



# Background Brief

---

HJR 21 (2015) - Study of Personal Information Ownership  
*State Administrative and Veteran's Affairs Interim Committee*

---

*Prepared by Sheri Scurr, Research Analyst,  
Montana Legislative Services Division  
April 19, 2016*

## **Self Regulation and the Online Collection of Personal Information for Behavioral Advertising**

### **Purpose and Scope**

This research brief offers background information for the committee's further examination of specific personal information ownership issues that the committee identified at its Feb. 10, 2016, meeting. The scope of this brief is limited to the topic of regulating online collection of a consumer's personal information for online behavioral advertising. Behavioral advertising is based on consumer profiles built by collecting information about consumers online. A glossary of terms relevant to this topic has been provided as an attachment. (See Glossary B.)

This brief seeks to answer the following questions:

- ▶ What are the stakes?
- ▶ What is the self-regulatory framework?
- ▶ Are the regulations and standards working?

### **What Are The Stakes?**

#### **E-commerce is a significant part of the world economy**

The e-commerce market place is big, really big, and getting bigger fast. American consumers spent \$186 billion through online transactions in 2010, and the number of online sales has been increasing dramatically since then.

Orangecollarmedia.com info graphic  
<http://visual.ly/online-shopping-statistics>

Worldwide, online retail spending was \$1.6 trillion (USD) in 2015, and this spending is projected to keep growing by double digit rates each year for the foreseeable future.

According to analysts for CNN, in 2012, big data was a \$300 billion-a-year industry and employed 3 million people in the United States.<sup>1</sup>

The e-commerce marketplace is also very competitive. Many retailers compete for the same consumers. However, the vast majority of online stores fail to generate significant revenue.<sup>2</sup>

LemonStand infographic  
<http://i1.wp.com/blog.lemonstand.com/wp-content/uploads/2015/06/eCommerce-Market-Size-Info-graphic.png?resize=639%2C1906>

## **Online behavioral advertising is critical for businesses to grow**

Given this lucrative but competitive market place, online businesses need to be smart about advertising. How much traffic a website experiences is directly related to the business's ability to generate revenue. But, attracting visitors to websites is only half the battle. The businesses must also attract the right customers -- those who not only visit the website, but who will ultimately purchase products. Online behavioral advertising helps online businesses not only attract more traffic on their websites, but also attract the consumer demographic most interested in their products.

Thus, the online behavioral advertising industry is a big business all its own. The industry consists of various types of companies that are not necessary ad companies, but include businesses that sell space for ads:

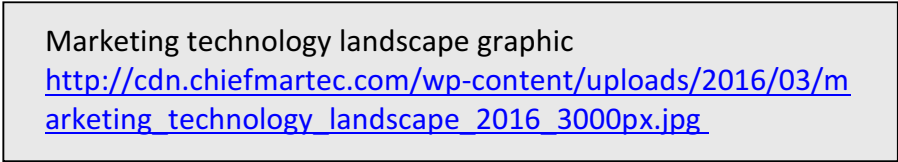
---

<sup>1</sup> Jason Morris and Ed Vavandera, "Why big companies buy, sell your data," August 23, 2012, CNN.com.

<sup>2</sup> Ross Paul, "Just How Big Is the eCommerce Market? You'll Never Guess", LemonStand online blog, June 26, 2015. LemonStand states that it is a blog for e-commerce professionals. The data source cited in the article is eMarketer, which provides research and information on how to do business in the digital world.

- ▶ Search engines, such as Google, Yahoo!, Bing, and others - who sell ad space for top of the page slots when search results are displayed.  
<https://www.google.com> (search for "data broker companies")
- ▶ Data collection, aggregation, and brokering companies such as:
  - Acxiom <http://www.acxiom.com/about-acxiom/>
  - Connotate  
[http://pages.connotate.com/data-aggregation-web-scraping.html?gclid=CI7o3Nb3\\_MsCFQiqQodpg8Eqw](http://pages.connotate.com/data-aggregation-web-scraping.html?gclid=CI7o3Nb3_MsCFQiqQodpg8Eqw)
  - Import.io <https://www.import.io/> (web scraping)
- ▶ Data analytics companies
  - Slide Show of top 10  
<http://www.eweek.com/c/a/Enterprise-Applications/10-Hot-Data-Web-Analytics-Companies-That-You-Should-Know-781120>
  - Google Analytics - FAQ on Data Sharing  
<https://support.google.com/analytics/answer/1011397?hl=en&rd=1>
- ▶ Ad serving companies, such as:
  - AdRoll home <https://www.adroll.com>
  - Google Ads <https://www.google.com/ads/>
  - AdServices <http://www.adservices.net/internet.php>

These are just a few companies in a vast universe of online content and advertising companies.



## Consumer concerns and risks

A survey conducted by the Pew Research Center in 2014 found:

- ▶ 91% of adults in the survey "agree" or "strongly agree" that consumers have lost control over how personal information is collected and used by companies.

- ▶ 61% of adults in the survey "disagreed" or "strongly disagreed" with the statement: "I appreciate that online services are more efficient because of the increased access they have to my personal data."
- ▶ 21% of internet users said they had an email or social networking account compromised or taken over without their permission.
- ▶ 12% reported they had been stalked or harassed online.
- ▶ 11% reported they had important personal information stolen such as their Social Security Number, credit card, or bank account information.
- ▶ 6% said they had their reputation damaged because of something that happened online.
- ▶ 6% said they had been the victim of an online scam and lost money.
- ▶ 4% said they had something happen online that led them into physical danger.<sup>3</sup>

Other research notes:

- ▶ The FTC's top consumer complaint is identity theft.<sup>4</sup>
- ▶ Cybercrime affected 12.7 million Americans in 2014 and caused \$16 billion in losses.<sup>5</sup>

---

<sup>3</sup> See Lee Rainie, Sara Kiesler, Ruogu Kang, and Mary Madden, "Anonymity, Privacy, and Security Online", Pew Research Center, September 5, 2013. See also, Pew Research Center, "Public Perceptions of Privacy and Security in the Post-Snowden Era," November 12, 2014.

<sup>4</sup> Reported on the ReputationDefender webpage at <https://www.reputationdefender.com/privacy>. The website attributes this information to Javeline Research.

<sup>5</sup> Reported on ReputationDefender website at <https://www.reputationdefender.com/privacy>. The website attributes this information to the FTC.

## Privacy protection is also a business interest

A survey by Pew Research Center found that 86 % of Internet users surveyed said they have tried various ways to minimize their online "footprints", such as clearing cookies, encrypting their email, avoiding using their real name, or using virtual networks that mask their internet protocol (IP) addresses.<sup>6</sup>

No surprisingly then, various privacy and security companies have been responding to the increasing demand for better online privacy and security products, not only for individual consumers, but also for business. Some of these companies provide services, some provide software, and some offer products or information to "expose the dark underworld" of online tracking.

Some examples are listed below:

- ▶ Article in PCWorld, Best Free Software  
[http://www.pcworld.com/article/237027/best\\_free\\_software\\_for\\_protecting\\_your\\_pc\\_and\\_your\\_privacy.html](http://www.pcworld.com/article/237027/best_free_software_for_protecting_your_pc_and_your_privacy.html)
- ▶ PrivacyPC - 2016 Best Internet Privacy Software Review  
<http://privacy-pc.com/internet-privacy-software-review>
- ▶ Ghostery - helping businesses help consumers to control online tracking  
<https://www.ghostery.com/about-us/about-ghostery/>  
- See privacy policy related to free products - Section II - "Opt-in"
- ▶ Abine  
<https://www.abine.com/index.html>
- ▶ ReputationDefender  
<https://www.reputationdefender.com/>  
- note website requests personal information for free consultation - also note the use and disclosure, tracking technologies, and choice and opt out sections

---

<sup>6</sup> See Lee Rainie, Sara Kiesler, Ruogu Kang, and Mary Madden, "Anonymity, Privacy, and Security Online", Pew Research Center, September 5, 2013.  
<http://www.pewinternet.org/2013/09/05/anonymity-privacy-and-security-online/>

- ▶ Disconnect Me  
<https://disconnect.me/trackerprotection#trackers-we-dont-block>  
- note security risk warning for this site
- ▶ StopDataMining.Me  
<http://www.stopdatamining.me/>  
- note this website's privacy policy

It should be noted that while many privacy protection companies are legitimate and offer great products, many are less reputable. Many are themselves mining data and some websites, such as disconnect.me and stopdatamining.me are themselves security risks.

## What is the Self-Regulatory Framework?

This section discusses the self-regulatory framework for the online data collection and behavioral advertising industries. Recommended standards of practice are established by international groups, the FTC, and business associations.

### EU-U.S. Privacy Shield

---



A U.S. company collecting personal information about Europeans and transmitting that data to the U.S. may voluntarily participate in the EU- U.S. Privacy Shield. This framework replaces the Safe Harbor framework, but essentially incorporates the same principles and standards of practice,<sup>7</sup> plus a few more. The main *new* requirements for participating companies are as follows:

- ▶ A Privacy Shield participant must include in its privacy policy a declaration of the organization's commitment to comply with the Privacy Shield Principles, so that the commitment becomes enforceable under U.S. law.

---

<sup>7</sup> See Part 2 - Policy Principles in a previous legislative staff paper: Legislative staff report by Sheri Scurr: "[HJR 21 - Property Rights Theory, Policy Principles, and Options for Further Study](#)," Feb. 10, 2016.

- ▶ When a participant's privacy policy is available online, it must include a link to the Department of Commerce's Privacy Shield website and a link to the website or complaint submission form of the independent recourse mechanisms that is available to investigate individual complaints.
- ▶ A participant must inform individuals of their rights to access their personal data, the requirement to disclose personal information in response to lawful request by public authorities, which enforcement authority has jurisdiction over the organization's compliance with the Framework, and the organization's liability in cases of onward transfer of data to third parties.<sup>8</sup>

A participant must annually self-certify to the U.S. Department of Commerce that the company complies with the Privacy Shield principles. Consumers may check which companies have self-certified compliance and check up on the current status of their certification by going to the following website:

<https://safeharbor.export.gov/list.aspx>

## Asia-Pacific Economic Cooperation (APEC)

---



The U.S. government also participates in the APEC Cross Board Privacy Rules (CBPR) system. According to the CBPRs website, it is "a voluntary accountability-based system to facilitate privacy-respecting data flows among APEC economies." One component of this system is a regulatory cooperative arrangement to ensure that each of the system's program requirements can be enforced by participating APEC economies.

There are currently four participating APEC CBPR system economies: the United States, Mexico, Japan, and Canada. <http://www.cbprs.org/>

APEC has published its own privacy framework:

<http://www.cbprs.org/GeneralPages/PrivacyinAPECRegion.aspx>

---

<sup>8</sup> U.S. Department of Commerce, Fact Sheet: Overview of the EU-U.S. Privacy Shield Framework, Feb. 29, 2016. Available at <https://www.commerce.gov/news/fact-sheets/2016/02/fact-sheet-overview-eu-us-privacy-shield-framework>.

## Organization for Economic Co-operation and Development (OECD)



The OECD is an intergovernmental organization comprised of 29 member countries, including the United States. Discussions at the OECD produce guidelines that sometimes evolve into formal agreements. With respect to the Internet, the OECD states its objective is to: "Provide policy guidance on how to maximize the benefits of the data-driven economy, while mitigating the associated risks." <sup>9</sup>  
<http://www.oecd.org/about/>

The OECD publishes reports and guidelines related to online consumer privacy:  
<http://www.oecd.org/sti/ieconomy/privacy.htm>

## Federal Trade Commission (FTC)



PROTECTING AMERICA'S CONSUMERS

The FTC is an independent government agency established by Congress. It's Office of Technology Research and Investigation under the

Bureau of Consumer Protection investigates complaints and may prosecute companies for violations of federal laws related to online privacy and data security, including connected cars, smart phones, algorithmic transparency, payment technologies, fraud, big data, and "the Internet of Things".  
<https://www.ftc.gov/about-ftc/bureaus-offices/bureau-consumer-protection/of-fice-technology-research-investigation>

The Office of Consumer Protection offers tips and advise for businesses and hosts workshops, conferences, and webinars.

The FTC staff recently released a report entitled "the Internet of Things: Privacy & Security in a Connected World" (January 2015). The report summarizes a workshop with various stakeholders and staff recommendations for best practices related to the long-standing Fair information Practice Principles (FIPPs).

<https://www.ftc.gov/news-events/press-releases/2015/01/ftc-report-internet-t-hings-urges-companies-adopt-best-practices>

---

<sup>9</sup> See the following web page for a list of current membership, which includes the United States: <http://www.oecd.org/about/membersandpartners/>.



## **Internet Policy Task Force (Dept. of Commerce)**

---



Headed by the Department of Commerce, the Internet Policy Task Force includes that National Telecommunications and Information Administration, the Patent and Trademark Office, the National Institute of Standards and Technology, and the International Trade Administration. The task force provides advise offers standards of practice in several areas, including online privacy.

<https://www.ntia.doc.gov/category/internet-policy-task-force>

In 2010, the task force issued a "green paper" that outlined the task force's recommendations for data privacy based on the Fair Information Practice Principles.

<https://www.ntia.doc.gov/report/2010/commercial-data-privacy-and-innovation-internet-economy-dynamic-policy-framework>

On April 5, 2016, the Department of Commerce announced it was launching a broad review of consumer privacy policy and the Internet economy, sending out a "notice of inquiry" requesting comments. The NOI asks a series of questions related to Internet privacy policies and Internet commerce.

<https://www.ntia.doc.gov/federal-register-notice/2016/rfc-potential-roles-government-fostering-advancement-internet-of-things>

## **Digital Advertising Alliance (DAA)**

---



According to the DAA website: "The Digital Advertising Alliance (DAA) establishes and enforces responsible privacy practices across industry for relevant digital advertising, providing consumers with enhanced transparency and control. Through multifaceted Principles that apply to data gathered from a particular device in either the desktop or mobile environments, the DAA program addresses practices for multi-site data collection and use. The DAA is an independent non-profit organization led by the leading advertising and marketing trade associations."

<http://www.aboutads.info/>

The DAA established self-regulatory principles fo multi-site and cross-app data collection, mobile devises, and online behavioral advertising.

<http://www.aboutads.info/principles>

The DAA does not have a stand-alone enforcement program. Rather, the DAA

website states the DAA works in cooperation with the Direct Marketing Association and the Council of Better Business Bureaus. The website has a link where complaints may be reported. <http://www.aboutads.info/enforcement>

The following types of companies participate in the DAA: advertising, auto dealers, consumer packaged goods, financial services, health and pharmaceutical, media and publishing, retail, technology, telecommunications, travel and hospitality, and various others. Participating companies are listed on the DAA website at: <http://www.aboutads.info/participating>

## **Network Advertising Initiative (NAI)**

---



According to the NAI "about us" web page: NAI is a non-profit organization that is the leading self-regulatory association dedicated to responsible data collection and its use for digital advertising. Since 2000, we have been working with the leaders in online advertising to craft policies that help ensure responsible data collection and use practices. The result is the development of high standards that are practical and scalable to benefit everyone."

<https://www.networkadvertising.org/>

Members of the NAI must adhere to a code of conduct, and NAI says it has a "robust" compliance program that includes sanctions. According to NAI, its self-regulation program is the "gold standard" for self-regulation of third-party advertising, ad tech, and related businesses.

<https://www.networkadvertising.org/code-enforcement>

NAI states its membership includes more than 100 companies. Its members are listed on its website:

<https://www.networkadvertising.org/participating-networks>

## **Interactive Advertising Bureau (IAB)**

---



The IAB states that its mission is to empower the media and marketing industries to thrive in the digital economy. According to its website: "It is comprised of more than 650 leading media and technology companies that are responsible for selling, delivering, and optimizing digital advertising or marketing campaigns. Together, they account for 86 percent of online advertising in the United States. Working with its member companies, the IAB develops technical standards and best practices and fields critical research on interactive advertising, while also educating brands, agencies, and the wider business community on the importance of digital marketing."

<http://www.iab.com/our-story/>

The IAB also has a mandatory code of conduct for its members and offers compliance programs.

<http://www.iab.com/guidelines/understanding-iab-compliance-programs/>

## **Is Self-Regulation Working?**

[ To Be Researched ]