Online Trust Alliance
an **Internet Society** initiative

Online Trust Audit – 2020 U.S. Presidential Campaigns

Recognizing excellence in security, consumer protection and responsible privacy practices

8 October 2019

Internet Society's Online Trust Alliance

Online Trust Audit – 2020 Presidential Campaigns

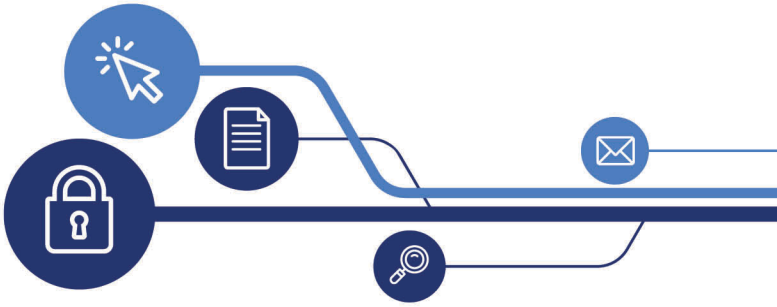
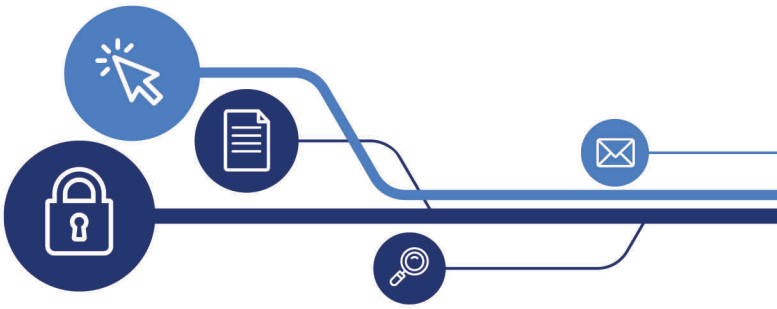


Table of Contents

Internet Society's Online Trust Alliance

Online Trust Audit – 2020 Presidential Campaigns



Executive Summary

Data protection, privacy, and security have dominated recent headlines, leading to increased scrutiny across multiple industry sectors, including in the U.S. Congress. The 10th Online Trust Audit & Honor Roll, [1] published by the Internet Society's Online Trust Alliance (OTA)[2] in April 2019, evaluates the consumer protection, security, and privacy protection practices of nearly 1,200 organizations across several sectors.

Given increased concerns about security and privacy in the political realm and the continuing drumbeat of high-profile data breaches,[3] [4] we conducted an Audit of the websites and email practices of 2020 U.S. presidential campaigns using the same methodology as the Online Trust Audit. In September of 2015, we published a similar Audit of the 2016 U.S. presidential campaigns' websites and email at the time.[5]

This Audit examines three main categories:

- **Privacy** – data sharing, retention, notice, and third-party restriction policies in the privacy statement, as well as analysis of third-party tracking on the website
- **Website 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

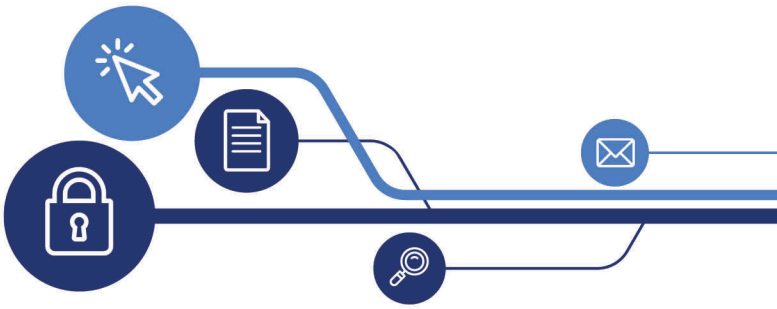
Campaigns earn Honor Roll status by having an overall score of 80% or higher with no failure in any of the three categories. The results for the campaigns are shown in Figure 1 below. Disappointingly, only 30% (seven) of the campaigns made the Honor Roll, while 70% had a failure in one or more categories. There was no middle ground (a score not high enough to earn Honor Roll status, but no failures); all campaigns either made the Honor Roll or had a failure.

ONLINE TRUST AUDIT RESULTS – 2020 U.S. PRESIDENTIAL CAMPAIGNS

Honor Roll	Had a Failure	
Pete Buttigieg (D)	Michael Bennet (D)	Tim Ryan (D)
Kamala Harris (D)	Joe Biden (D)	Mark Sanford (R)
Amy Klobuchar (D)	Cory Booker (D)	Joe Sestak (D)
Beto O'Rourke (D)	Steve Bullock (D)	Tom Steyer (D)
Bernie Sanders (I)	Julian Castro (D)	Joe Walsh (R)
Donald Trump (R)	John Delaney (D)	Elizabeth Warren (D)
Marianne Williamson (D)	Tulsi Gabbard (D)	Bill Weld (R)
	Wayne Messam (D)	Andrew Yang (D)

Figure 1 – 2020 Presidential Campaign Audit Results

[1] 2018 Online Trust Audit & Honor Roll, https://www.internetsociety.org/resources/ota/2019/2018-online-trust-audit-and-honor-roll/
[2] Internet Society's Online Trust Alliance https://www.internetsociety.org/ota/
[3] 2018 Cyber Incident & Breach Trends Report https://www.internetsociety.org/resources/ota/2019/2018-cyber-incident-breach-trends-report/
[4] Recent cyberattacks require vigilance https://blogs.microsoft.com/on-the-issues/2019/10/04/recent-cyberattacks-require-us-all-to-be-vigilant/
[5] 2016 Presidential Candidates Online Trust Audit https://www.internetsociety.org/resources/ota/2015/2016-presidential-candidates-online-trust-audit/



All campaigns listed in the failure column had a failure in the privacy category, and two campaigns also failed in the consumer protection category. Overall, we found that campaigns have strong website security, reasonable email and domain protections, and poor privacy scores. Privacy statements are the biggest concern, causing failure for 70% of the campaigns.

In this report, we analyze findings in the main categories and dive into areas of success and failure amongst 23 presidential campaigns active as of 7 October 2019.

This report serves four primary objectives:

- Promote best practices and provide tools and resources to help public and private sectors enhance their security, data protection, and privacy practices.
- Recognize leadership and commitment to best practices that aid in the protection of online trust and confidence in online interaction.
- Help improve campaigns' email and domain protection, security, and privacy practices.
- Assist consumers in making informed decisions about the security and privacy practices of websites they frequent.

The information and results included in the report are not an endorsement, condemnation, or opinion regarding any campaign and serve solely to help educate voters and campaigns about the privacy, site security, and email and domain protection status of the campaigns' online presence.

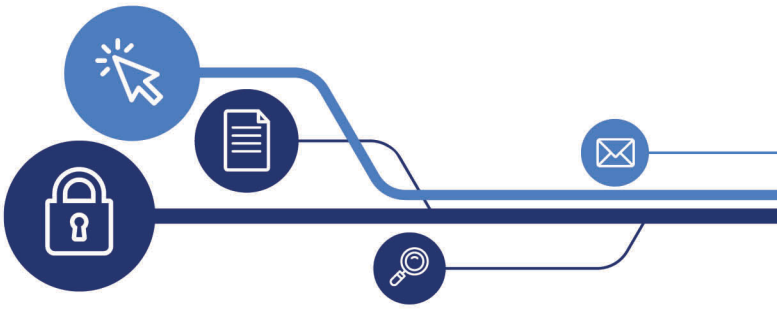
Background

OTA has conducted ten Online Trust Audits, which are recognized as a benchmark of organizations' commitment to security, privacy, and consumer protection best practices. As cyber threats increase 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, website, and mobile application, whether commercial or political.

As with making any payments or donations, or signing up for any online service, users are encouraged to evaluate campaigns to see if the 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 statements vary significantly, from stating that they disallow any sharing to language effectively enabling campaigns to share personal information broadly with any third party.

OTA conducted an evaluation of the 2020 U.S. presidential campaigns using the same criteria as the 2018 Online Trust Audit (released in April 2019) to examine their security, consumer protection, and stated privacy practices.

Each category (privacy, site security, and consumer protection) is worth 100 baseline points, with bonus points available for emerging best practices. To qualify for the Honor Roll, campaigns must achieve a combined score of 80% or higher, yet not fail (score less than 60) in any single category. The detailed methodology and criteria are in Appendix B.



The list of campaigns audited was selected according to Ballotpedia.org, which as of 7 October 2019 listed 19 Democratic candidates and four Republican candidates. Campaign websites are also listed on Ballotpedia.org under each candidates' profile (the complete list is shown in Appendix D).[6] Campaigns' website privacy statements, websites, and email practices were examined by signing up for email and using publicly available tools and data.

Data collection started the week of 19 August and final verification was done on 26 September. A preliminary report was sent to campaigns the week of 30 September, and some campaigns made updates, which were evaluated on 7 October. 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 have changed since the analysis was completed.

It is also important to note that this Audit is limited to an analysis of the campaigns' websites, email communication, and posted privacy statements. Outside the scope of the Audit are any side data-sharing agreements a campaign may have, including with their national political parties.

Presidential Campaign Audit Highlights

The online presence for campaigns is much like other organizations – they need a place to communicate their messages, they collect data on their "customers" for purposes of direct communication and fundraising, and they need to have appropriate online services to support both mass communication (via email and social media) and financial transactions.

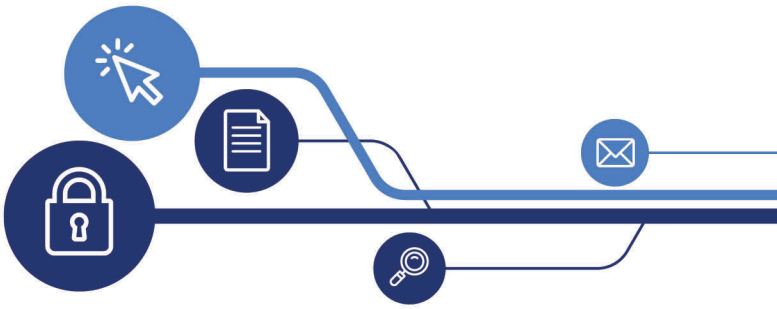
It is also important to note that most of the campaigns have an online presence less than a year old, so they can take advantage of current hosting and email services, which generally have the latest security protocols and capability built into their offerings. Therefore, one would expect adoption of recommended best practices to be straightforward, though we found that this is not necessarily the case.

Honor Roll Achievement

Similar to the Audit of 2016 presidential campaigns, Honor Roll achievement for the 2020 campaigns lagged behind all other sectors in the 2018 Online Trust Audit, this time by more than a 2:1 ratio. Figure 2 compares the percentage of organizations in each sector that earned Honor Roll status in the full Audit with the results for the campaigns. Honor Roll achievement ranged from 30% for the 2020 campaigns to 91% for U.S. federal government organizations.

Likewise, Figure 3 shows the failure rate (percentage of organizations failing in one or more category) by sector. Unsurprisingly, campaigns fare poorly here as well, with a 70% failure rate, compared to an overall average of 27% for sectors in the 2018 Online Trust Audit.

[6] Presidential candidates, 2020 https://ballotpedia.org/Presidential_candidates,_2020



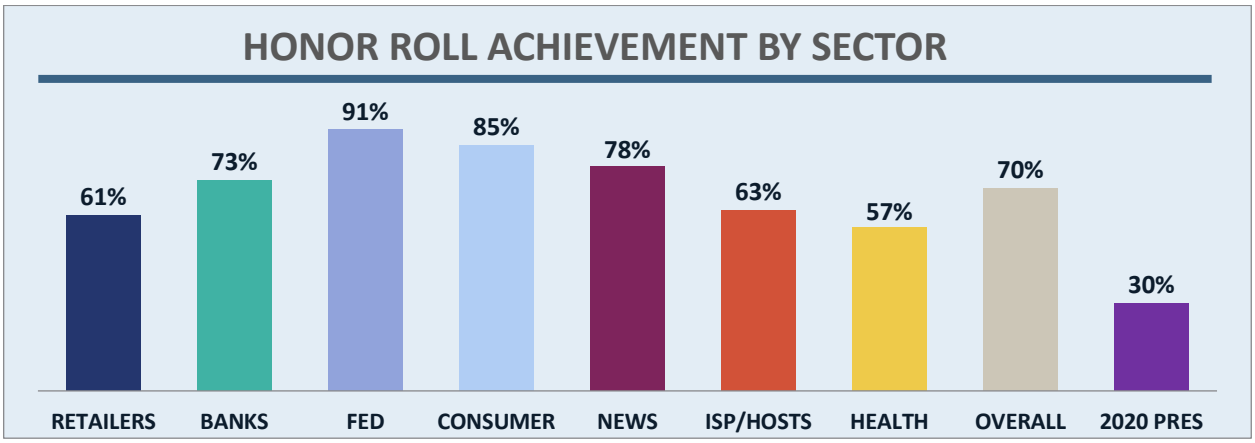


Figure 2 – Honor Roll Achievement by Sector

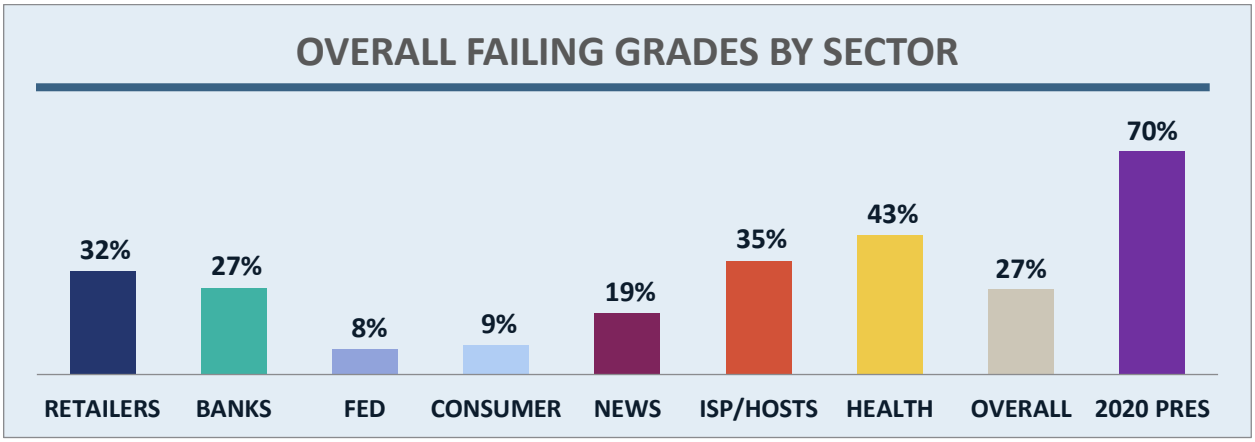


Figure 3 – Percent of Organizations with Failing Grade by Sector

Failure Rates

To understand the high failure rate for campaigns, it is useful to look further inside the data. Figure 4 shows failure rates for each of the three main audited categories. While campaigns had excellent results in site security (no failures), the consumer protection failure rate of 9% (vs 13% overall for other sectors) should be even lower, and the failure rate due to privacy raises big concerns. The failure rate of 70% in the privacy category was nearly five times the overall failure rate for other sectors. Of the 16 campaigns that had a failure, all failed in privacy, and two also failed in consumer protection.

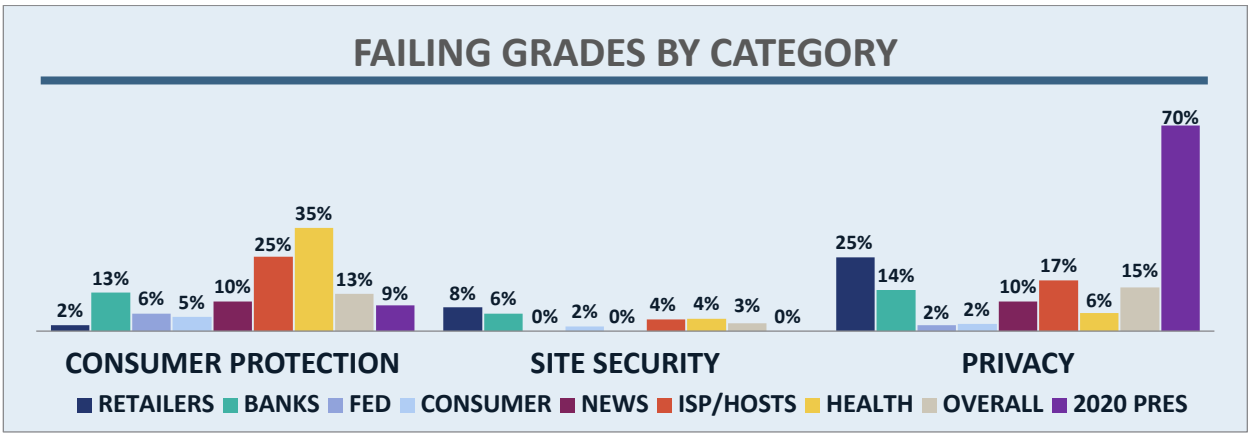


Figure 4 – Percent of Organizations with Failing Grade by Sector and Category

Average Baseline Scores

Figure 5 below shows the average baseline score (out of 100) in each main category by sector. As expected, the 2020 campaigns' scores are near the top in site security, likely primarily due to their new and straightforward server infrastructures. Given that email authentication (mechanisms to help recipients verify the sender of the message) is integrated into most modern email services, average consumer protection scores for campaigns are lower than expected, but can be attributed to two campaigns that have no email authentication at all – if those are removed, the average jumps to 88.

The average campaign privacy score of 57 highlights the weakness in that category. Given that the failure bar is 60, it is easy to see why so many campaigns failed in this area. By contrast, the average score was 70 in other audited sectors. Since campaign websites use very few trackers, the low privacy scores are reflective of their privacy statements, which generally allow free sharing of data with unidentified third parties.

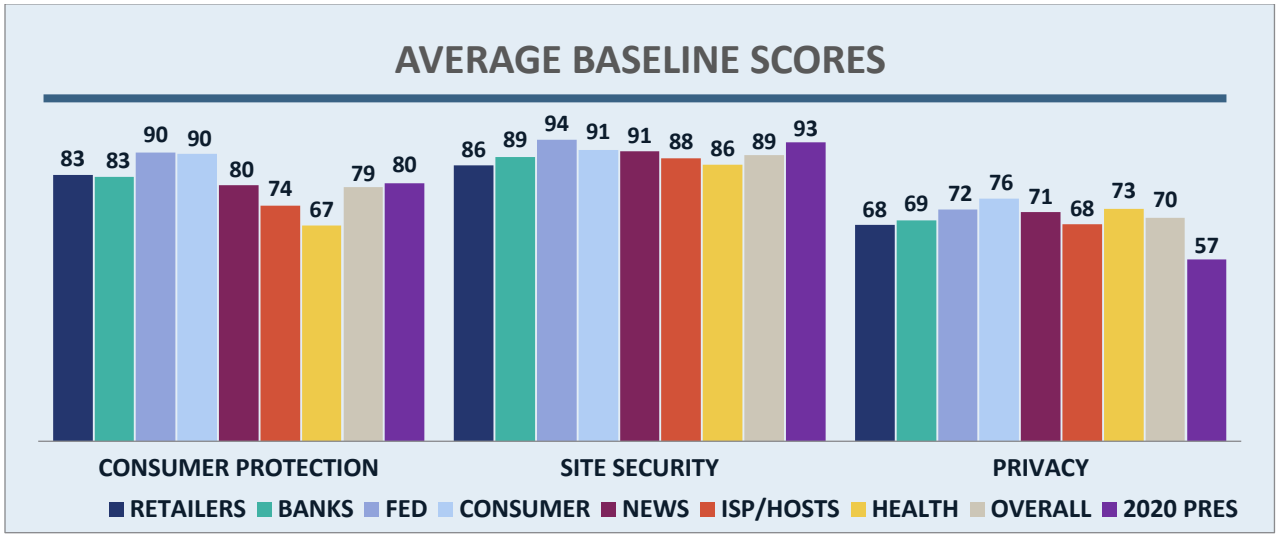
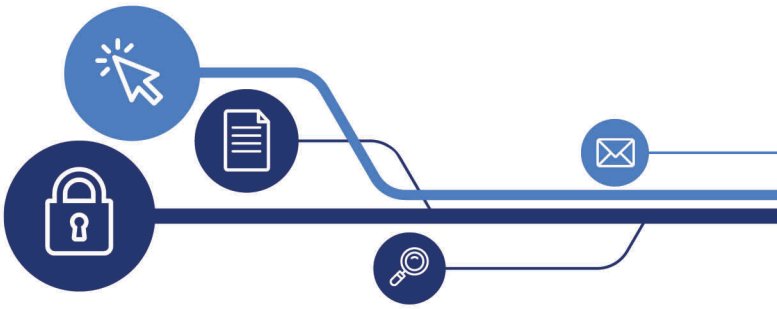


Figure 5 – Major Category Scores by Sector



Though this may be understandable in the context of sharing data within political parties, it is still concerning since there are few stated limits regarding sharing of data with third parties, regardless of their affiliation. This specific issue is the cause of the 70% failure rate.

Privacy Practice Findings

Summary Results

Explanation of the recommended best practices and associated assessment for privacy can be found in Appendices A and B. As shown in Figure 6, the 100-point baseline score for privacy is divided into 55 points for the content of the *privacy statement* (data sharing, data retention, notice of data sharing, and binding of third-party vendors' use of data) and 45 points for *third-party tracking* on the site (fewer trackers is better, and points are deducted for presence of third-party trackers known to freely share data). The average campaign site score for the privacy statement portion was 13 out of 55, less than half the score of any other sector, and the primary driver of failures. The average campaign score for third-party tracking was 44 out of 45, among the top scores. What caused the low privacy statement scores? There were a variety of reasons:

- **Lack of Privacy Statement –** Four campaigns had no discoverable privacy statement. This yields a statement score of 0 and is an automatic failure. This may be an oversight, but is inexcusable since every campaign website is collecting data. Fortunately, it can be remedied quickly by adding a privacy statement.
- **Inadequate Statement –** Many campaign privacy statements were silent on the issue of data sharing, retention, etc. so they did not give clear notice and transparency about their practices. Such disclosures are generally accepted best practice.
- **Freely Sharing Data –** Several privacy statements said they could share data with "like-minded entities" or unidentified third parties, effectively putting no limits on the use of personal data.

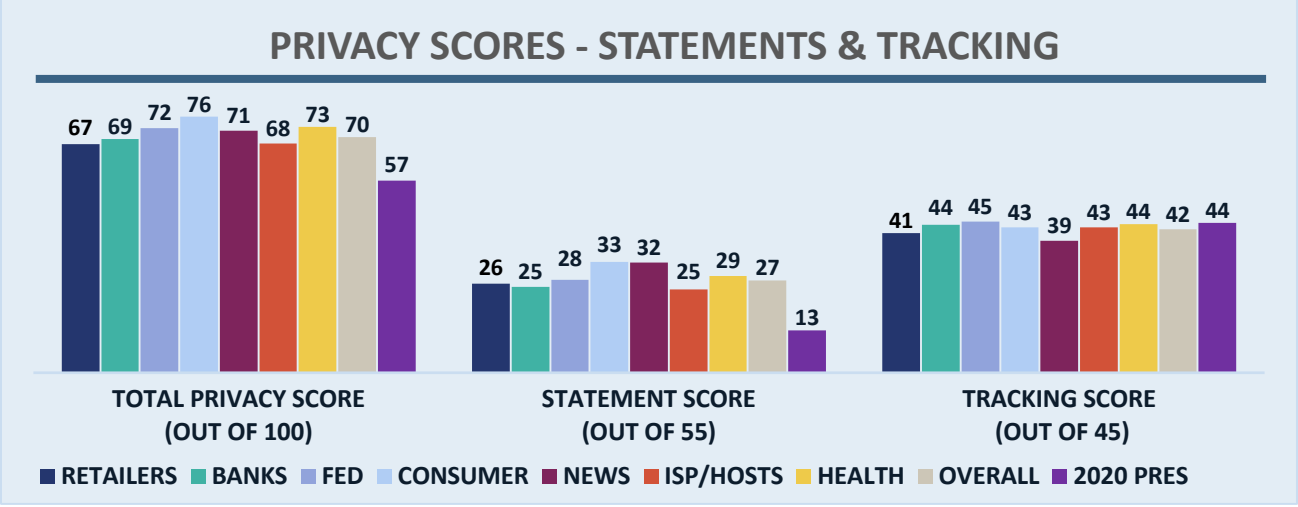
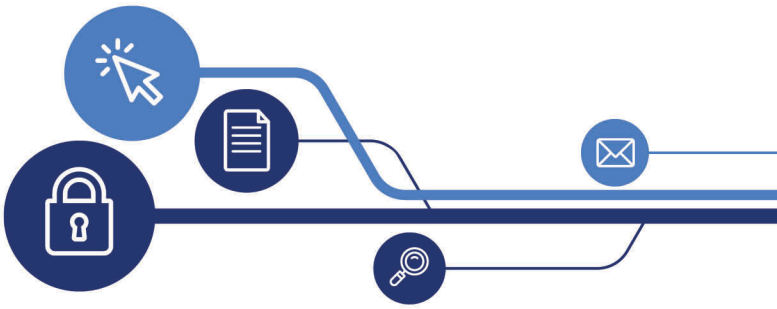


Figure 6 – Privacy Statement and Tracking Scores by Sector



Of the campaign sites that failed in privacy, there were some common scoring tiers. As mentioned, four sites had no privacy statement at all. Eight sites scored bare minimum points by having a privacy statement linked from the home page and placing a date stamp on that statement. Four sites earned a few additional points by layering their privacy statements or addressing issues such as data retention. The most common statement regarding data sharing was that it could be shared with "like-minded" organizations, which is in contrast to current generally accepted practices in the U.S. and directly counter to newer regulations such as the General Data Protection Regulation (GDPR) in the European Union and the California Consumer Privacy Act (CCPA), which goes into effect in 2020.

The remaining seven sites had passing scores in privacy, and these campaigns were the only ones to earn Honor Roll status. They earned passing grades by outlining restrictions in their sharing of data, whether directly or via sharing with third parties. However, even these campaigns barely cleared the bar – all but one of these sites had privacy scores between 60 and 70. There is significant room for improvement for all campaigns in disclosing to website visitors what personal data is being collected, for what purpose, who it will be shared with (and why), and how long it will be retained.

To remedy the low privacy scores, campaigns should implement a privacy statement (if absent), openly state their data sharing practices (if silent), restrict data sharing to only the third parties necessary for the proper operation of their site and services, and require those third parties to adhere to the same restrictions and protections as the campaign itself. While widespread sharing of voter data is known to be quite common within political parties, campaigns should recognize that voters may not want their information shared in such a manner, and may not even be aware of these practices. Campaigns should consider collecting, sharing and retaining less personal information, using more specific and explicit language about their privacy practices, and taking an "opt-in" only approach to sharing.

Data Handling – What Happens to the Data?

Presidential campaigns collect data on website visitors like any other organization OTA assesses in Online Trust Audits. There are, however, some unique aspects to presidential campaigns. For example, if a visitor to the site makes a donation, the campaign is required to collect certain information on that user to properly file with the U.S. Federal Election Commission.[7]

OTA advocates for data sharing that is limited and if personal data is shared the nature and extent of that sharing must be explained clearly in the privacy statement. Here the presidential campaigns did not fare well, as can be seen in Figure 7. Further, only one campaign had a statement expressly stating that they *do not* share data with other organizations. This compares to an average of 67% for other sectors.

[7] Federal Election Commission – Recording receipts https://www.fec.gov/help-candidates-and-committees/keeping-records/records-receipts/

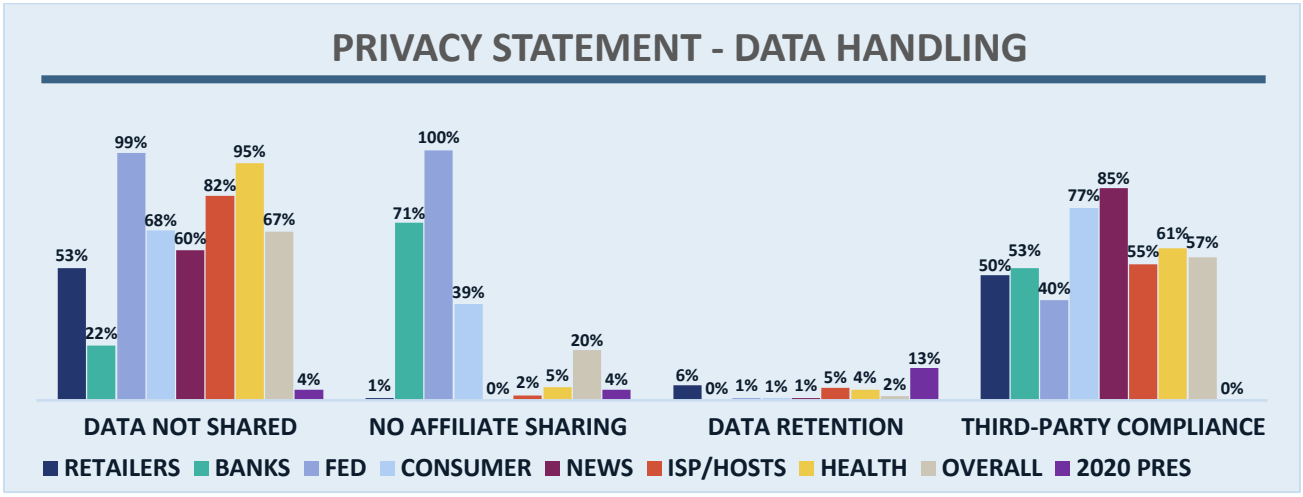


Figure 7 – Privacy Statement Data Handling by Sector

In addition to a lack of disclosure about data sharing, many had a sharing statement like this:

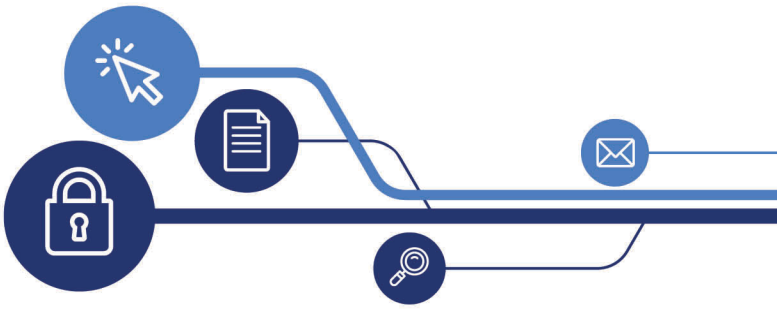
> *"….with candidates, organizations, campaigns, groups or causes that we believe have similar political viewpoints, principles or objectives;"*

The open-ended nature of a statement like this is different than what we generally see in other types of organizations, or as recommended in privacy best practice. Language like this is so broad that essentially it conveys to a user that the campaign may share personal data with any organization.

Statements like this are also troubling because they don't precisely define categories of third parties, which many privacy laws around the world require.[8] [9] For example, if a campaign shares personal data with a payment vendor it should disclose that in the privacy statement, ideally naming the specific vendor or vendors. None of the campaigns had a statement like this. There was also very low adoption of this among other organizations in the broader Online Trust Audit (less than 1%). While these campaigns, like most organizations in the Audit, are not necessarily held to global standards since they are in the U.S., OTA still advocates this as a good way to help users understand where their data is going and how it might be being used.

Another concerning finding regarding data handling is that no campaigns had language saying they hold third-party vendors to at least the same standards laid out in their own privacy statements. This is shown in the rightmost cluster of bars in Figure 7 and is a stark contrast to the 57% of organizations in other sectors that have such language. Given that campaigns work with many vendors to provide services such as polling, this practice is important to assure users their data is being handled correctly by third parties.

[8] General Data Protection Regulation (GDPR) https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en
[9] Brazilian General Personal Data Protection Act (LGPD) http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2019/Lei/L13853.htm#art1



Presidential campaigns may collect data in similar ways to other organizations, but because of their short duration, they are unique in another area OTA advocates: data retention. Compared to a company or a government organization, most campaigns start and end quickly, but they collect similar data that should be disposed of appropriately when it is no longer needed for the purposes of the campaign. Given this fact, it is important that campaigns explain their data retention policies, consider their users' expectations, and apply a data minimization approach to collection, sharing and retention.

The bar for the Online Trust Audit is that privacy statements have some language addressing data retention, but we do not require it to be specific. The bar, however, is far higher in laws like GDPR in the European Union or CCPA in the California, due to come into effect on 1 January 2020. Interestingly, as shown in Figure 7, just 13% (three) campaigns have such language, outscoring all other audited sectors (which average 2%).

In addition to personal data collected directly by an organization, OTA advocates that organizations be transparent if they are collecting data from other sources. Given that campaigns work with many different organizations during their run this is particularly important, and 70% of the campaigns (vs 43% of other sectors) had language stating that they also use data they get from third parties (polling data is a good example of this for campaigns).

Clearly campaigns are collecting, storing, and sharing personal data. That data also needs to be protected. In the Audit, we checked to see if privacy statements included language informing users that their data is being protected with the latest security technologies – 61% of campaigns had language along these lines (far short of the 85% seen in other sectors).

Contacting the Organization – What are the Options?

After informing users how their data is being collected and shared, campaigns need to inform users how they can contact the campaign and what options they have regarding their data. An aspect that was measured for the first time in this year's Audit revolves around users understanding what data organizations have about them and how to contact organizations about that data.

The U.S. presidential campaigns actually fared well in offering users a way to contact them – 78% had a point of contact listed in the privacy statement. Where they lagged, however, was in explaining what users could request regarding their data. Just 13% of campaigns had language about what information users could request about their data, and none had language about users being able to request their data be deleted.

Readability – Navigating and Understanding

Clearly the information in privacy statements is important. However, even if the statement contains all the important information, users must be able to understand what they are reading. Several of OTA's best practices cover the general concept of "readability." The goal is not only to make sure all the information users need is in the statement, but that it is conveyed in an easily accessible way.

Two criteria in the Audit deal with how the content is formatted. First, OTA recommends the use of "layered" notices to help users navigate privacy statements. This can be done with something as simple as a table of contents or something more complex like an interactive statement with links. As shown in Figure 8, just 26% of campaigns had a layered statement of any kind, roughly half of what was seen in other sectors.

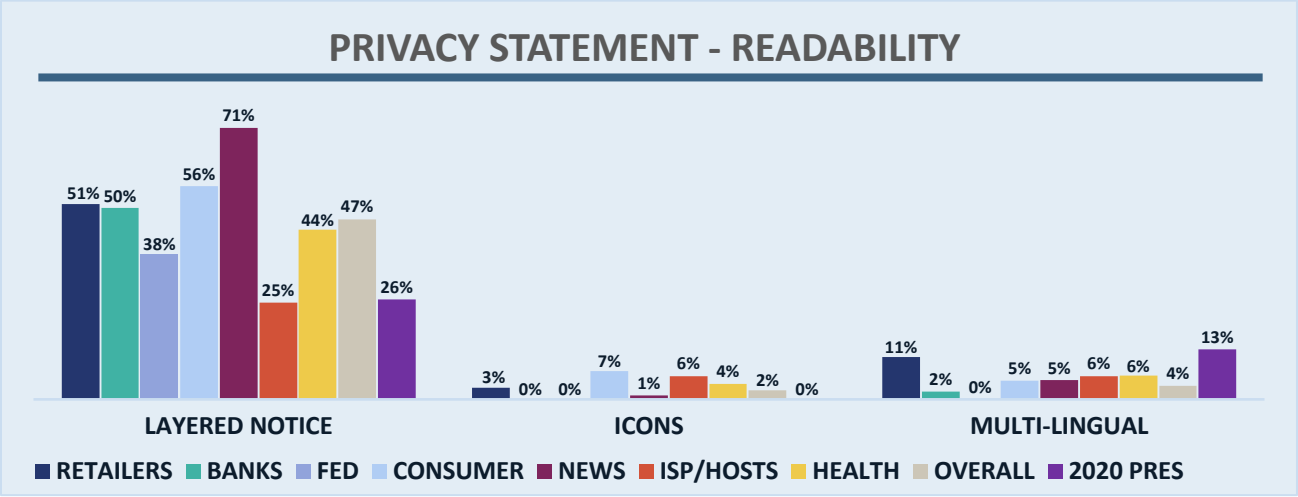


Figure 8 – Privacy Statement Readability by Sector

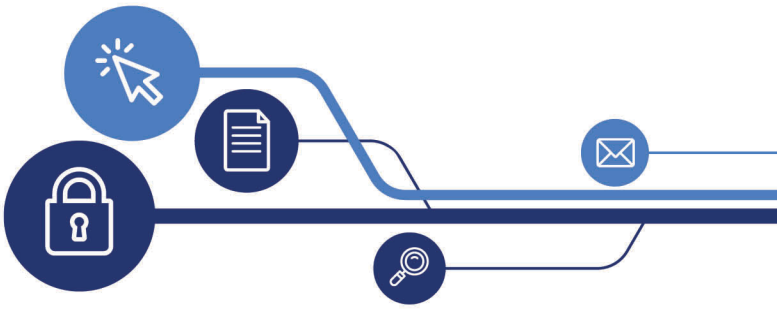
Second is the use of icons, which help readers understand what they are reading and also assists readers of varying degrees of literacy. Here again Figure 8 shows that campaigns did not fare well since none of them used icons.

OTA also advocates that statements be available in multiple languages. Figure 8 shows that just 13% of campaigns made their statements available in multiple languages (all Spanish). Though low, this is higher than other sectors, which average 4%.

Another criterion OTA added in this year's Audit was the general concept of "readability." GDPR, and many other privacy laws around the world, require that statements be readable at certain reading levels. OTA analysts found that 22% of campaigns had statements that were readable (vs 32% for other sectors). One side note is that analysts noticed many of the statements look extremely similar, clearly drawing from a common template. This is part of the reason few campaigns had readable statements – many were obviously using the same structure, and in some cases the same language.

For example, the paragraph below appeared word-for-word in ten of the campaigns' statements:

> *"We may change this Privacy Policy from time to time. If we make changes, we will notify you by revising the date at the top of the policy and, in some cases, we may provide you with additional notice (such as adding a statement to our homepage or sending you an email or mobile notification). We encourage you to review the Privacy Policy whenever you access the Sites to stay informed about our information practices and the ways you can help protect your privacy."*



To be clear, there is nothing wrong with using a template for a privacy statement, but it does not give flexibility to campaigns to differentiate their privacy practices. In addition, this particular statement puts the onus on the user, rather than on the campaign, to proactively check the privacy statement. Using archives or statements of changes would be a much more efficient way to notify users of changes (see the section below for findings on date stamps and archives).

This presents an opportunity for political organizations to come together and develop an "industry-standard" of privacy best practices that all campaigns should follow.

Transparency – What Has Changed?

Another key way to inform users about the status of a privacy statement is to ensure there is a date stamp. OTA advocates putting the date stamp at the top. As seen in Figure 9, 39% of campaigns had a date stamp at the top (4% had it at the bottom), which is under the 47% overall average across other sectors. This still leaves more than half the campaigns with no date stamp at all. This is a simple way to inform users regarding how up to date the information is.

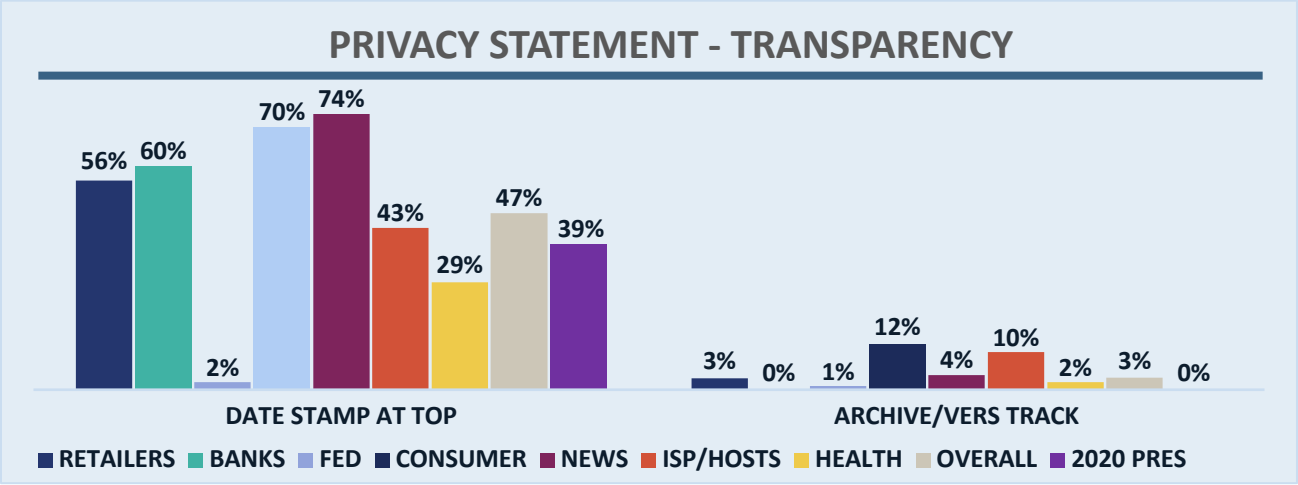
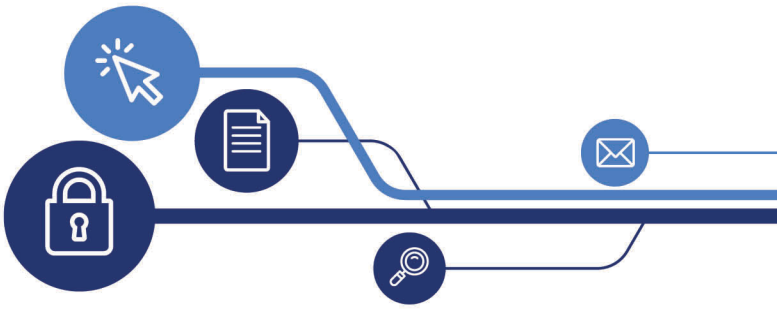


Figure 9 – Privacy Statement Transparency by Sector

A related best practice is the use of archives, or some way for users to see what was in prior privacy statements, and therefore what has changed over time. As seen in Figure 9, perhaps unsurprisingly none of the campaigns offer access to prior versions of the privacy statement, though two did update their privacy statement during the data collection period. An archive would allow users to easily see what those changes were. An even better approach would be to highlight the specific changes that were made and why.

A final transparency related element is private WHOIS registrations. This is an area of concern due to the transparency issue of domain ownership (discoverable via a WHOIS lookup).[10] More than four-fifths (83%) of

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

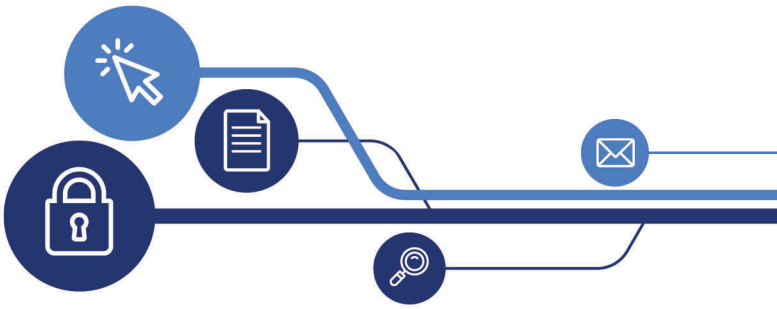


campaign sites have a private registration, which is nearly four times higher than other sectors. It is understandable that the domains may have originally been registered privately (before the campaign was launched), but this should be changed once the sites are public. Given the preponderance of fake or alternate sites using candidates' names as part of the domain name, this lack of transparency compounds the problem, so public registration is a simple step campaigns can take to increase trust and lead by example. An added reason for making the information public is that campaigns are involved in matters that are in the public interest, namely government elections.

Site Security Findings

This category scores the use and configuration of server security, data encryption for website sessions, and other site protections, as well as discovery of known vulnerabilities on the website. Explanation of the recommended best practices and associated assessment for site security can be found in Appendices A and B. As illustrated in the middle set of bars in Figure 5, campaign sites outperformed all but the U.S. federal government in the baseline scoring for this category, which again is not surprising given their straightforward and recent infrastructure. Specific findings for various best practice recommendations were as follows:

- **Optimized SSL/TLS –** Using public assessment tools from Qualys SSL Labs and ImmuniWeb, all sites earned an "A" or "A+" in this area, and had trusted certificates as well as certificate transparency.
- **TLS 1.3 –** This is the latest encryption protocol, and is supported by 58% of campaigns, more than five times the rate of any other sector.
- **AOSSL –** Adoption of this key best practice, which encrypts the entire web session between a client and server, was 100% among campaigns, matching U.S. federal government sites for the highest rate. Given that citizens are submitting personal information and making donations on campaign sites, this is an important practice.
- **Certificate Authority Authorization (CAA) –** this is a relatively new capability that allows domain owners to declare which certificate authorities are allowed to issue certificates on their behalf. No campaign sites support it (vs 6% across other sectors).
- **Web App Firewall –** 58% of campaign sites have implemented a web application firewall, which is under the overall average of 71% for other sectors. Given that these sites are new, adoption should be higher.
- **Vulnerability Reporting Mechanism –** None of the sites had a means to report security vulnerabilities, and though it is not as common to see this for "informational" sites, it is still important to provide a means for security researchers and others to report vulnerabilities. In the broader Audit, 9% of news/media sites and 11% of organizations overall support such a mechanism either directly or through bug bounty programs.
- **Other Elements –** Malware was not detected on any campaign sites (vs 2% across other sectors). None were on IP blacklists. Two sites (8%) had outdated software. None had reported cross-site scripting (XSS) vulnerabilities (vs 21% in other sectors).



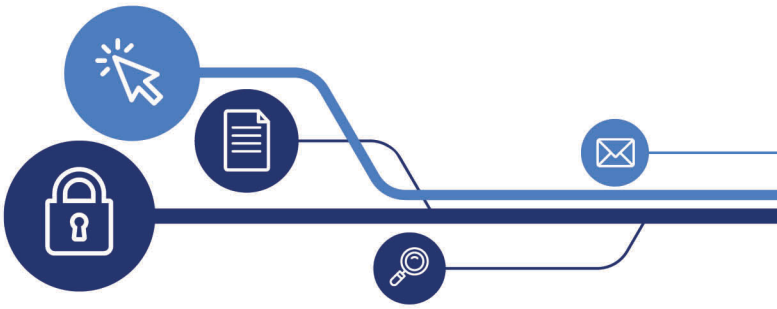
Consumer Protection Findings

Explanation of the recommended best practices and associated assessment for consumer protection can be found in Appendices A and B. This category scores the adoption of email authentication and associated technologies to help protect consumers from phishing (fraudulent email purporting to come from a known entity). 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 Internet Service Providers (ISPs) and email systems to reject or quarantine forged email. Finally, opportunistic Transport Layer Security (TLS) encrypts sessions between mail servers to prevent fraud and eavesdropping in transit.

As seen in Figure 5, campaigns scored slightly higher than the overall baseline scoring average in this category (80 vs 79). This is surprising given that most utilize current email services, which generally incorporate email authentication capability. In general, adoption was strong, though two campaigns had no email authentication at all and therefore failed in the consumer protection category (they also failed in the privacy category). In the Audit of 2016 presidential campaigns, no campaigns failed in consumer protection, so this is actually a step back. Specific results for key best practice recommendations were as follows:

- **SPF and DKIM –** Adoption of the recommended best practice of using both SPF and DKIM at the top-level domain (TLD, the domain of the website) was 87%, well above the average of 76% for other sectors. Use of SPF at the TLD was 87%, slightly under the average of 89% for other sectors, while use of DKIM at the TLD was 91%, above the average of 83% for other sectors. Though these results are solid, the fact that two campaigns have no email authentication is disappointing given the spotlight on phishing during the 2016 presidential campaign (where the chair of Hilary's Clinton's 2016 campaign enabled the hack of the Democratic National Committee by falling for a phishing message), and the fact that campaigns have the ability to use the latest email services.[11]
- **DMARC –** 61% of campaigns had a DMARC record (vs 51% for other sectors) and 30% use DMARC "enforcement", a policy of "reject" or "quarantine" for messages that fail authentication (vs 24% for other sectors). This is a major improvement from the Audit of 2016 campaigns, where only one campaign supported DMARC. Given that campaigns are using current email services and the significant concern about phishing in the political realm, all should be using DMARC.
- **Opportunistic TLS –** Use of opportunistic TLS is 87%, well above the overall average of 73% for other sectors.
- **IPv6 –** Campaign sites far outpaced other sectors – 74% vs 12% – likely due to their newer infrastructure.
- **Domain Locking –** All but two have locked their domain. This is a simple issue that should be addressed immediately to help prevent unauthorized domain transfer.

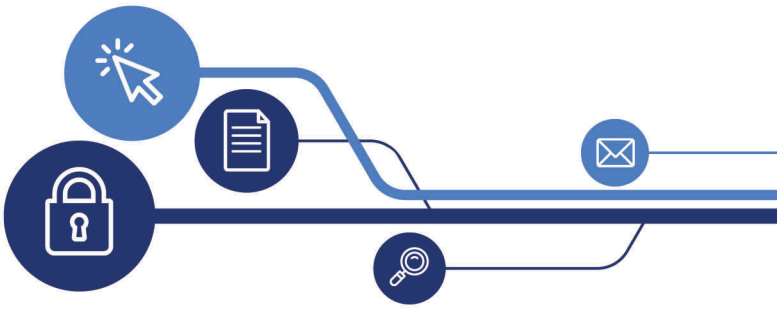
[11] Inside story: How Russians hacked the Democrats' emails, AP, 4 November 2017 https://apnews.com/dea73efc01594839957c3c9a6c962b8a



Comparing Campaign Results – 2020 vs 2016

After examining the findings for the 2020 campaigns, it is useful to take a look back and see how they compare to the findings for the 2016 campaigns. These are the highlights:

- **Overall results**
  - 2020 campaigns had slightly better Honor Roll results – 30% vs 26% for 2016 campaigns. These are based on small samples (23 in both 2020 and 2016).
  - Failure rates were slightly lower – 70% of 2020 campaigns had a failure vs 74% of 2016 campaigns.
- **Privacy**
  - This was by far the weakest area, and the cause of high failure rates for both 2020 and 2016 campaigns, which is surprising given the increased attention on privacy over the last four years.
  - Overall, privacy scores were similar (lagging all other sectors), and the low scores were largely driven by broad data sharing language in the privacy statements.
  - Use of layered notices improved (26% vs 0%), support for multi-lingual statements dropped (13% vs 21%), and use of private domain registrations jumped significantly (83% vs 44%).
- **Site security**
  - Scores were at or near the highest of all sectors for both 2020 and 2016 campaigns.
  - Significant growth was seen in support for "always-on SSL" (100% vs 70%), and use of a web application firewall (58% vs 35%).
- **Consumer protection**
  - 2020 campaigns actually took a step back compared to the 2016 campaigns – two 2020 campaigns had no email authentication at all and thereby failed the category, while all 2016 campaigns had passing scores.
  - SPF and DKIM support at top-level domains swapped places – SPF dropped from 91% to 87%, while DKIM grew to 91% from 78%.
  - DMARC adoption was a bright spot, growing from 4% to 61%, and DMARC records with "enforcement" grew from 0% to 30%.
  - Use of opportunistic TLS for email also grew significantly, from 57% to 87%.



Conclusion

Overall, we found that 2020 U.S. Presidential campaigns have strong site security, reasonable consumer protection, and poor privacy statements that allow free sharing of data. The excellent site security scores are no surprise given the use of current hosted services by the campaigns. The lack of email authentication or poor implementation by several campaigns is a surprise since these are long-established best practices and all the campaigns audited four years ago fully implemented email authentication. Privacy – especially the free sharing of data – remains the biggest concern and was the cause of failure for seven in ten campaigns.

We encourage all campaigns to remain vigilant regarding site security, monitoring and configuring their sites to address new exploits or vulnerabilities as they emerge. Though we have not yet seen a widespread breach of campaign data, they are prime targets for those seeking to monetize the data or undermine trust in the political system.

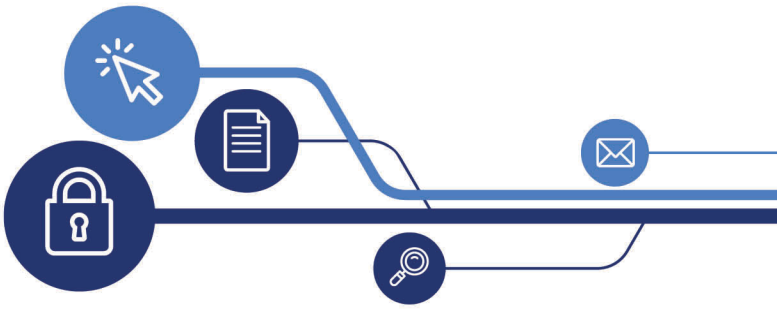
Consumer protection – specifically email authentication – is important to maintain trust in campaign communication and prevent unsuspecting users from falling victim to malware, ransomware, and phishing. We encourage all campaigns to fully implement SPF and DKIM, and to implement DMARC at an "enforcement" level.

As outlined, the campaigns' published privacy statements (and for some the lack of a statement altogether) raise significant concerns. Disclosing that data may be shared with "like-minded" organizations may be a common practice for campaigns, but is still concerning in light of the depth of demographic and financial information being collected. Since even campaigns who made the Honor Roll had poor privacy scores, OTA calls on all campaigns to consider updating their statement and practices to better reflect consumer concerns pertaining to the collection, use, retention and sharing of their personal information.

Last but not least, all campaigns need to be prepared for a breach and develop a comprehensive breach readiness plan. 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 campaigns should be afforded the same level of protection.

The following appendices detail the list of recommended best practices in each category, the methodology and scoring used in the Audit, and the complete list of audited campaigns.

Let's work together in a bipartisan effort to enhance online security and privacy.



Appendix A – Recommended Best Practices

Privacy, Transparency & Disclosures

The 2018 Audit showed modest increases in the transparency and readability of published privacy statements, with clear room for improvement. More statements are presented in a layered manner, disclosures are more complete and language is shifting toward more consumer-friendly wording instead of a contract written for a legal audience. Some of this may be the result of increased awareness of, and compliance with, the EU's General Data Protection Regulation (GDPR).

With the advent of GDPR it is more important than ever for organizations to embrace data stewardship. In addition, organizations need to be aware of other regional transborder rules such as the APEC Cross-Border Privacy Rules System. These are a set of voluntary yet enforceable privacy standards to allow data to flow across the Asia-Pacific region.[12] In 2020, the California Consumer Privacy Act (CCPA), which is largely modeled after the GDPR principles, will also go into effect, forcing U.S.-based organizations to implement additional privacy protections if they wish to engage in the largest market in the U.S.[13] OTA has been advocating for increased transparency and discoverability of privacy statements since 2009, including recommending disclosure of data collection, usage, sharing and retention practices. Best practices include:

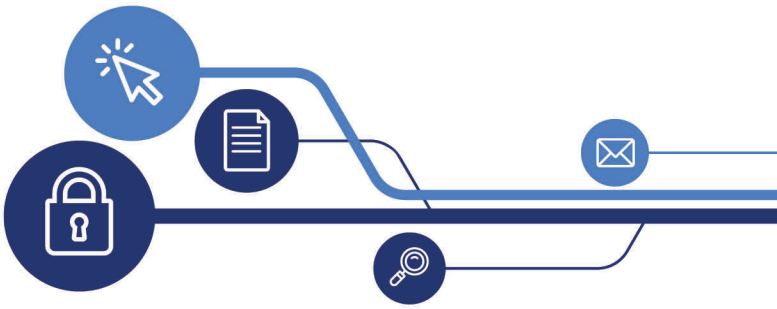
Basic notice/disclosure items

- Make sure the privacy statement has a link and is easily discoverable from the home page.
- Place the revision date of the statement at the top of the page.
- Provide access to archived versions of the statement, allowing users to see what has changed.
- Use a simple layered and/or short notice designed to help consumers understand the statement.
- Use icons to help consumers navigate privacy statements in conjunction with layered/short notices.
- Write statements for the site's target audience and demographics. Consider providing multi-lingual versions supporting non-English-speaking site visitors.

Clearly state key compliance policies

- Compliance with Children's Online Privacy Protection Act (COPPA) or related regulations.[14]
- Disclose whether the site honors Do Not Track (DNT) browser settings and preferably honor users' DNT browser settings [note: this will be removed from the Audit starting in 2020].
- Provide a summary of the data retention policy, including a specific timeframe and for what reason data is retained.

[12] APEC Cross-Border Privacy Rules http://www.cbprs.org/
[13] California Consumer Privacy Act https://en.wikipedia.org/wiki/California_Consumer_Privacy_Act
[14] COPPA https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions



Protect privacy and define protected sharing

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

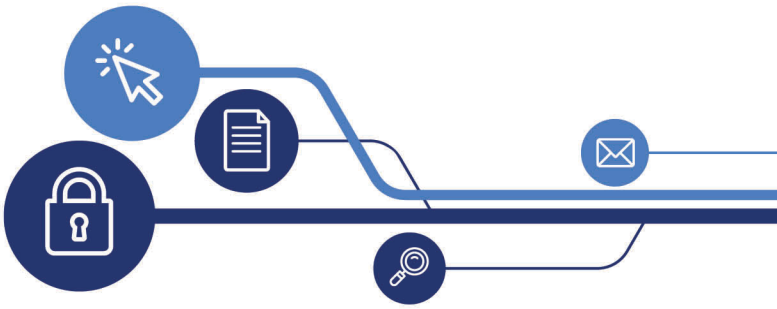
Site, Server & Infrastructure Security

A site's trustworthiness is largely defined by the security of the infrastructure as well as its associated privacy practices. Users need assurance that the site and its data are secure. Proper implementation of best practices in this category also protects the site itself from attack. The 2018 Audit has been expanded with deeper evaluation of DNS health, IP reputation, application security and patching cadence. In addition, the bar was raised this year in server security scoring by combining results from ImmuniWeb, Qualys SSL Labs, Mozilla's Observatory and Sucuri's SiteCheck. Best practices include:

- Optimize SSL/TLS implementation using information gleaned from public tools, focusing on vulnerabilities that earn a letter grade of "F" or that have failure (60 points or less) in a major subcomponent of the scoring (which normally leads to an overall grade of "C").[15] [16] This includes eliminating use of insecure ciphers and older, insecure protocols as well as vulnerabilities to the POODLE and ROBOT exploits.[17]
- Implement content security policy and associated headers for third-party content used on the site. This can prevent vulnerabilities introduced by outside content.[18] [19] [20]
- Review capabilities of certificate authorities to ensure that they meet your support requirements. Use EV SSL certificates for classes of sites that are frequently spoofed and where users need to be assured they are visiting and browsing a legitimate site.
- Implement Certification Authority Authorization (CAA) to prevent issuance of unauthorized certificates.[21]

---

[15] ImmuniWeb SSL Test https://www.immuniweb.com/ssl/
[16] Qualys SSL Labs https://www.ssllabs.com/projects/documentation/
[17] DROWN (Decrypting RSA with Obsolete and Weakened eNcryption) https://drownattack.com/
[18] ImmuniWeb Website Security Test https://www.immuniweb.com/websec/
[19] Observatory by Mozilla https://observatory.mozilla.org/
[20] Sucuri SiteCheck https://sitecheck.sucuri.net/
[21] CAA Overview https://blog.qualys.com/ssllabs/2017/03/13/caa-mandated-by-cabrowser-forum



- Implement HTTP Strict Transport Security (HSTS), also referred to as Always on SSL (AOSSL) or HTTPS everywhere, on all pages to maximize data security and online privacy. HSTS helps ensure that all data exchanged between the site and device is encrypted.
- Implement a Web Application Firewall to monitor HTTP conversations and block common attacks such as cross-site scripting (XSS) and SQL injections.
- Proactively scan sites for malicious links, iFrame exploits, malware and malvertising.[22]
- 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.
- Provide a discoverable and accessible vulnerability reporting mechanism for site visitors and third parties to report vulnerabilities.

Domain, Brand & Consumer Protection

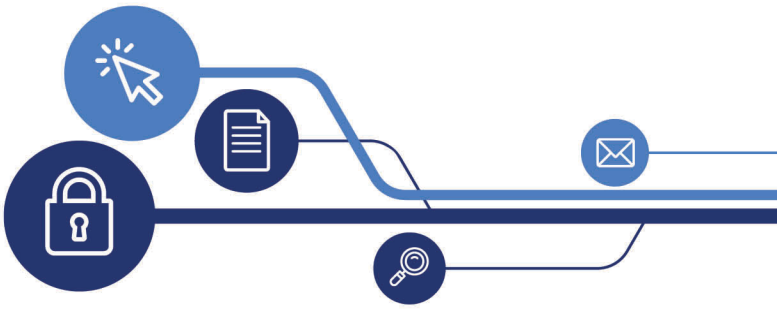
By utilizing email authentication (SPF and DKIM), organizations can help protect their brands and prevent consumers from receiving spoofed and forged email. Email authentication allows senders to specify who is authorized to send email on their behalf. Building on email authentication protocols, DMARC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

IPv6 expands the number of unique IP addresses, thereby supporting the growth of the Internet, including demand for new IP addresses driven by IoT.[23] [24]

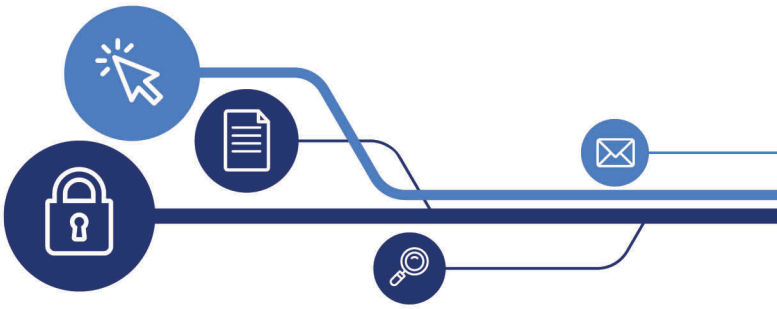
Best practices include:

- Implement both SPF and DKIM for top-level domains, "parked" domains (not used for email) and any major subdomains seen on websites or used for email.
- Optimize SPF records with no more than 10 DNS lookups.
- Implement DMARC, initially in "monitor" mode to get receiver feedback and verify accuracy of email authentication, and eventually to assert a "reject" or "quarantine" policy to receivers.
- Mandate the use of DMARC reporting capabilities with RUA (aggregate) and RUF (message-specific forensic) reports.
- Implement inbound email authentication checks and DMARC on all networks to help protect against malicious email and spear phishing purporting to come from legitimate senders.

[22] OTA Advertising & Content Integrity https://www.internetsociety.org/resources/ota/2017/advertising-content-integrity/
[23] Why You Need IPv6 https://www.infoblox.com/solutions/ipv6-readiness
[24] IPv6 Security https://www.internetsociety.org/deploy360/ipv6/security/



- Implement opportunistic TLS to protect email in transit between mail servers.
- Ensure that domains are locked to prevent domain takeovers.
- Implement DNSSEC to help protect a site's DNS infrastructure.
- Deploy IPv6.
- Implement Distributed Denial of Service (DDoS) mitigation technologies and processes.
- Implement multi-factor authentication.



Appendix B – Methodology & Scoring Criteria

The Audit criteria and methodology evolve every year, reflecting developments in security standards, privacy norms and real-world deployment. OTA actively solicits input from the Internet at-large through a 60-day call for public comments.[25] In addition, several U.S. government agencies and industry standards organizations are consulted. After review, the OTA Trust Audit Planning Committee incorporates some of the core security and privacy directives, including Fair Information Practice Principles (FIPPs), NIST standards, and those supported by the Internet Society's Deploy360 Programme.[26] Reflecting this combined input, weighting and scores are re-examined annually and re-allocated to address the evolving threat landscape, regulatory environment and ease of deployment. The end result focuses on accepted best practices reflecting real-world deployment, bridging the gap between the standards and business communities. The final methodology for this year's Audit was published in August 2018 and promoted broadly to provide organizations the ability to re-evaluate their practices and optimize their scores.[27]

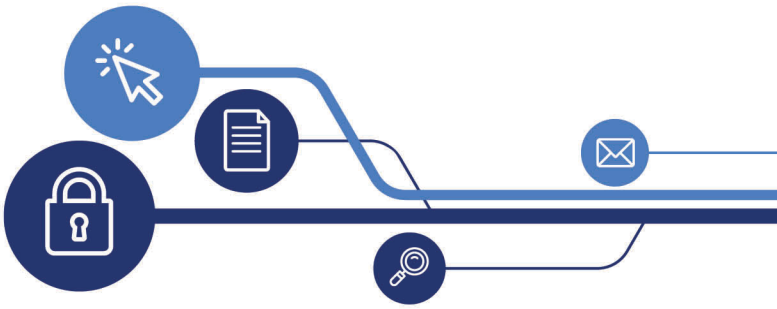
The Online Trust Audit includes a composite analysis focusing on three major categories:

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

Sites were eligible to receive 300 base points (up to 100 points in each category), and up to 60 bonus points (20% of the base score) for implementing emerging best practices. Additionally, organizations could lose points for having regulatory settlements, data breaches, observed vulnerabilities and other key deficiencies. To qualify for the Honor Roll, sites had to receive a composite score of at least 80% of the baseline points *and* **a score of at least 60** in each of the three main categories. The failure bar was raised to 60 in 2017, recognizing that "security is only as strong as the weakest link" and sites are built on a "chain of trust".

The 2018 Audit has been powered by technical analysis and data provided from more than a dozen organizations. Data sampling was initiated the week of 19 August 2019, tracked bi-weely and verified again on 26 September 2019. Advance copies of the report were sent to campaigns the week of 30 September, and any updates were evaluated on 7 October. Organizations providing data directly or through public tools included Agari, Disconnect, dmarcian, ImmuniWeb, Infoblox, Internet.nl, Microsoft, Mozilla, Qualys SSL Labs, Sucuri, Symantec, Valimail and Verisign. Additional data was obtained from public data sources including BugCrowd, Google, HackerOne, Open Bug Bounty, Twitter and others. It is important to note that a site's configuration or practices may have changed since the sampling and the data only reflects findings during this snapshot in time.

[25] Call for comments press release: https://www.internetsociety.org/news/press-releases/2017/ota-requests-public-comments-for-2018-online-trust-audit-methodology/
[26] Internet Society Deploy360 Programme https://www.internetsociety.org/deploy360/
[27] August 23, 2018 methodology press release https://otalliance.org/news-events/press-releases/internet-society%E2%80%99s-online-trust-alliance-announces-methodology-tenth



Privacy, Transparency & Disclosures

Best practices for all organizations include providing users with clear notice, transparency and control of the data being collected, tracked and shared with third parties. The privacy score is comprised of up to 100 points covering: inclusion of appropriate disclosures; structure of the privacy statement itself (including adoption of generally accepted Fair Information Practice Principles (FIPPS)); and tracking and third-party data collection.[28] Privacy statements were read and scored by OTA/Internet Society analysts.

Privacy Statement – 55 points possible. Sites can receive maximum scores by adhering to the following guidelines:

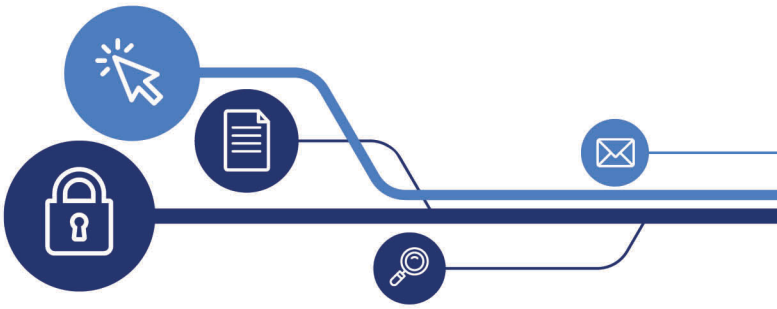
- Link / discoverability from the home page
- Date stamping of privacy statement on the top of the page
- Disclosure regarding handling of browser Do Not Track (DNT) setting
- Data retention policy statement with a specific timeframe reference (timeframe new in 2018)
- Personal data not shared, except with third parties who deliver the service
- Personal data not shared with affiliates or partners (separated from core data sharing in 2018)
- Vendor compliance – disclosure that service providers must comply with the organization's privacy statement and are prohibited from the use or sharing of data for any purposes other than providing services on behalf of the site
- Version tracking (or access to prior versions), including posting of revision mark-ups (was bonus points prior to 2018)
- Designed as a layered and/or short notice
- Compliance with Children's Online Privacy Protection Act[29]

Third-Party Tracking on Site – 45 points possible for sites with no third-party trackers (with the exception of anonymous analytics). Observed trackers known to share data with third parties result in reduced points.[30]

Bonus Points

- Use of consumer-friendly icons to assist navigation
- Localized/multi-lingual statement where English may be a "second language"
- Honoring of a user's Do Not Track browser (DNT) setting

[28] FIPPS https://cryptome.org/2014/11/nstic-fipps.pdf
[29] COPPA https://www.ftc.gov/tips-advice/business-center/privacy-and-security/children's-privacy
[30] Third party tracking data – Primary source includes data from https://disconnect.me/trackerprotection/blocked netting out https://disconnect.me/trackerprotection/unblocked



- Cross device Tracking Disclosures (added in 2017) [31]
- Implementation of tag management systems or privacy solutions to manage third party tags

Penalty Points

- Data breaches – for breaches of more than 1000 records. For the 2018 Audit, the penalty was scaled proportionately with the size of the data breach – *penalty if qualifying incident between June 1, 2017 and December 31, 2018*
- Regulatory settlements with the Federal Trade Commission (FTC), Federal Communications Commission (FCC), Consumer Financial Protection Bureau (CFPB)[32], State or global – *penalty if settlement between June 1, 2017 and December 31, 2018.*
- Public vs. Private WHOIS registration – *penalty if private*

Site, Server & Infrastructure Security

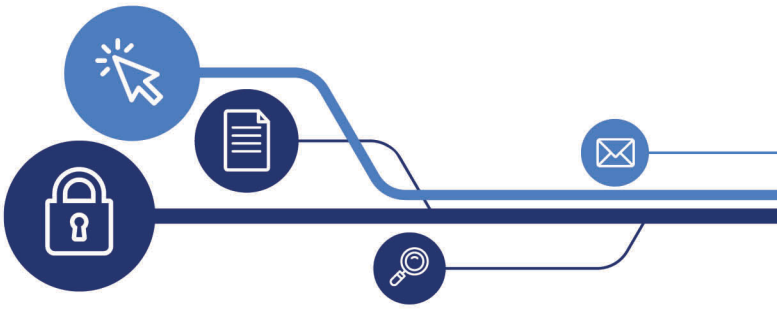
Best practices to secure data in transit and collected by websites, and prevent malicious exploits running against clients' devices. Sites were eligible to score up to 100 base points, provided any single core SSL/TLS criteria (ciphers, key exchange or protocol support) did not score below 60. Sites were tested with several tools to look for known vulnerabilities, HSTS configuration and mismatched certificates. [33, 34] In 2017 server security was expanded to include application security, patching cadence and IP reputation. It was extended further in 2018 to include robust assessments of content security policy and preventions related to third-party content on sites. Support of Always On SSL was incorporated into baseline scoring in 2018.[35]

Bonus / Penalty Points

- Extended Validation SSL Certificates (EV SSL) – *bonus points* [36]
- Certificate Authority Authorization (CAA) – new in 2018 – *bonus points*
- Web Application Firewall – *bonus points*
- Testing for XSS, iFrame exploits, malware, malicious links – *penalty if these threats exist*
- Vulnerability & Bug Reporting Mechanism – Instituted in 2017, sites earn bonus points for reporting mechanisms including online forms and/or using third-party bug bounty reporting. Data was analyzed by online searches using keywords, as well as searching third-party bug bounty programs including HackerOne and Bugcrowd [37] – *bonus points*

---

[31] FTC Cross Device Tracking Recommendations https://www.ftc.gov/system/files/documents/reports/cross-device-tracking-federal-trade-commission-staff-report-january-2017/ftc_cross-device_tracking_report_1-23-17.pdf
[32] CFPB https://www.consumerfinance.gov/
[33] Qualys SSL Labshttps://ota.ssllabs.com/
[34] ImmuniWeb https://www.immuniweb.com/ssl/
[35] AOSSL https://www.internetsociety.org/resources/ota/2017/always-on-ssl-aossl/
[36] EV SSL https://www.internetsociety.org/resources/ota/2017/extended-validation-certificates-evssl/
[37] NTIA Vulnerability Reporting Guidelines and practices https://www.ntia.doc.gov/other-publication/2016/multistakeholder-process-cybersecurity-vulnerabilities

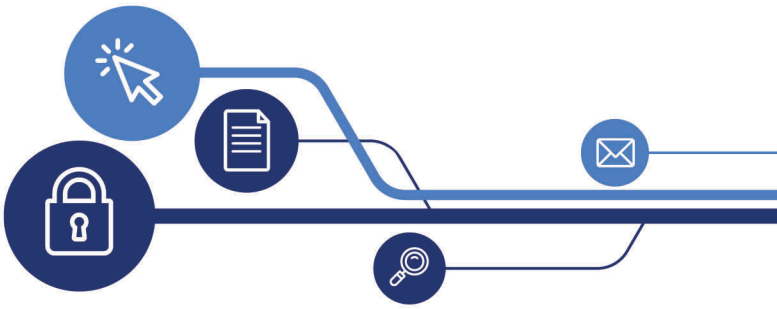


Domain, Brand & Consumer Protection

Email continues to be the top attack vector of choice, driving business email compromise (BEC), credential and identity theft, bank account takeovers and distribution of malware.[38] The FBI reports that BEC fraud has amounted to $12.5 billion in financial losses since 2013, most of which could have been prevented.[39] For the past decade OTA has advocated for end-to-end email authentication to help detect and block malicious and spoofed email for all domains and subdomains managed by an organization. Adoption helps protect consumers and email recipients from distribution of malware, key loggers and related threats including ransomware, cryptomining and account takeovers, while additionally protecting the reputation of the targeted brand.

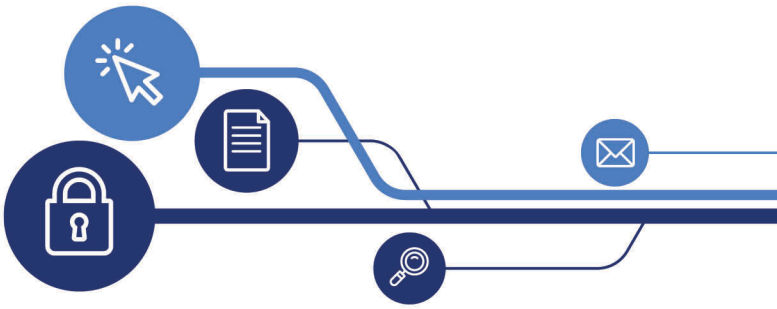
- Email authentication (Sender Policy Framework (SPF) and DomainKeys Identified Mail (DKIM)) at top-level ("corporate") domains, and email subdomains. The 2018 Audit increases weight on authenticating top level domains (most recognizable to the user and most frequently spoofed), with reduced points for separate delegated sub-domains. In addition, sites with invalid SPF records did not receive credit – *part of base score* [40]
- Domain-based Message Authentication, Reporting & Conformance (DMARC). DMARC records where p=none and have no reporting (RUA or RUF) do not receive any credit. Referred to as "naked DMARC records", they do not provide any consumer or brand protection value since receiving networks do not respond to the policy and the brands do not get authentication and abuse reports. Weight was increased on use of the "reject" policy – *part of base score* [41]
- Implementation of "opportunistic" Transport Layer Security (TLS) for email – *bonus points* [42]
- Domain locking – *penalty if domain not locked*
- Domain Name System Security Extensions (DNSSEC) – *bonus points* [43]
- Implementation of Internet Protocol version 6 (IPv6) for web server access – *bonus points* [44]
- Multi-factor authentication – Though multi-factor authentication was awarded bonus points in the 2017 Audit, it was not repeated in this Audit due to insufficient data sources across all sectors.

[38] Verizon Data Breach Investigations Report, page 11 https://enterprise.verizon.com/resources/reports/DBIR_2018_Report.pdf
[39] Business Email Compromise the $12 Billion Scam https://www.ic3.gov/media/2018/180712.aspx
[40] OTA email authentication overview, resources and tools https://www.internetsociety.org/resources/ota/2017/email-authentication-dmarc/
[41] OTA overview of DMARC and resoruces https://www.internetsociety.org/resources/ota/2017/dmarc/
[42] SSL/TLS security and deployment best practices https://www.internetsociety.org/resources/ota/2017/transport-layered-security-tls-for-email/
[43] DNSSEC Basics https://www.internetsociety.org/deploy360/dnssec/basics/
[44] IPv6 https://www.internetsociety.org/deploy360/ipv6/



Appendix C – Best Practice Checklist

DNS, Domain, Brand & Consumer Protection		
❑	Valid SPF records & DKIM at the corporate and sub domains	Base Score
❑	DMARC records with reject/quarantine policy	Base Score
❑	Naked DMARC records (p=none and no RUA or RUF)	Invalid
❑	Opportunistic TLS for email	Bonus Points
❑	Implement DNSSEC	Bonus Points
❑	IPv6 Adoption	Bonus Points
❑	Multi-Factor Authentication	Bonus Points
❑	Domain locked	Penalty for not locking
❑	Inbound email authentication and DMARC checking	Not scored; recommended
Site, Server & Infrastructure Security		
❑	Server Security & Configuration	Base Score – aggregate, multiple tests
❑	SSL/TLS Certificate, Protocol, Key Exchange, Ciphers	Base Score – aggregate, multiple tests
❑	Always on SSL (https by default)	Base Score
❑	Server Patching Cadence	Base Score
❑	Certification Authority Authorization (CAA)	Bonus Points
❑	Certificate Type (EV SSL)	Bonus Points
❑	Web Application Firewall	Bonus Points
❑	Malware, malicious links	Penalty
❑	XSS / iFrame Vulnerability	Penalty
❑	Vulnerability / Bug Reporting Mechanism	Bonus Points
❑	Anti-Bot Protection	Not scored, recommended
❑	DDoS Mitigation Mechanisms	Not scored, recommended
Privacy Statement, Tracking, Transparency & Disclosures		
❑	Link to privacy statement on home page	Base Score
❑	Privacy statement date stamp at top of page	Base Score
❑	Layered short notice design (links/expand sections)	Base Score
❑	Children's Online Privacy Protection Act (COPPA) or related reg's	Base Score
❑	"Do Not Track" (DNT) disclosure	Base Score
❑	Data retention statement	Base Score
❑	Personal data not shared, except to third parties for service	Base Score
❑	Personal data not shared with affiliates/partners	Base Score
❑	Vendors contractually held to privacy statement	Base Score
❑	Archived/prior version of privacy statement available	Base Score
❑	Icons used to clearly identify sections	Bonus Points
❑	Multi-lingual statement option clearly linked	Bonus Points
❑	Honor DNT browser setting	Bonus Points
❑	Disclosure of cross-device tracking	Bonus Points
❑	Disclosure whether data shared for legal purposes	Bonus Points
❑	Notify user if personal data is requested by 3rd party	Bonus Points
❑	Tag Management System (TMS) in place	Bonus Points
❑	Presence of 3rd Party trackers that share data	Penalty, number of trackers
❑	Data breach reported	Penalty, number of incidents, size of breach
❑	FTC/FCC/CFPB/State/International enforcement action	Penalty, number of settlements
❑	Is your WHOIS record Private?	Penalty
❑	Comply with regulations in appropriate jurisdictions (e.g, GDPR)	Recommended



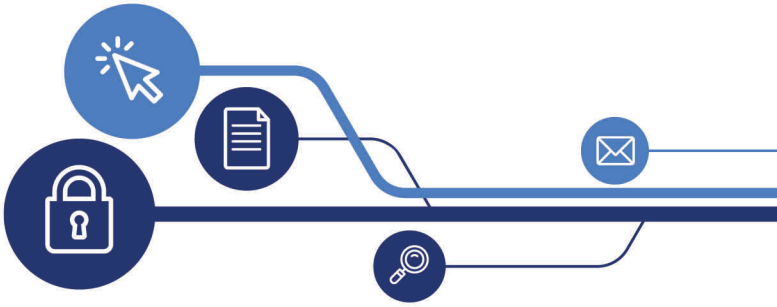
Appendix D – Campaign Sites and Privacy Statements

The following table lists the URLs for the audited campaign sites and associated privacy statements.

Candidate	Campaign Website	Privacy Statement
Michael Bennet (D)	https://michaelbennet.com/	https://michaelbennet.com/privacy-policy/
Joe Biden (D)	https://joebiden.com/	https://joebiden.com/privacy-policy/
Cory Booker (D)	https://corybooker.com/	https://corybooker.com/privacy-policy/
Steve Bullock (D)	https://stevebullock.com/	https://stevebullock.com/privacy-policy/
Pete Buttigieg (D)	https://peteforamerica.com/	https://peteforamerica.com/privacy-policy/
Julian Castro (D)	https://www.julianforthefuture.com/	https://www.julianforthefuture.com/privacy-policy/
John Delaney (D)	https://www.johndelaney.com/	https://www.johndelaney.com/privacy-policy/
Tulsi Gabbard (D)	https://www.tulsi2020.com/	https://www.tulsi2020.com/privacy-policy
Kamala Harris (D)	https://kamalaharris.org/	https://kamalaharris.org/privacy-policy/
Amy Klobuchar (D)	https://amyklobuchar.com/	https://amyklobuchar.com/privacy-policy/
Wayne Messam (D)	https://wayneforusa.com/	None found
Beto O'Rourke (D)	https://betoorourke.com/	https://betoorourke.com/privacy-policy/
Tim Ryan (D)	https://timryanforamerica.com/	None found
Bernie Sanders (I)	https://berniesanders.com/	https://berniesanders.com/privacy-policy/
Mark Sanford (R)	https://www.marksanford.com/	None found
Joe Sestak (D)	https://www.joesestak.com	https://www.joesestak.com/privacy-policy/
Tom Steyer (D)	https://www.tomsteyer.com/	https://www.tomsteyer.com/privacy-policy/
Donald Trump (R)	https://www.donaldjtrump.com/	https://www.donaldjtrump.com/privacy-policy/
Joe Walsh (R)	https://www.joewalsh.org	None found
Elizabeth Warren (D)	https://elizabethwarren.com/	https://elizabethwarren.com/privacy-policy
Bill Weld (R)	https://www.weld2020.org/	https://www.weld2020.org/privacy_policy
Marianne Williamson (D)	https://www.marianne2020.com/	https://www.marianne2020.com/privacy-policy
Andrew Yang (D)	https://www.yang2020.com/	https://www.yang2020.com/privacy_policy/

Internet Society's Online Trust Alliance

Online Trust Audit – 2020 Presidential Campaigns



About the Internet Society's Online Trust Alliance (OTA)

The Internet Society's Online Trust Alliance (OTA) identifies and promotes security and privacy best practices that build consumer confidence in the Internet. Leading public and private organizations, vendors, researchers, and policymakers contribute to and follow OTA's guidance to help make online transactions safer and better protect users' data. The Internet Society is a global nonprofit dedicated to ensuring an open, globally connected, trustworthy, and secure Internet for everyone.

1910-01