Welcome 2017 Online Trust Audit
Congressional Staff Briefing

Recognizing Excellence in Security,
Privacy & Consumer Protection

Objectives:

• Drive adoption and awareness of data security principles and responsible privacy practices
• Move organizations from a “compliance” mindset to embrace “stewardship”
• Incentivize businesses and developers to enhance their security, data protection and privacy practices
• Recognize leadership and excellence
9th Annual Audit Overview

- Over 1,000 web sites
  - Internet Retailer Top 500
  - Bank 100 (previously FDIC 100)
  - Consumer Services 100
  - News/Media 100
  - Federal Gov't 100
  - ISP/Carriers/Hosters 100
  - OTA Members

- Scoring
  - 100 baseline points for each category
  - Weighted composite analysis
  - Bonus points for emerging practices
  - Penalties for vulnerabilities, data loss incident & fines/settlements
  - Honor Roll = 80% or higher overall, no failure(s)
  - Failure for less than 60 points in each category

Record Achievement

- Record achievement despite a bar that continues to rise
- New criteria & shifts in additional requirements
- Minimum failure thresholds raised
## 2017 “Top of Class”

![Top 50 Sites](image)

### “Top of Class” – Top 50

<table>
<thead>
<tr>
<th>Sector</th>
<th>Site</th>
<th>Sector</th>
<th>Site</th>
</tr>
</thead>
<tbody>
<tr>
<td>C, O</td>
<td>Airbnb</td>
<td>C, O</td>
<td>IdentityGuard</td>
</tr>
<tr>
<td>R, O</td>
<td>AmericanGreetings Corp.</td>
<td>C</td>
<td>Indeed</td>
</tr>
<tr>
<td>C</td>
<td>Blogger</td>
<td>C</td>
<td>Instagram</td>
</tr>
<tr>
<td>C</td>
<td>Booking.com</td>
<td>C, O</td>
<td>LifeLock</td>
</tr>
<tr>
<td>C</td>
<td>Box</td>
<td>C, O</td>
<td>LinkedIn</td>
</tr>
<tr>
<td>R</td>
<td>BuildDirect Technologies Inc.</td>
<td>R</td>
<td>LivingSocial Inc.</td>
</tr>
<tr>
<td>G</td>
<td>Census Bureau</td>
<td>C</td>
<td>Meetup</td>
</tr>
<tr>
<td>R</td>
<td>Chewy Inc.</td>
<td>L, O</td>
<td>MicrosoftAzure</td>
</tr>
<tr>
<td>R</td>
<td>Costco</td>
<td>L, O</td>
<td>MicrosoftOutlook.com</td>
</tr>
<tr>
<td>G</td>
<td>Health &amp; Human Services (Healthcare.gov)</td>
<td>N, O</td>
<td>MSN</td>
</tr>
<tr>
<td>I</td>
<td>DigitalOcean</td>
<td>C, O</td>
<td>OneDrive</td>
</tr>
<tr>
<td>C</td>
<td>Dropbox</td>
<td>C</td>
<td>Pinterest</td>
</tr>
<tr>
<td>R</td>
<td>Etsy Inc.</td>
<td>C, O</td>
<td>PublishersClearingHouse</td>
</tr>
<tr>
<td>G</td>
<td>Federal Communications Comm. (FCC)</td>
<td>E, N</td>
<td>Reddit</td>
</tr>
<tr>
<td>G</td>
<td>Federal Deposit Insurance Corp. (FDIC)</td>
<td>C</td>
<td>Snapchat</td>
</tr>
<tr>
<td>R</td>
<td>Fitbit Inc.</td>
<td>C</td>
<td>Spotify</td>
</tr>
<tr>
<td>C</td>
<td>Foursquare</td>
<td>I</td>
<td>Squarespace</td>
</tr>
<tr>
<td>R, O</td>
<td>Gap Inc.</td>
<td>R</td>
<td>TheRealReal</td>
</tr>
<tr>
<td>C</td>
<td>Glassdoor</td>
<td>C, O</td>
<td>Twitter</td>
</tr>
<tr>
<td>C</td>
<td>GoogleDocs</td>
<td>G</td>
<td>U.S. Dept. of Education</td>
</tr>
<tr>
<td>I</td>
<td>GoogleEmail</td>
<td>G</td>
<td>U.S. PostalService</td>
</tr>
<tr>
<td>N</td>
<td>GoogleNews</td>
<td>R</td>
<td>UnderArmourInc.</td>
</tr>
<tr>
<td>C</td>
<td>GooglePlay</td>
<td>C</td>
<td>UpWork</td>
</tr>
<tr>
<td>I</td>
<td>GoogleSites</td>
<td>C</td>
<td>YouTube</td>
</tr>
<tr>
<td>C, I</td>
<td>iCloud</td>
<td>C, I</td>
<td>Zynga</td>
</tr>
</tbody>
</table>

### Top 50 Segment Performance

<table>
<thead>
<tr>
<th>Code</th>
<th>Segment</th>
<th>% of Top 50</th>
</tr>
</thead>
<tbody>
<tr>
<td>C</td>
<td>ConsumerServices</td>
<td>52%</td>
</tr>
<tr>
<td>R</td>
<td>InternetRetailers</td>
<td>20%</td>
</tr>
<tr>
<td>I</td>
<td>ISPs, Carriers &amp; Hosters</td>
<td>14%</td>
</tr>
<tr>
<td>G</td>
<td>Government</td>
<td>12%</td>
</tr>
<tr>
<td>N</td>
<td>News &amp; Media</td>
<td>6%</td>
</tr>
<tr>
<td>F</td>
<td>FDIC 100</td>
<td>0%</td>
</tr>
</tbody>
</table>
Top 10 .gov

Sector Performance

- News/Media segment surge exponentially
- Retailers and Consumer have steady growth
- Banks plunge
Bi-Modal Results

- Over 60% of the Fed 100 and 65% of the Bank 100 fail!
- Effectively, sites embraced best practices or failed

Wide-Ranging Scores

- Many sectors clustered around 80% Honor Roll threshold
Causes of Failures

- Overlooking the basics & fundamentals
- 36% failed in one area, 11% failed in 2-3 areas

Failure Analysis

- **Consumer Protection** – Sites failing to counter phishing exploits
- **Security** – Insecure ciphers & protocols
- **Privacy** – Lack of full disclosures & excessive third-party trackers
Consumer Protection – 2017

- **Base points**
  - Email authentication
    - SPF and DKIM at top-level and subdomains (↑ TLD weight)
  - DMARC record and policy
  - DMARC reject/quarantine
    - Increased weight for reject
  - Invalid SPF / DMARC & “naked” DMARC records not counted

- **Bonus points**
  - TLS for email
  - DNSSEC
  - IPv6
  - Multi-factor authentication

- **Penalty points**
  - Domain locking (not locked)

Embracing OMB Directives

- Federal sites leading significantly in all but MFA (new)
- Email authentication (SPF & DKIM), an OMB directive, covered in following slides
Email Authentication Overview

- **SPF**
  - Authenticates Message Path
  - Authorized senders in DNS

- **DKIM**
  - Authenticates Message Content
  - Public encryption keys in DNS

**DMARC**

- Consistency
  - A method to leverage the best of SPF and DKIM

- Policy
  - Senders can declare how to process unauthenticated email

- Visibility
  - Reports on how receivers process received email

- Aggregated Insights
  - Telemetry into mail streams (RUA)

- Failure & Spoofed email reports
  - (RUF)

---

Fighting Spearphishing

- SPF & DKIM allow recipient to verify sender
- DMARC allows sender to get reports, tell receiver how to handle messages that fail authentication
- Recommend implementation for inbound & outbound email
- All domains – top-level and subdomains
- Observed many (>70) inaccurate / malformed SPF records
Fighting Spearphishing

- Federal sites lagging in protection from spoofed email
- Understates the risks for members of Congress’ domains

DMARC – Emerging Standard

- Growth in all sectors
- Real value when sites instruct ISPs / receivers to “reject” or “quarantine” unauthenticated email
- Note impact of invalid DMARC records (3% overall)
Site Security – 2017

• Base points
  ▫ Server & SSL/TLS implementation
  ▫ Application / network security
  ▫ IP reputation, patching cadence

• Bonus points
  ▫ Extended Validation certificates
  ▫ “HTTPs everywhere”, HSTS
  ▫ Web application firewall
  ▫ Vulnerability reporting mechanism

• Penalty points
  ▫ XSS / iFrame vulnerabilities
  ▫ Malware / Malicious links
  ▫ Bot risk

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.

Overall Security

- Encryption becoming the “norm”, jumping from 30% to 52%
- Extended Validation certs recognized for brand protection
Security Assessment Tools

- Bonus points (new in 2017)
  - Discoverable on the site
  - Discoverable via third-party reporting program
- Ties to NTIA, NIST and FTC recommendations
- 36% of Consumer sites support it
- Other segments <3%

Vulnerability / Bug Reporting
Example

Privacy – 2017

- **Base points**
  - Privacy policy (55 pts)
    - Data sharing, retention, third-party sharing
    - DNT disclosure
    - Layered notices
    - Link on home page
    - COPPA
    - Date stamp on top of page
  - Third-party trackers on site (45 pts)

- **Bonus points**
  - Redline version archived
  - Use of Icons
  - Cross device tracking disclosure
  - Honoring DNT / Multi-lingual policy
  - Tag management 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.
Overall Privacy

- 2017 Shifted more weight on the privacy policy disclosures
- Shifting from compliance to stewardship
- Driving towards GDPR

Tracking Tags / Calls

- Analysis of third party tracking, sharing, retargeting
- Does not apply to trackers used for anonymous site metrics
- Ranged from 0 to over 59 on a single site!
- Average of 42 unique trackers per “Consumer Services” site
- Use of multiple tools
  - OTA tools
  - Disconnect
  - Ensighten
Transparency

- Beyond compliance, advancing transparency

Version Tracking
Version Tracking

Updates: Privacy Policy
We want to be as transparent as possible about the changes we make to our Privacy Policy. In this archive you can see the previous versions of the policy. We’ve also included a page that compares the current policy to the previous versions to make it as easy as possible to see what has changed.

• Current version
  • Comparison
    • March 1, 2017
    • Comparison
    • August 25, 2016
    • Comparison
    • June 30, 2014
    • Comparison
    • March 25, 2014
    • Comparison
    • August 19, 2013

Readability

• Complexity vs Comprehensible?
• Is English the primary language of all of your users?
Use of Icons

Layered Notices
### Layered Notice

![Layered Notice Image]

### Data Handling

#### PRIVACY POLICY - DATA HANDLING

- **Data Not Shared**
  - 51%
  - 62%
  - 93%
  - 72%
  - 58%
  - 74%
  - 43%
  - 19%

- **Data Retention**
  - 69%
  - 62%
  - 81%
  - 66%
  - 60%
  - 40%
  - 59%
  - 49%

- **Vendor Confidentiality**
  - 49%
  - 48%
  - 74%
  - 74%
  - 51%
  - 20%
  - 48%

<table>
<thead>
<tr>
<th>Category</th>
<th>IR 100</th>
<th>IR 500</th>
<th>BANKS</th>
<th>FED</th>
<th>CONSUMER</th>
<th>NEWS</th>
<th>ISP/HOSTS</th>
<th>OVERALL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Not Shared</td>
<td>51%</td>
<td>62%</td>
<td>93%</td>
<td>72%</td>
<td>58%</td>
<td>74%</td>
<td>43%</td>
<td>19%</td>
</tr>
<tr>
<td>Data Retention</td>
<td>69%</td>
<td>62%</td>
<td>81%</td>
<td>66%</td>
<td>60%</td>
<td>40%</td>
<td>59%</td>
<td>49%</td>
</tr>
<tr>
<td>Vendor Confidentiality</td>
<td>49%</td>
<td>48%</td>
<td>74%</td>
<td>74%</td>
<td>51%</td>
<td>20%</td>
<td>48%</td>
<td></td>
</tr>
</tbody>
</table>

- Control on the sharing and usage of user data
- “If you do not retain it you can not lose it”
What Have We Learned

- Need to move beyond compliance
- Requires ongoing commitment & vigilance
- Everyone’s job within an organization
- Need to think beyond the US legal framework
- Responsible privacy practices enhance trust
- Learn from others’ mistakes

Checklist & Resources

- Evaluate your own site
- https://otalliance.org/TrustAudit
  - Methodology
  - Checklists
  - Listing of free public tools
  - Recorded webinars
Next Steps

- Evaluate your own site & use the checklist
- Possible new segments
  - Healthcare / Top 100 hospitals / medical center
  - EU & APAC segments
- Tentative Timing
  - September open call for comments
  - January / February publish new criteria and enhancements
  - April / May testing
  - June – Release of 2018 Audit

Open Dialog & Next Steps

- Online Trust Audit  [https://otalliance.org/TrustAudit](https://otalliance.org/TrustAudit)
- Methodology
- Questions