer, financing or lending transaction or in any other situation where personal information may be disclosed or transferred as one of the assets of HFA.
https://www.hillaryclinton.com/legal/privacy-policy/ Updated April 12, 2015

6. **Ted Cruz** – In order to maximize your experience with our website and Cruz Crew and to provide its features and services, we may periodically access your contact list and/or address book on your mobile device. You hereby give your express consent to access your contact list and/or address book. Whenever you voluntarily disclose personal information on publicly-viewable screens or pages, that information will be publicly available and can be collected and used by others. If you wish, we will delete your account information; to do so, please close your account by sending an email to cruzcrewhelp@tedcruz.org. https://www.tedcruz.org/privacy-policy Updated July 7, 2015

7. **Carly Fiorina** – May provide or sell your email address or other personal information to third parties for fundraising or other purposes. Additionally, we may share your personal information with select third parties who offer goods or services we think may be of interest to you…. we may partner with other organizations or companies to provide co-sponsored or co-branded promotions, services or events and may share your personal information with our co-sponsor(s) and partners.

   Please be aware that third-party websites that process payments for Carly for President and websites for our advertisers, sponsors, affiliated entities and other third parties that are accessible through this Site may have their own privacy and data collection policies and practices. We are not responsible for the privacy practices of such sites and will not be responsible for any actions or policies of such third parties.

   Your browser and other mechanisms may permit you to send do-not-track signals or other similar signals to express your preferences regarding online tracking. To the extent you employ such browser do-not-track signals or other similar mechanisms, we will use commercially reasonable efforts to honor such requests received by us to the extent we have the capacity and resources to identify and process your request. Due to the potential for rapid and diverse developments of technology in this area, we cannot guarantee that we can process every type of request that exists or may be developed in the future. As noted above, third parties, such as our advertising partners, may collect data that relates to you. We cannot control third parties' responses to do-not-track signals or other such mechanisms.
   https://carlyforpresident.com/privacy Updated May 1, 2015

8. **Jim Gilmore** – No posted or discoverable privacy policy http://gilmoreforamerica.com/

9. **Lindsey Graham – Silent on use, sharing and retention**
http://www.lindseygraham.com/privacy/ No date posted

10. **Mike Huckabee – Silent on sharing**
http://www.mikehuckabee.com/privacy-policy No date posted

11. **Bobby Jindal** – We may share your Personal Information with our service providers and affiliates, as well as other organizations that share our views. We may make this information available to other third parties. We also will disclose Personal Information to any new or successor entity, should Jindal for President be reorganized, acquired or merged with another entity, in whole or part.
    https://www.bobbyjindal.com/privacy-policy/ Updated June 24, 2015

12. **John Kasich – No posted privacy policy** https://johnkasich.com/

13. **Lawrence Lessig** - with organizations, groups, or causes that we believe have similar viewpoints, principles, or objectives; We are not responsible for the actions of any service providers or other third parties, nor are we responsible for any additional information you provide directly to any third parties, and we encourage you to become familiar with their privacy practices before disclosing information directly to any such parties.
    https://lessigforpresident.com/privacy-policy/ Updated September 11, 2015

14. **Martin O'Malley** – We will never provide your e-mail address or any of your personal information to any other person or organization, for any purpose, except –To Governor O'Malley's Leadership PAC, O'Say Can You See PAC.
    https://martinomalley.com/privacy-policy/ No date posted

15. **George Pataki** – We will not sell your personal identifiable information to any party. We reserve the right to share your information with trusted third parties who assist us in operating our website, or servicing you, so long as those parties agree to keep this information strictly confidential. We also release individual information when required to comply with the law, enforce our site policies, or protect ours or others' rights, property, or safety. And, as noted above, on occasion, we may also share information — that you voluntarily provide us — with like-minded organizations, committees, or candidates committed to the our principles. By voluntarily providing your information, you are agreeing that we may use that information in the manners described.
    http://georgepataki.com/privacy-policy/ Updated May 24, 2015

16. **Rand Paul** – It is our policy not to share the personal information we collect from you through our Sites with third parties, except as described in this Policy or as otherwise disclosed on the Sites. For example, we may share personal information as follows: with vendors, consultants, and other service providers or volunteers who are engaged by or working with us and who need access to such information to carry out their work for us; with organizations, groups, or causes that we believe have similar viewpoints, principles, or objectives - We are not responsible for the actions of any service providers or other third parties, nor are we responsible for any additional information you provide directly to any third parties, and we encourage you to become familiar with their privacy practices before disclosing information directly to any such parties.
    https://www.randpaul.com/privacy Updated April 7, 2015

17. **Marco Rubio** – We will not sell your personal identifiable information to any party. We reserve the right to share your information with trusted third parties who assist us in operating our website, or servicing you, so long as those parties agree to keep this information strictly confidential. And, as noted above, on occasion, we may also share information — that you voluntarily provide us — with like-minded organizations, committees, or candidates committed to the our principles.
    https://marcorubio.com/privacy/ Updated March 30, 2015

18. **Bernie Sanders** – Though we make every effort to preserve your privacy, we may share Personal information as follows: When we have a good-faith belief that release is appropriate to comply with the law (for example, a lawful subpoena); To protect the rights or property or safety of our supporters, employees, volunteers or others; With vendors, service providers, consultants, employees, contractors, or volunteers who need to know such information to carry out their duties; With groups, causes, organizations, or candidates we believe have similar views, goals, and principles; https://berniesanders.com/privacy-policy/ Updated May 21, 2015

19. **Rick Santorum** – Personally Identifiable Information: SANTORUM FOR PRESIDENT will not rent or sell your personally identifiable information to others. SANTORUM FOR PRESIDENT may share your personally identifiable information with third parties for the purpose of providing RICKSANTORUM.COM services to you. If we do this, such third parties' use of your information will be bound by this Privacy Policy. Except as otherwise described in this Privacy Policy, SANTORUM FOR PRESIDENT will not disclose personal information to any third party unless required to do so by law or subpoena or if we believe that such action is necessary to http://www.ricksantorum.com/privacy No date published

20. **Jill Stein – No privacy policy published / discoverable** www.jill2016.com

21. **Donald Trump** – Voluntary Information: You may voluntarily provide information to us in the course of using this website. By entering your name, email address, postal address, phone number, cell phone number, or other personal information in forms, registering, signing up, making a contribution, or otherwise providing the information through this website, we collect information you voluntarily provide. By providing this information, you consent to our contacting you through these means. Additionally, from time to time, we may share your voluntarily provided information to like-minded organizations.
https://www.donaldjtrump.com/about/privacy-policy/ No date published

22. **Scott Walker** - We may share your personally identifiable information with third parties for the purpose of providing our services to you. If we do, this Privacy Policy will bind such third parties' use of your information. Except as otherwise described in this Privacy Policy, We will not disclose personal information to any third party unless required to do so by law or subpoena or if we believe that such action is necessary to (a) conform to the law, comply with legal process served on us or our affiliates; (b) to enforce this policy, take precautions against liability, to investigate and defend ourselves against any third-party claims or allegations, to assist government enforcement agencies, or to protect the security or integrity of our sites; and (c) to exercise or protect the rights, property, or personal safety of our users, Us, or others.
https://www.scottwalker.com/privacy Updated July 11, 2015

23. **Jim Webb – No privacy policy posted** https://www.webb2016.com/, though a Google search yields a policy (https://www.webb2016.com/privacy-policy/) that can't be linked from the main site and appears to be an orphaned page from the exploratory committee site.