BEGINNS AT 1:15 PM
Opening Remarks

Scott McDonald, Ph.D.
President & CEO
Voice of the Consumer

Allie Bohm
Policy Counsel

Public Knowledge
Public Knowledge promotes freedom of expression, an open internet, and access to affordable communications tools and creative works. We work to shape policy on behalf of the public interest.
Voice of the Consumer
Carnegie Mellon Study
Users Care About Privacy

Facebook's "Privacy Trainwreck": Exposure, Invasion, and Drama

danah boyd
September 8, 2006

Facebook's New Terms Of Service: "We Can Do Anything We Want With Your Content. Forever."

This post has generated a lot of responses, including from Facebook. Check them out here.

Is Facebook's Application Dashboard Missing a Privacy Gauge?
By Chris Conley, Policy Attorney, ACLU of Northern California Technology and Civil Liberties Project
MARCH 25, 2010 | 5:40 PM

Is Facebook Unliking Privacy?
By Chris Conley, Policy Attorney, ACLU of Northern California Technology and Civil Liberties Project
FEBRUARY 8, 2010 | 10:27 AM

Facebook Revolt at Hand?
By Suzanne Ito, ACLU
MAY 5, 2011 | 1:29 PM

The Hidden Secrets of Online Quizzes
By JR Raphael
PAID MAY 10, 2009 | 4:08 PM PT

Rough seas nearly sink Facebook's Beacon
After a rough couple of weeks and plenty of complaints, the social-networking site alters its controversial advertising program. But is it enough?

Facebook Ads Reveal Users’ Sexual Preferences

Millennials do care about Internet privacy, they’re just smarter about it
An Ariane Center survey reveals younger folks are more willing to share personal data – but also more likely to demand something in return
Targeted Advertising
Privacy Settings Can Be Misleading
Privacy Settings Can Be Misleading

Who should see this?

- Public + Developers
  Anyone on or off Facebook
- Friends + Developers
  Your friends and more!
History
Fair Information Practice Principles

1. There must be no personal-data record-keeping systems whose very existence is secret.
2. There must be a way for individuals to find out what information about them is in a record and how it is used.
3. There must be a way for individuals to prevent information about them obtained for one purpose from being used or made available for other purposes without their consent.
4. There must be a way for individuals to correct or amend a record of identifiable information about them.
5. Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take reasonable precautions to prevent misuse of the data.
Sector-Specific Privacy Laws

PUBLIC LAW 100-618—NOV. 5, 1988

102 STAT. 3195

Section 1. SHORT TITLE.
This Act may be cited as the “Video Privacy Protection Act of 1988.”

SEC. 2. AMENDMENT.
(a) In general.—Section 212 of title 18, United States Code, is amended—
(1) by redesignating section 212a as section 212;
(2) by inserting after section 212a the following:

“§ 2171. Wrongful disclosure of video tape rental information
(a) Definitions.—For purposes of this section—
(1) the term ‘consumer’ means any renter of a video tape, subscriber of a service or subscriber of video services; and
(2) the term ‘video tape service provider’ means any person engaged in the business of, or offering any rental service or video service;

(b) Violation.—Any person who, knowing that the information will be used to disclose confidential information about a customer or subscriber, discloses or compounded any information of that type of information shall be subject to the penalties provided in section 2171a of title 18, United States Code.

§ 2171a. Civil penalties
(a) In general.—Any person who discloses confidential information about a customer or subscriber shall be subject to the penalties provided in section 2171a of title 18, United States Code.

(b) Criminal penalties.—Any person who discloses confidential information about a customer or subscriber shall be subject to the penalties provided in section 2171a of title 18, United States Code.

§ 2171b. False statements
(a) In general.—Any person who, knowing that a statement is false, makes a false statement in order to secure the rental or sale of a video tape or video service shall be subject to the penalties provided in section 2171a of title 18, United States Code.

(b) Criminal penalties.—Any person who, knowing that a statement is false, makes a false statement in order to secure the rental or sale of a video tape or video service shall be subject to the penalties provided in section 2171a of title 18, United States Code.

§ 2171c. False statements
(a) In general.—Any person who, knowing that a statement is false, makes a false statement in order to secure the rental or sale of a video tape or video service shall be subject to the penalties provided in section 2171a of title 18, United States Code.

(b) Criminal penalties.—Any person who, knowing that a statement is false, makes a false statement in order to secure the rental or sale of a video tape or video service shall be subject to the penalties provided in section 2171a of title 18, United States Code.
State Laws
Section 5
General Data Protection Regulation (GDPR)
Potential GDPR Consent Screens
Recommendations

• Meaningful notice and consent.
• Robust security safeguards.
• Meaningful redress.
Where to Learn More

• Here’s How Congress Should Respond to Facebook/Cambridge Analytica (blog):

• Letter to Congress re: Facebook Data Protection Hearing:

• Is GDPR Right for the United States? (blog):
  – https://www.publicknowledge.org/news-blog/blogs/is-the-gdpr-right-for-the-united-states
How Adequate Are Existing Privacy Policies for Research? A Meta Analysis

Paul Donato
Chief Research Officer

ARF the Advertising Research Foundation

ARF TOWNHALL
Research Ethics
Partnered with GreenBook
## Review Coverage

<table>
<thead>
<tr>
<th>GDPR</th>
<th>Associations</th>
<th>Research</th>
<th>Social</th>
<th>Ad-Tech/ Tech</th>
<th>DAA</th>
</tr>
</thead>
<tbody>
<tr>
<td>GDPR</td>
<td>AAPOR</td>
<td>comScore</td>
<td>Facebook</td>
<td>Amazon</td>
<td>2009 OBA</td>
</tr>
<tr>
<td>AAAA</td>
<td>GFK</td>
<td></td>
<td>Instagram</td>
<td>Apple</td>
<td>2011 Multi Site Data</td>
</tr>
<tr>
<td>ANA</td>
<td>IPSOS</td>
<td></td>
<td>Pinterest</td>
<td>Axiom/ Liveramp</td>
<td>2013 Mobile</td>
</tr>
<tr>
<td>DMA*</td>
<td>Kantar</td>
<td></td>
<td>Snapchat</td>
<td>Google</td>
<td>2015 Cross Device</td>
</tr>
<tr>
<td>ESOMAR</td>
<td>Nielsen</td>
<td></td>
<td>Spotify</td>
<td>Neustar</td>
<td></td>
</tr>
<tr>
<td>IAB*</td>
<td></td>
<td></td>
<td>Twitter</td>
<td>Oath</td>
<td></td>
</tr>
<tr>
<td>Insights Association</td>
<td></td>
<td></td>
<td>Oracle Data Cloud</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NMSBA</td>
<td></td>
<td></td>
<td></td>
<td>Viant</td>
<td></td>
</tr>
</tbody>
</table>

* Treated in discussion with DAA
Some Key Requirements

- Readiness Plan
- Freely given unambiguous consent to drop cookies
- Analytics may require second consent
- Consent for profiling and auto-decisions
- Data Protection Officer
- Access to data, correct and erasure
- Allowable contacts: contract, loyalty program, contest, membership, balanced solicitation with prior purchase
## Association Codes (2009 - 2018)

<table>
<thead>
<tr>
<th>Principles</th>
<th>Participants</th>
<th>Profession</th>
<th>Clients</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Chain of Trust</td>
<td>Mostly Research</td>
<td>• No unfair criticism</td>
<td>• Methods Description</td>
</tr>
<tr>
<td>• Honesty</td>
<td></td>
<td>• Promote Trust</td>
<td>• Sample stats</td>
</tr>
<tr>
<td>• Objective</td>
<td></td>
<td>• Guideline (Casro &amp; DMA) enforcement</td>
<td>• Sources of error</td>
</tr>
<tr>
<td>• Integrity</td>
<td>Delete PII asap</td>
<td>• US EU Safe Harbor</td>
<td>• Audit available</td>
</tr>
<tr>
<td>• Quality</td>
<td>No Selling</td>
<td>• Report sponsorship</td>
<td>• Report multi-client</td>
</tr>
<tr>
<td></td>
<td>No Direct Action</td>
<td>• Address Complaints</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Pre-Existing relation</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>○ No unsolicited email</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>○ Name Provider</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Indicate recontact</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Data Breach Notice</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Contractor level of care</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Consent to forward PII</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Compared to other sectors, association codes are very similar and strong but traditional. Of note, almost all include responsibilities to the Profession.
### Research Policies (2015 -2018)

#### Participants
- Not forward PII unless contractor
- No Selling/Fund Raising
- Minimize data collection and retention
- Use cookies, flash, web beacons, log files, digital fingerprint, location
- CASRO Standards
- PII with consent or within subsidiaries
- Significant differences
  - Some detailed, some less
  - Some cover employees some not

#### Digital Participants
- References to DAA, NAI, EDAA
- Opt-out
- Minimal Collection
- YOY Retention
- Delete PII asap
- No PII to third parties
- Significant differences

#### Neuro
- References to ESOMAR, ARF, MMA and CASRO
- No Stress
- No incidental discovery
- No sales
- Consent to process
- Minimal PII
- Convey Purpose
- Very similar in content

Compared to other sectors, research codes are very different. Only digital references AdTech
# Social Policies (2017 - 2018)

## Public
- Safety
- Security
- Prevent Fraud
- Prevent Harm

## Users
- Information used
  - You give
  - Your Use
  - Original Content
- To develop services
- To communicate
- Some mention:
  - Gyroscope, accelerometer, microphone, camera, location, wireless and app usage
  - Others: Posts are public
- Can delete, restrict but shares not deleted
- DAA codes referenced
- Less legalize

## Research
- Product R&D
- Research and Academia
  - Social Welfare
  - Technology Advancement
  - Public Interest
  - Health and well being

---

*Similar in principles but significant differences driven by functionality*
Tech / AdTech Policies (2017 - 2018)

Tech
- May know,
  - Heart rate
  - Pictures
  - Messages
  - And everything else
- The most conservative policy reviewed

AdTech
- Info we collect
  - You Give
  - Your Use
  - Our Ads
- Collect location, cookies, local storage,
  - To offer tailored content and ads
- Share personal information with consent
- Will share non-PII to advertisers, publishers, ..
- Share PII within company
- Will share with over 100 third parties
- Aboutads.com & Opt-out channel
- No time limits/4 mo to 5 yr limits
- Privacy By Design, TRUSTe
- Store Email Content
- Third-party, onboarding, retail, …

There is a wide variety of data uses and hence content of data use policies
Is there a law?

- Section 5 of the FTC Act, which states “unfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce, are hereby declared unlawful.” Advertisements or claims that misrepresent or omit information that would be material to consumers could be considered “deceptive.”

- They include, but are not limited to, the following: tell the truth about what the app can do, disclose key information clearly and conspicuously, build privacy considerations into the app from the start, offer choices that are easy to find and easy to use, honor your privacy promises, protect kids’ privacy, collect sensitive information only with consent, and keep user data secure.

- For a comprehensive list of these guidelines and a detailed explanation of each, please refer to the FTC’s guide “Marketing Your Mobile App, Get It Right from the Start”.

- Enforcement Actions
  - Visio
  - Turn
  - Jerk
  - Epic
  - Silver Push

<table>
<thead>
<tr>
<th>Online Behavioral Advertising</th>
<th>Multi Site Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Principles proposed by the FTC in 2009</td>
<td>• For non-advertising applications</td>
</tr>
<tr>
<td>• Educate consumers and business</td>
<td></td>
</tr>
<tr>
<td>• Transparency to consumers</td>
<td></td>
</tr>
<tr>
<td>• Service providers &amp; desktop applications w access to URLs need consent in advance of advertising</td>
<td></td>
</tr>
<tr>
<td>• Consent before change of data use</td>
<td></td>
</tr>
<tr>
<td>• Consent for collecting sensitive data</td>
<td></td>
</tr>
<tr>
<td>• Mechanism for policing and reporting violations</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Mobile Environments</th>
<th>Cross Device</th>
</tr>
</thead>
<tbody>
<tr>
<td>• OBA Expanded to mobile (cross-app data, &quot;precise&quot; location data, personal, photo and directory data)</td>
<td>• Reaffirms consent on one device implies consent on others but requires transparency</td>
</tr>
<tr>
<td>• Consent on one device implies consent on others</td>
<td></td>
</tr>
</tbody>
</table>

- **Online Behavioral Advertising**
  - Principles proposed by the FTC in 2009
  - Educate consumers and business
  - Transparency to consumers
  - Service providers & desktop applications w access to URLs need consent in advance of advertising
  - Consent before change of data use
  - Consent for collecting sensitive data
  - Mechanism for policing and reporting violations

- **Multi Site Data**
  - For non-advertising applications

- **Mobile Environments**
  - OBA Expanded to mobile (cross-app data, "precise" location data, personal, photo and directory data)
  - Consent on one device implies consent on others

- **Cross Device**
  - Reaffirms consent on one device implies consent on others but requires transparency
BBB & DMA Enforcement

ADVERTISING SELF-REGULATORY COUNCIL/COUNCIL OF BETTER BUSINESS BUREAUS

ONLINE INTEREST-BASED ADVERTISING ACCOUNTABILITY PROGRAM

FORMAL REVIEW
Case Number: 71-2017

COMPANY:

CHALLENGER:
Online Interest-Based Advertising Accountability Program

DECISION
DATE: January 25, 2017
A few features a review would consider:

- Language less precise
  - as long as necessary, reasonable steps, reasonable security, limited retention…
- Withdrawal of consent does not withdraw the right to data retention
- Should deletion be considered withdrawal of consent?
- De-identification is a key part to many of these policies, but the process of de-identification is not specified in any detail
  - For example, The Netflix Competition
- No mention of encryption
- Privacy Analytics
- Research on Language
- [https://centerforplainlanguage.org/](https://centerforplainlanguage.org/) (Time.com)
  - Making a Science of Privacy Statements
## Summary & Recommendation

<table>
<thead>
<tr>
<th>GDPR</th>
<th>Associations</th>
<th>Research</th>
<th>Social</th>
<th>Ad-Tech/ Tech</th>
<th>DAA</th>
</tr>
</thead>
<tbody>
<tr>
<td>EU foundation with to-be-passed ePrivacy controlling cookies, messaging, emails …</td>
<td>Codes similar, strong but traditional</td>
<td>Significant differences in detail, little related to AdTech</td>
<td>Generally very detailed and driven by functionality</td>
<td>Wide variety, sometimes sharing of PII across member companies, sometimes third parties</td>
<td>The basis of most social and AdTech policies</td>
</tr>
</tbody>
</table>

One opportunity is for the working group to evaluate and update the DAA standards into a single document that reflects AdTech in 2018.
Fireside Chat about GDPR

Scott McDonald, Ph.D.
President & CEO

Ben Hoxie
Director of Product Management
Industry Panel
Input on Data & Research Privacy Standards

Moderator

Paul Donato
CRO
ARF

Rick Bruner
Vice-Chair, USA
I-COM

Rolfe Swinton
Director,
Data Assets
GfK

Tania Yuki
Founder & CEO
Shareablee