Protecting Your Privacy

Cal Poly Information Security Office
infosec@calpoly.edu
Why protect your privacy?
How Target Figured Out A Teen Girl Was Pregnant Before Her Father Did

Kashmir Hill  Forbes Staff

Welcome to The Not-So Private Parts where technology & privacy collide

Every time you go shopping, you share intimate details about your consumption patterns with retailers. And many of those retailers are studying those details
We’ll focus on three points:

• How does tracking work?

• Who performs tracking?

• What can you do?
Tracking = collect individualized data + associate behavior

- Collect individualized data: Collect user information and behavior across sites, devices, and services.
- Association: correlate data into desired behavior, like clicking an ad or purchasing a product.
Website Tracking

• Most websites run tracking code adding a **unique ID** to your browser.
• Common tracking code runs on different websites, all using the same ID to associate website behavior to you.
<table>
<thead>
<tr>
<th>Setting</th>
<th>Blocking Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>+ all</td>
<td></td>
</tr>
<tr>
<td>cnn.com</td>
<td>++</td>
</tr>
<tr>
<td>adnxs.com</td>
<td>-</td>
</tr>
<tr>
<td>ads-twitter.com</td>
<td>-</td>
</tr>
<tr>
<td>ajax.googleapis.com</td>
<td>+</td>
</tr>
<tr>
<td>amazon-adsystem.com</td>
<td>-</td>
</tr>
<tr>
<td>bing.com</td>
<td>-</td>
</tr>
<tr>
<td>bounceexchange.com</td>
<td>-</td>
</tr>
<tr>
<td>chartbeat.com</td>
<td>-</td>
</tr>
<tr>
<td>cnn.io</td>
<td>+</td>
</tr>
<tr>
<td>cnnlabs.io</td>
<td>+</td>
</tr>
<tr>
<td>cookielaw.org</td>
<td>+</td>
</tr>
<tr>
<td>criteo.net</td>
<td>-</td>
</tr>
<tr>
<td>3qdfnco3bamip.cloudfront.net</td>
<td>+</td>
</tr>
<tr>
<td>doubleclick.net</td>
<td>-</td>
</tr>
<tr>
<td>ensighten.com</td>
<td>-</td>
</tr>
<tr>
<td>facebook.com</td>
<td>+</td>
</tr>
<tr>
<td>facebook.net</td>
<td>+</td>
</tr>
</tbody>
</table>
Tracking personal information

• I’ll let Google answer for me:
  – https://support.google.com/google-ads/answer/7019460

• Let’s also ask Facebook:
  – https://www.facebook.com/business/ads/ad-targeting
And a lot more data:

- Social networks
- Smartphone information like location data
- Alexa/Siri/Cortana searches
- Internet activity through Internet Service Providers
- Professional organizations
- Physical/online store purchases
- And much, much more…
How is all of this data collected? Who owns this data?

- Companies use, buy, and sell tracking data.
- There are large corporations whose sole function is to analyze and sell tracking data.
  - Acxiom
  - Nielsen
  - Experian & Equifax
Black Market Data Brokers

- Credit card breaches, password breaches, and other data is released.
- Black market sellers compile and sell data, often in bulk.
- Stolen credit cards cost from $1 - $50, per card.
Black Market Data Brokers
What can you do?

- Use an adblocker (uBlock Origin works best).
- Opt-out of tracking/data sharing on supporting services.
- Request personal data from services.
- Install trusted apps on smartphones.
- Search data breach sites for your information.
Using an Adblocker

• Controversial: many sites are ad-supported.
• Benefit is they stop tracking.
  – Many malicious ads contain malware.
• Personal recommendation: uBlock Origin
  – Unobtrusive, resource-light, and selectively blocks parts of pages.
• Whitelist sites you want to support.
Opting out of tracking + requesting data

• Many sites contain an opt-out and data request option.
• Stops tracking preemptively.
• Available in Facebook/Google account settings.
• Acxiom Opt-Out Site
Request your personal data

• Many services allow you to download your personal data.
• Google, Facebook, Apple support.
Demo – Google Settings

• myaccount.google.com
Install only trusted smartphone apps

• Each app requires certain permissions to run.

• Inspect and ask: do these permissions make sense?
Install only trusted smartphone apps
Search data breach sites for your information

• Data breaches are often compiled into bundles of millions (now over 1 billion) records.

• Sites like HaveIBeenPwned collect them and allow searching, stripping out sensitive data.

• Never reuse your passwords.
haveibeenpwned.com
haveibeenpwned.com

**Notify me**

Get notified when future pwnage occurs and your account is compromised.

infosec@calpoly.edu

Just to make sure you're not a robot, please solve this puzzle first:

- [ ] I'm not a robot

notify me of pwnage
Questions?
Information Security Office

Report abuse to abuse@calpoly.edu
infosec@calpoly.edu