



ARF

TOWNHALL

Research Ethics

Partnered with GreenBook



Opening Remarks

Scott McDonald, Ph.D.
President & CEO



ARF
TOWNHALL
Research Ethics
Partnered with GreenBook



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



Terms of Service

These Terms of Service are a contract between you and Infinity Box Inc., a company with its principle place of business at 12157 W. Linebaugh Ave., PMB 327 Tampa, FL 33626 USA ("Infinity Box"). Infinity Box operates www.wufoo.com ("Wufoo Site") and the form document generation, collection and storage services therein (collectively the "Service"). By using the Wufoo Site and any services accessible from the Wufoo Site, you are agreeing to be bound by the following terms and conditions ("Terms of Service").

If you do not agree to these Terms of Service or any part thereof, your only remedy is to not use the Wufoo Site or the Service. VIOLATION OF ANY OF THE TERMS BELOW WILL RESULT IN THE TERMINATION

Accept Terms *

I agree to the Terms of Service.

Submit

Users Care About Privacy

CONSUMERIST

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."

2:15:09
11:14 PM EDT

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

FEBRUARY 8, 2010 | 10:27 AM

Is Facebook Unliking Privacy?



By [Chris Conley](#), Policy Attorney, ACLU of Northern California Technology and Civil Liberties Project

MARCH 26, 2010 | 5:46 PM

GIGAOM Get our newsletter

Topics: Analysis Events Reports Publisher's Corner

The industry leader in emerging technology research [Subscribe](#)

Facebook's Instant Personalization Is the Real Privacy Hairball

by [Chris Conley](#) Apr 22, 2010 - 11:00 AM CDT

PCWorld
FROM IDG



NEWS

The Hidden Secrets of Online Quizzes



By [JR Raphael](#)

PCWorld | MAY 12, 2009 4:00 PM PT



REVIEWS NEWS VIDEO HOW TO SMART HOME CARS DEALS DOWNLOAD

CULTURE

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?

BY CAROLINE MCCARTHY / NOVEMBER 30, 2007 12:16 AM PST



Facebook Revolt at Hand?



By [Suzanne Ito](#), ACLU
MAY 14, 2010 12:16 PM

TAGS: National Security, Privacy & Technology, Consumer Privacy



Yesterday, Facebook reportedly called an "all hands" meeting to discuss its privacy policies. That's because they are facing a brewing revolt among Facebook users alarmed by the company's, ahem, cavalier attitude toward protecting your privacy.

HUFFPOST

TECH 16/01/2012 06:44 GMT | Updated 17/03/2012 05:12 GMT

Facebook Ads Reveal Users' Sexual Preferences

News All topics Video SlideShows Deals Online Courses Newsletter Resources/White Papers

ITWORLD

Home > IT Management

THANK YOU FOR NOT SHARING

By [Dan Tynan](#), [ITWorld](#) | APRIL 22, 2013

Millennials do care about Internet privacy, they're just smarter about it

An Annenberg Center survey reveals younger folks are more willing to share personal data — but also more likely to demand something in return

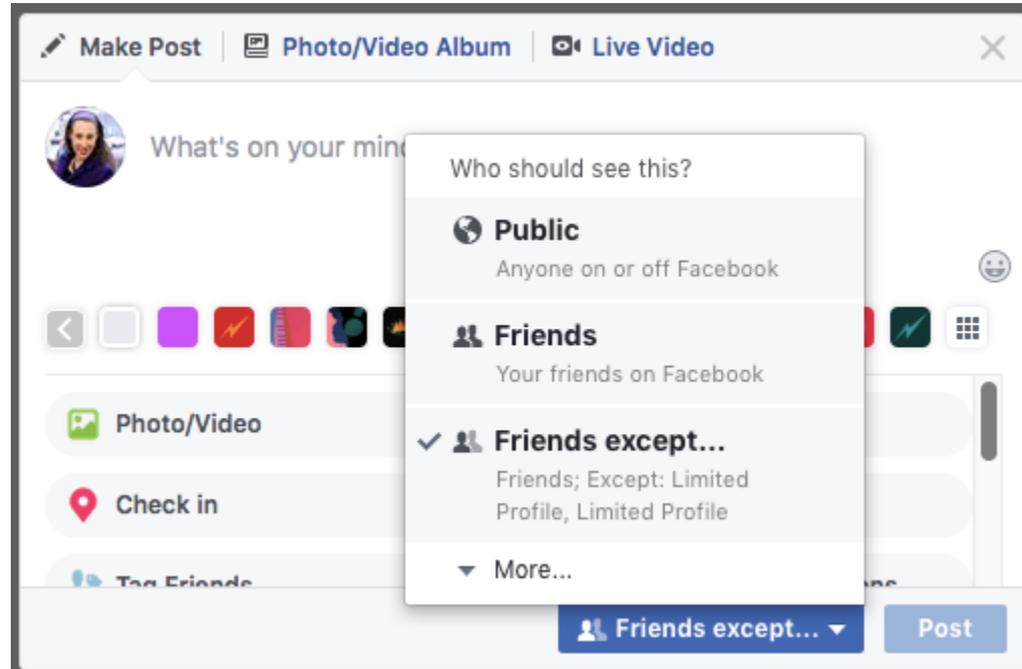


Targeted Advertising

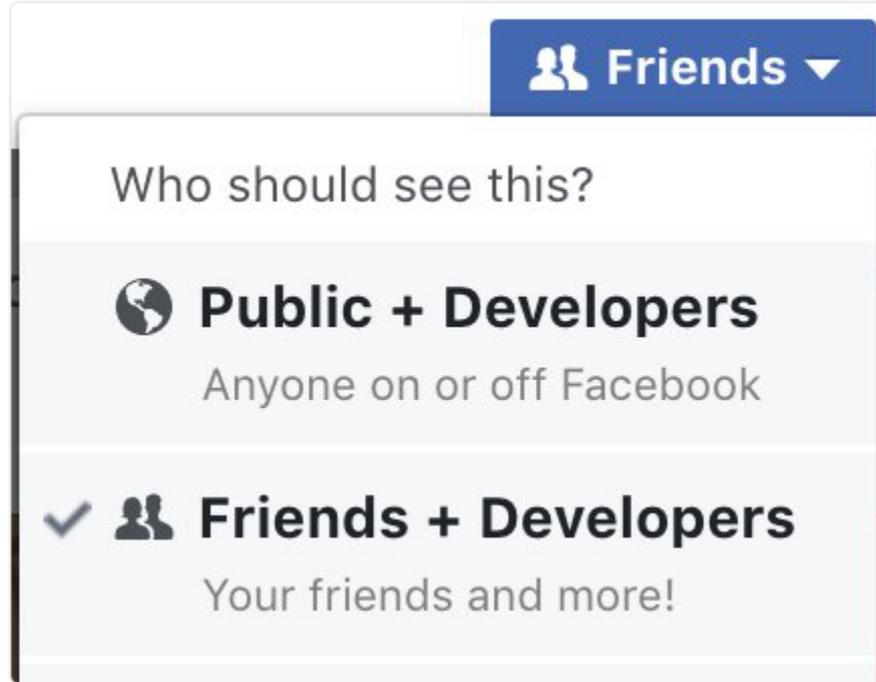
The image displays a collage of browser windows illustrating targeted advertising. The top row shows two browser tabs: **economist.com** and **multichannel.com**. Both display a Cisco Webex advertisement with the text "Cisco Webex. The more intuitive way to work." and a blue "Explore Webex" button. The **multichannel.com** browser also shows a small profile picture of a man in the top right corner of the page.

The bottom row shows three browser tabs: **mashable.com**, **forbes.com**, and **thestreet.com**. The **mashable.com** and **forbes.com** tabs display the same Cisco Webex advertisement. The **forbes.com** browser also shows a small profile picture of a woman in the top right corner of the page. The **thestreet.com** tab displays a Reebok advertisement for "CLASSIC LEATHER" shoes, featuring a pair of white sneakers and a "SHOP NOW" button.

Privacy Settings Can Be Misleading



Privacy Settings Can Be Misleading



History



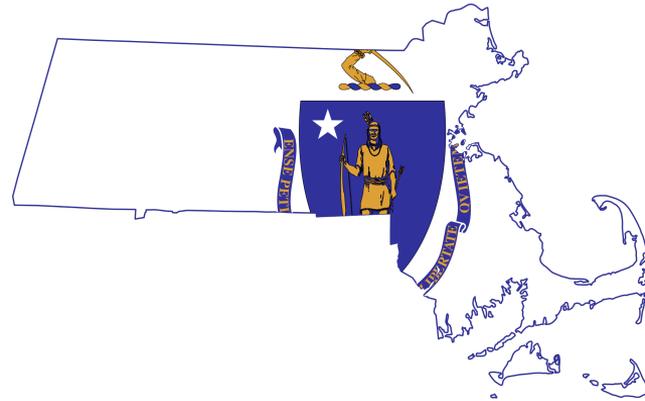
Fair Information Practice Principles

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

<p>PUBLIC LAW 100-618—NOV. 5, 1988 102 STAT. 3195</p> <p>Public Law 100-618 100th Congress</p> <p>An Act</p> <p>To amend title 18, United States Code, to preserve personal privacy in the rental, purchase, or delivery of video tapes or similar audio-visual materials, and for other purposes.</p> <p><i>Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,</i></p> <p>SECTION 1. SHORT TITLE.</p> <p>This Act may be cited as the "Video Privacy Protection Act of 1988".</p> <p>SEC. 2. CHAPTER 121 AMENDMENT.</p> <p>(a) IN GENERAL.—Chapter 121 of title 18, United States Code, is amended—</p> <p>(1) by redesignating section 2710 as section 2709;</p> <p>(2) by inserting after section 2709 the following:</p> <p>"§ 2710. Wrongful disclosure of video tape rental information.—(a) DEFINITIONS.—For purposes of this section—</p> <p>"(1) the term 'consumer' means any renter or subscriber of goods or services from a video tape rental service provider;</p> <p>"(2) the term 'ordinary course of business' means the collection activities, order fulfillment, request for transfer of ownership,</p> <p>"(3) the term 'personally identifiable information' means information which identifies a person as having obtained specific video materials or services from a video tape rental service provider; and</p> <p>"(4) the term 'video tape service provider' means any person engaged in the business, in or affecting interstate commerce, of rental, sale, or delivery of prerecorded cassette tapes or similar audio visual material, or other entity to whom a disclosure is made in accordance with paragraph (D) or (E) of subsection (b)(2), but only with respect to information contained in the disclosure.</p> <p>"(b) VIDEO TAPE RENTAL AND SALE RECORDS.—A video tape rental service provider who knowingly discloses, to any person, personally identifiable information concerning any consumer shall be liable to the aggrieved person for the redaction of such information under subsection (d).</p> <p>"(2) A video tape service provider may disclose personally identifiable information concerning any consumer—</p> <p>"(A) to the consumer;</p> <p>"(B) to any person with the informed, written consent of the consumer given at the time the disclosure is made;</p> <p>"(C) to a law enforcement agency pursuant to a subpoena issued under the Federal Rules of Criminal Procedure or an equivalent State warrant, a grand jury subpoena, or a court order;</p>	<p>100 STAT. 1848 PUBLIC LAW 99-508—OCT. 21, 1986</p> <p>Public Law 99-508 99th Congress</p> <p>Oct. 21, 1986 [H.R. 4932]</p> <p>Electronic Communications Privacy Act of 1986 18 USC 2510 note.</p> <p>To amend title 18, United States Code, to provide for the protection of communications, other than wire communications, from interception, and for other purposes.</p> <p><i>Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,</i></p> <p>SECTION 1. SHORT TITLE.</p> <p>This Act may be cited as the "Electronic Communications Privacy Act of 1986".</p> <p>TITLE I—INTERCEPTED COMMUNICATIONS</p> <p>RELATIONSHIP TO OTHER LAWS</p> <p>SEC. 101. FEDERAL PENALTIES.</p> <p>(a) DEFINITIONS.—(1) Section 101 of title 18, United States Code, is amended—</p> <p>(A) by striking out "an oral communication" in lieu of "a communication";</p> <p>(B) by inserting "(including switching station)" after "communication" after "or communications" and such term includes any communication, but such term does not include any communication transmitted by a cordless telephone communication system;</p> <p>(2) Section 2510(2) of title 18, United States Code, is amended—</p> <p>(A) by striking out "any communication" in lieu of "any communication, but such term does not include any communication transmitted by a cordless telephone communication system";</p> <p>(B) by inserting "or of a communication" after "or communications" and such term includes any communication, but such term does not include any communication transmitted by a cordless telephone communication system;</p> <p>(3) Section 2510(4) of title 18, United States Code, is amended—</p> <p>(A) by inserting "or of a communication" after "or communications" and such term includes any communication, but such term does not include any communication transmitted by a cordless telephone communication system;</p> <p>(B) by striking out "any communication" in lieu of "any communication, but such term does not include any communication transmitted by a cordless telephone communication system";</p> <p>(C) by adding at the end thereof the following: "(12) electronic communications, including signals, writing, images, or sounds, transmitted by a cordless telephone communication system";</p>	<p>15 U.S.C.A. § 6502</p> <p>§ 6502. Regulation of unfair and deceptive acts and practices in connection with collection and use of personal information from and about children on the internet</p> <p>Currentness</p> <p>(a) Acts prohibited</p> <p>(1) In general</p> <p>It is unlawful for an operator of a website or online service directed to children, or any operator that has actual knowledge that it is collecting personal information from a child, to collect personal information from a child in a manner that violates the regulations prescribed under subsection (b) of this section.</p> <p>(2) Disclosure to parent protected</p> <p>Notwithstanding paragraph (1), neither an operator of such a website or online service nor the operator's agent shall be held to be liable under any Federal or State law for any disclosure made in good faith and following reasonable procedures in responding to a request for disclosure of personal information under subsection (b)(1)(B)(iii) of this section to the parent of a child.</p> <p>(b) Regulations</p> <p>(1) In general</p> <p>Not later than 1 year after October 21, 1998, the Commission shall promulgate under section 553 of Title 5 regulations that—</p> <p>(A) require the operator of any website or online service directed to children that collects personal information from children or the operator of a website or online service that has actual knowledge that it is collecting personal information from a child—</p> <p>(i) to provide notice on the website of what information is collected from children by the operator, how the operator uses such information, and the operator's disclosure practices for such information; and</p>
--	--	---

State Laws



Section 5



General Data Protection Regulation (GDPR)



Potential GDPR Consent Screens

EXAMPLE OF A GDPR CONSENT REQUEST

SCENARIO: A WEBSITE REQUESTS CONSENT TO SHARE DATA WITH A BRAND FOR PRODUCT OFFERS

Pop-up Dialog

We would like to share your browsing habits on our site with **Brand Name and their analytics partners**, to understand what offers may be of interest to you.

These data will be deleted after 6 months. You can withdraw permission at any time in **My Data**. [Learn more?](#)

DETAILS OF RECIPIENTS AND CATEGORIES OF RECIPIENTS. TEXT LINKS TO CONTACT DETAILS OF THE CONTROLLER AND THEIR DATA PROTECTION OFFICER.
ARTICLE 13, PARA 1, A, B, AND E.

DURATION
ARTICLE 13, PARA 2, A.

CAN SAY NO
RECITAL 12.

PURPOSE OF PROCESSING, AND NOTIFICATION OF PROFILING.
ARTICLE 13, PARA 1, C, AND PARA 2, F.

TEXT LINKS TO TOOL FOR WITHDRAWING CONSENT.
ARTICLE 7, PARAGRAPH 3.

TEXT LINKS TO TOOL TO COMPLAIN TO SUPERVISORY AUTHORITY, AND TO ACCESS, CORRECT, AND TRANSFER DATA, ETC.
ARTICLE 13, PARA 2, B, C, AND D.

PageFair

TRACKING QUESTIONS THAT MUST BE ASKED AT INSTALLATION

BASED ON THE E-PRIVACY REGULATION DRAFT TEXT PROPOSED BY THE EUROPEAN COMMISSION, JANUARY 2019

Tracking Preferences

Accept all cookies

Accept only first party cookies

Reject all cookies

SELECT AN OPTION TO CONTINUE

THIS IS THE LIST OF OPTIONS DESCRIBED IN RECITAL 23, AND REQUIRED IN ARTICLE 10.

ARTICLE 10, PARA. 2, SAYS THAT A USER MUST SELECT AN OPTION BEFORE INSTALLATION CAN CONTINUE.

PageFair

TRACKING QUESTIONS THAT MUST BE ASKED AT INSTALLATION

BASED ON THE E-PRIVACY REGULATION DRAFT TEXT AMENDED BY THE EUROPEAN PARLIAMENT LIBE COMMITTEE'S RAPPORTUEUR'S DRAFT REPORT, JUNE 2019

Tracking Preferences

Accept all tracking

Accept only first party tracking

Reject tracking unless strictly necessary for services I request

Reject all tracking

AMENDED RECITAL 23 MAKES REJECTION OF THIRD PARTY TRACKERS AND COOKIES THE DEFAULT.

THIS IS PROPOSED IN RECITAL 23 AS AMENDED, BUT RECITAL 21 SAYS THAT CONSENT IS NOT REQUIRED FOR "TECHNICAL STORAGE OR ACCESS WHICH IS STRICTLY NECESSARY AND PROPORTIONATE FOR ... THE USE OF A SPECIFIC SERVICE EXPLICITLY REQUESTED BY THE USER".

PageFair

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):
 - <https://www.publicknowledge.org/news-blog/blogs/heres-how-congress-should-respond-to-facebook-cambridge-analytica>
- Letter to Congress re: Facebook Data Protection Hearing:
 - <https://www.publicknowledge.org/documents/letter-to-senate-judiciary-and-commerce-committees-on-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



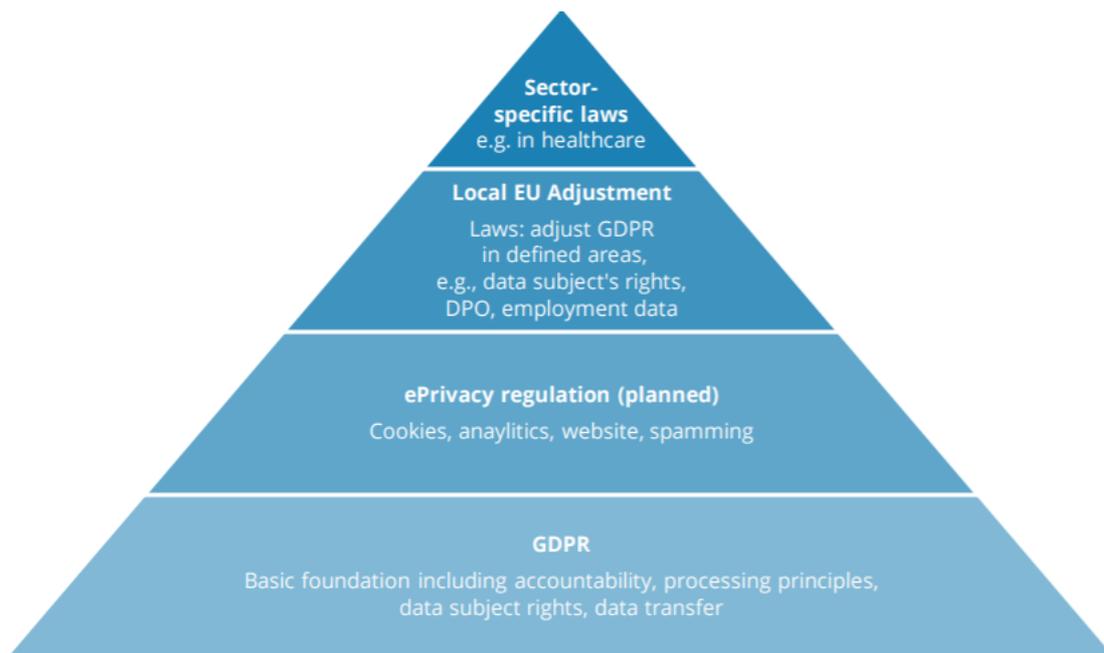
ARF
TOWNHALL
Research Ethics
Partnered with GreenBook

Review Coverage

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

* Treated in discussion with DAA

GDPR



Source: ANA ReedSmith

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)

Principles

- Chain of Trust
- Honesty
- Objective
- Integrity
- Quality

Participants

Mostly Research

- Delete PII asap
- No Selling
- No Direct Action
- Pre-Existing relation
 - No unsolicited email
 - Name Provider
- Indicate recontact
- Data Breach Notice
- Contractor level of care
- Consent to forward PII

Profession

- No unfair criticism
- Promote Trust
- Guideline (Casro & DMA) enforcement
- US EU Safe Harbor
- Report sponsorship
- Address Complaints

Clients

- Methods Description
- Sample stats
- Sources of error
- Audit available
- Report multi-client

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

DAA Self-Regulatory Principles (2009 - 2015)

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



DAA Self-Regulatory Principles (2009 - 2015)

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/> (Time.com)
 - Making a Science of Privacy Statements



Summary & Recommendation

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

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



Town Hall