Online Trust Alliance

2016 Presidential Candidate Website Audit
Review & Policy Panel Discussion

Webinar Will Start Shortly
Session will be recorded & posted at
https://otalliance.org/2016candidates
Submit questions

LEARN • INNOVATE • COLLABORATE

Online Trust Alliance

2016 Presidential
Candidate Website Audit
Review & Policy Panel Discussion

September 26, 2015

LEARN • INNOVATE • COLLABORATE

Online Trust Alliance

Program Panelists

Chris Babel
CEO
TRUSTe

Jules Polonetsky
Executive Director
Future of Privacy Forum

Craig Spiezle
Executive Director
Online Trust Alliance

Jeff Wilbur
VP Marketing
Iconix

LEARN • INNOVATE • COLLABORATE

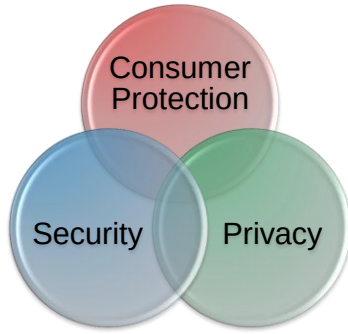
Disclaimers

- The information and results are neither an endorsement nor condemnation of any candidate or their website.
- The report serves to help educate voters and candidates of security, privacy and consumer protection best practices.
- Limited to an analysis of the candidate's site privacy policy as of September 20th.
- Out of scope are any side data sharing agreements which a candidate may have including with political parties or causes.
  - If such agreements were to conflict with the candidate's privacy policy, it would raise several policy and legal issues.

LEARN • INNOVATE • COLLABORATE

Audit & Honor Roll Overview

- **Analysis of ~1,000 web sites**
  - FDIC Banking 100
  - Internet Retailer Top 500
  - Top 50 Social
  - Top 50 News/Media
  - Top 50 Federal Gov't
  - OTA Members
  - IoT 50 (Home automation, Wearables)
  - 2016 Presidential Candidates (23)
- **Scoring**
  - Up to 100 points in each category
  - Bonus points for emerging practices
  - Penalty points vulnerabilities
  - Honor Roll = 80% of total points, 55% or better in each category



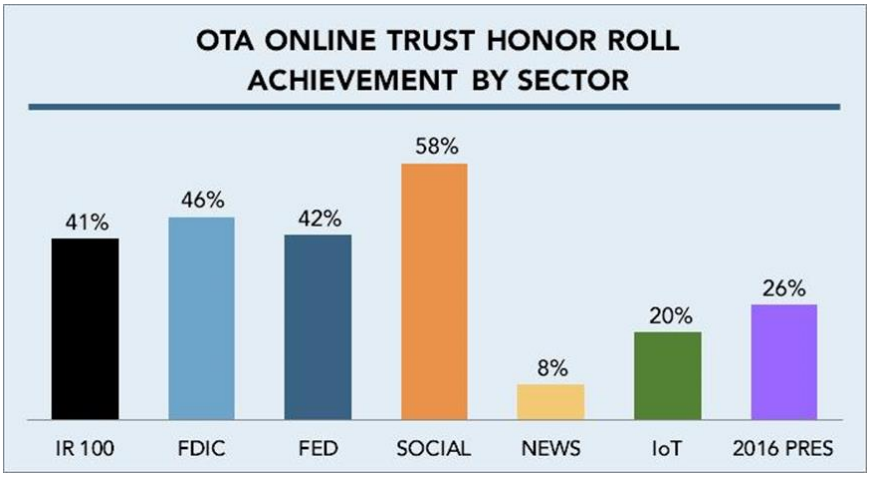
LEARN • INNOVATE • COLLABORATE

Audit Objectives

- Promote best practices and provide 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 promote online trust and confidence.
- Offer assistance to candidates to help improve their consumer protection, security and privacy practices.
- Assist consumers in making informed decisions about the security and privacy practices of sites they frequent.
- Shift the discussion from compliance to stewardship.

LEARN • INNOVATE • COLLABORATE

23 Candidates - How They Compare



LEARN • INNOVATE • COLLABORATE

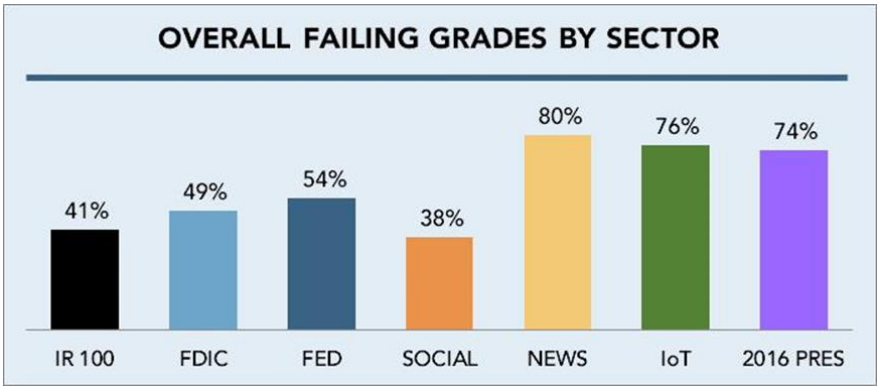
Honor Roll vs Failing Grades

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)

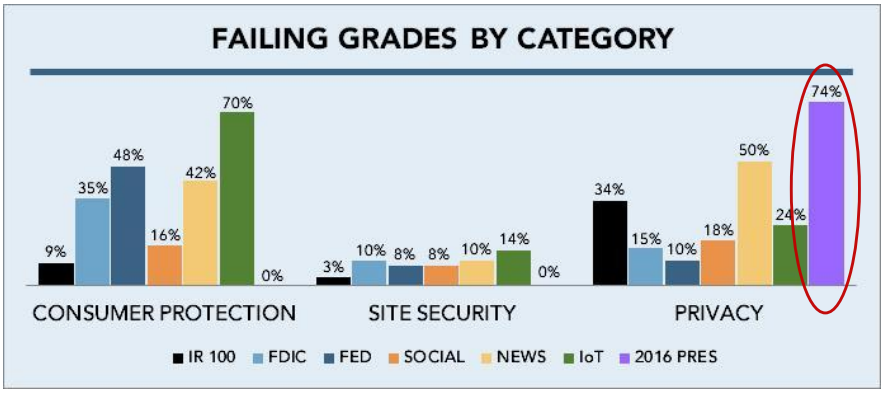
OTA Online Trust Alliance ONLINE TRUST HONOR ROLL 2015

LEARN • INNOVATE • COLLABORATE

How They Compare



Reasons for Failing



Strong Results

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%

- Exposed to spoof & spear phishing
- Inconsistent use of mailing domains
- Need to implement DMARC with reject policies ASAP

LEARN • INNOVATE • COLLABORATE

Server Scores

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%

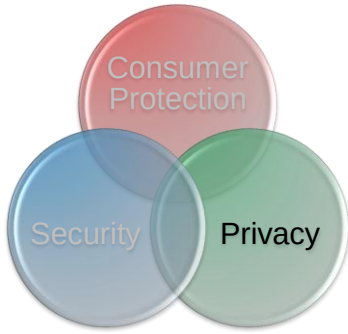
- Strong results expected due to simple infrastructure and “out of box configs”, yet will require ongoing management.
- Excellent support of AOSSL, increasing security and privacy of web session.
- Missed opportunity with EV SSL to enhance brands and counter domain spoofing & lookalike domains.

LEARN • INNOVATE • COLLABORATE

Privacy

Italics = new in 2015

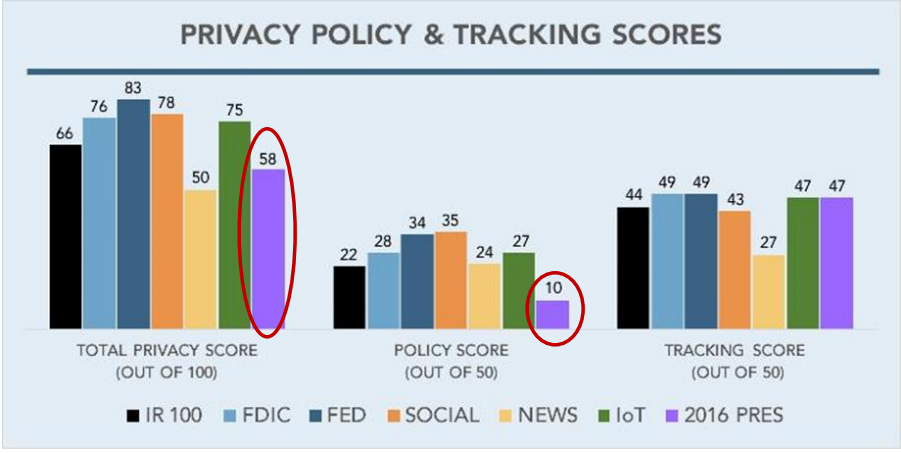
- Base points
  - Privacy policy
  - Third-party trackers on site
- Bonus points
  - Layered privacy policies
  - Multi-lingual policies
  - Use of Icons
  - Do Not Track status, policy
  - Tag mgmt or privacy solution
- Penalty points
  - WHOIS (if Private vs Public)
  - Data Breach Incidents
  - FTC / State Settlements



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

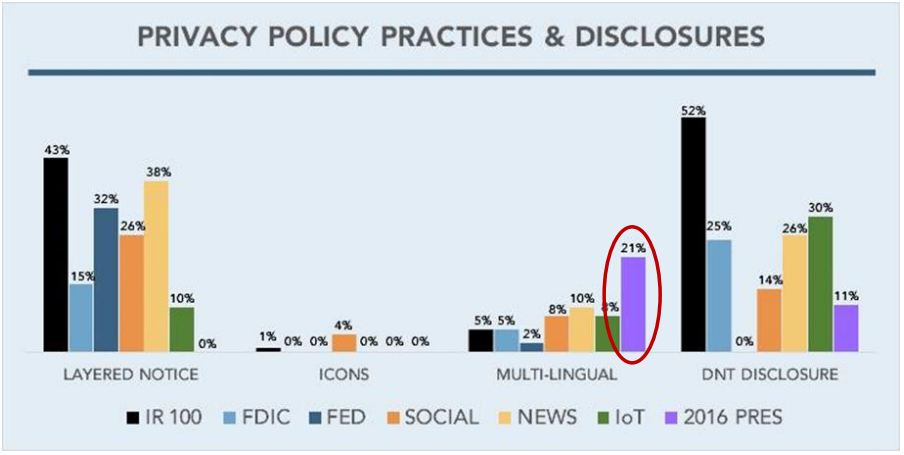
LEARN • INNOVATE • COLLABORATE

Privacy Concerns



LEARN • INNOVATE • COLLABORATE

Lagging Best Practices



LEARN • INNOVATE • COLLABORATE

OTA
Online Trust Alliance

Program Panelists

Chris Babel
CEO
TRUSTe

Jules Polonetsky
Executive Director & Co-Chair
Future of Privacy Forum

Craig Spiezle
CEO & President
Online Trust Alliance

LEARN • INNOVATE • COLLABORATE

Examples

- We may share information about you 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.

Examples

- We may share your personal information with 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.
- We will not sell your personal identifiable information to any party. 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.
- We also will disclose Personal Information to any new or successor entity, should XYZ for President be reorganized, acquired or merged with another entity, in whole or part.

Key Discussion Points

- Should candidate's sites be-exempt from Federal and State Reg's?
- Are they any different than kick-starter campaigns?
- How can you justify failing to have a privacy policy or adhere to FIPPs?
- Data sharing to like-minded organizations
- Reserving the right to sell PII for fundraising
- Are such data sharing practices commonplace?
- Should they be exempt from the FTC or State regulations, or since they are seeking contributions are no different than any commercial site?
- Should they have to comply with disclosure laws, CAN SPAM and other reg's?
- If a candidate site were to be found to be violating their own privacy policy and sharing PII with others are there any repercussions? If not, why not?

Concerns & Ramifications

> The RNC's cooperation with the Trump campaign defangs the Kochs' refusal to share data with Trump, especially since on Wednesday afternoon, the Washington Post reported that the RNC and the Kochs had reached an agreement similar to the one they struck ahead of the 2014 midterm election to share data.
>
> The candidates who have signed the data-sharing agreement with the RNC are: former Florida Gov. Jeb Bush, Sen. Marco Rubio of Florida, Wisconsin Gov. Scott Walker, New Jersey Gov. Chris Christie, Texas Gov. Rick Perry, neurosurgeon Ben Carson, businesswoman Carly Fiorina, former Sen. Rick Santorum of Pennsylvania, former Arkansas Gov. Mike Huckabee, Sen. Ted Cruz of Texas and Louisiana Gov. Bobby Jindal.

https://www.yahoo.com/politics/donald-trump-offered-access-to-the-republican-125451587376.html

Resources

- Presidential Candidate Audit https://otalliance.org/2016candidates
- IoT Working Group https://otalliance.org/IoT
- Email Integrity & Security https://otalliance.org/eauth
- Public Policy - https://otalliance.org/initiatives/public-policy
- Online Trust Honor Roll - https://otalliance.org/HonorRoll
- Email Integrity Audit – https://otalliance.org/emailaudit
- admin@otalliance.org +1 425-455-7400

On The Horizon

Nov 16 - OTA Salon Dinner
Commissioner Julie Brill & Congresswoman Suzan DelBene

Nov 17 – OTA Annual Meeting / Members & Invited Guests

Nov 18 – IoT Trustworthy Working Group

Nov 19 – IoT Congressional Staff Lunch & Briefing

Register
https://otalliance.org/news-events/upcoming-events

Online Trust Alliance

Back Up Slides

LEARN • INNOVATE • COLLABORATE

About OTA

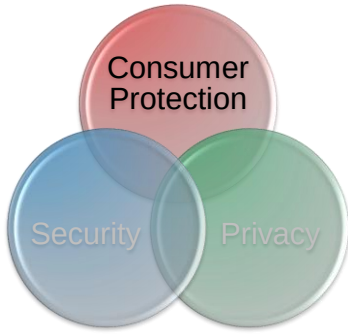
Mission - To enhance online trust and empowering users, while promoting innovation and the vitality of the internet.

- Goal 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, meaningful self-regulation and data stewardship.
- IRS approved 501c3 tax-exempt charitable organization
  - Supported by over 100 leading brands, advertisers, marketers, technology leaders, non-profits and government agencies.

LEARN • INNOVATE • COLLABORATE

Consumer Protection

- Base points *Italics* = new in 2015
  - Email authentication
    - SPF and DKIM at top-level and subdomains
  - DMARC record and policy
    - Policy=Reject for max points
- Bonus points
  - *TLS for email*
  - DNSSEC
- Penalty points
  - Domain locking (not locked)

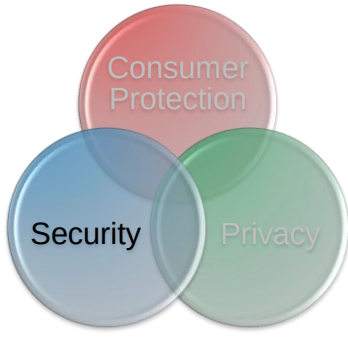


Best practices to help detect and prevent malicious and spoofed email and protect corporate domains

LEARN • INNOVATE • COLLABORATE

Infrastructure Security

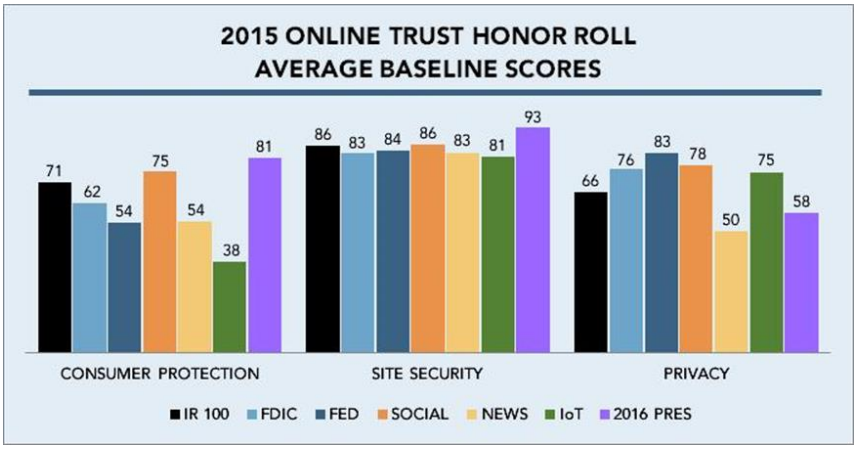
- Base points *Italics* = new in 2015
  - Server & SSL implementation
  - *Anti-bot*
  - *Domain validation cert*
- Bonus points
  - EV SSL
  - AOSSL
  - *Web App Firewall*
- Penalty points
  - XSS / iFrame vulnerabilities
  - Malware
  - Malicious links



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

LEARN • INNOVATE • COLLABORATE

Average Scores



SSL/TLS Deployment Best Practices

Observed Issues

- Support of TLS 2.0
- "Beast Attack"
- Mismatched certs
- Cross site scripting
- iframes exploits
- SHA1 depreciation – weak signature, need to upgrade to SHA2
- "Poodle" attack
- Servers accepting RC4 cipher
- FREAK Exploits
- Lack of support of Forward Secrecy with the reference browsers
- Tools https://ota.ssllabs.com & https://www.htbridge.com/ssl-check/

Privacy – Bonus Points

Layered Notice & Icons

- Publishers Clearing House http://privacy.pch.com/
- Reduced word count from over 4,000 words to 475!
- Adds clarity, readability & transparency
- Added bonus points for icons