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

Online Tracking: A Crash Course

Purpose and Scope

This research brief offers a basic foundation for the committee's further examination of specific personal information ownership issues that the committee identified at its Feb. 10, 2016. The scope of this brief is limited to the topic of tracking individuals when they use the Internet. A glossary of Internet-related terms (Glossary A) has been provided as an attachment.

This brief seeks to answer the following questions:

- Why are we tracked?
- How are we tracked?
- Who is tracking us?
- What tools are available to prevent or manage online tracking?

Why are we tracked?

There are legitimate reasons for tracking a person's online activity:

- To help us navigate the Web.
- To make websites work.
- To improve our future experiences with web-based services.
- To build and improve businesses.

There are also illegitimate and illegal reasons for online tracking:

- To commit fraud and financial crimes (e.g., identity theft, scams, extortion).
- To commit and act of cyberterrorism to intimidate and disrupt society.

- To conduct cyberwarfare, which is the term used to describe cyber attacks against another country's interests;
- To stalk, harass, or prey on someone (e.g, cyberbullying, revenge porn, soliciting sex).

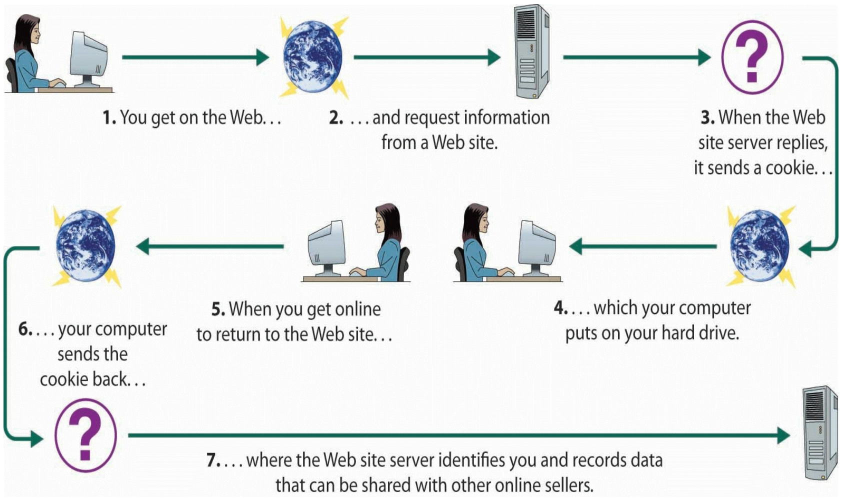
Legislation aimed at regulating the playing field for those with legitimate reasons to track consumers online will likely be different than legislation aimed at deterring or penalizing "bad actors" with less than honorable intentions.

How are we tracked?

Cookies

The most commonly used method for online tracking relies on a technology called a cookie. The term "cookie" evolved from a programer/developer who initially called the new technology a "magic cookie", harkening back to fortune cookies -- the cookies with a message inside.

Cookies are files with data inside. They allow website and browsing information to be remembered. When a person visits a website, cookies are sent from a data server linked to the website to the user's browser. The browser stores the cookies on the computer for future use. When the user gets back online and opens a previously visited website, the browser sends the cookie back to the data server for that website, and the information cycle of sending and receiving cookies continues.


1. You get on the Web. . .
2. . . . and request information from a Web site.
3. When the Web site server replies, it sends a cookie. . .
4. . . . which your computer puts on your hard drive.
5. When you get online to return to the Web site. . .
6. . . . your computer sends the cookie back. . .
7. . . . where the Web site server identifies you and records data that can be shared with other online sellers.

Source: www.flatworldknowledge.com

Cookies are not software programs and cannot direct a computer to perform a specific task or function.

Cookies may be referred to by their purpose or use, for example there are:

- preference cookies - to remember settings.
- security cookies - to authenticate users through login credentials and passwords.
- process cookies - to help users navigate and interact with the website.
- tracking cookies - used by advertisers, analytics companies, and data brokers to track users between websites.
- advertising cookies - a type of tracking cookie, deliver ads and track interests.
- analytics cookies - a type of tracking cookies that helps website owners understand their customers and measure website effectiveness.

Cookies may be either of the following types:

- a first-party cookie - directly related to the website the user is visiting (i.e, the website domain attribute for the cookie will match the website domain name of the website); or

- a third-party cookie - related to a domain or organization that is different than the one the user sees in the address bar for the website being visited. Third parties include advertisers, data analytics companies, data broker companies, and others organizations.

Examples of third-party cookies are:

- Flash cookies - developed by Adobe to track user preferences in Flash applications that support website content such as videos, animation, and other types of images.

- DoubleClick cookies - developed by a Google subsidiary to facilitate third-party advertising.

- Webtrends cookies - an analytics tool.

Cookies may be temporary or more permanent, and some may be easy to remove or more difficult to remove, such as:

- session cookies - used to remember only the current online session.

- persistent cookies - used to allow a more long-term memory, but, if they are traditional cookies, they may expire or be deleted.

- zombie cookies - a nontraditional cookie that recreates itself even after it has been deleted.

Alternatives to cookies

There are ways to track consumers online without using cookies. And, more alternatives are being developed because several types of cookies cannot be supported on mobile devises. Many of these alternative technologies and methods are less efficient than cookies, but are ways user information may be collected even if cookies are deleted or blocked.

Some of these alternatives are as follows:

- using an IP address.
- embedding a query string into a URL address http://example.com/over/there?name=ferret.
- using a web form with a hidden field to retain information.
- using a document object model (DOM) application.
- HTTP authentication.
- using an IDFA (an identifier for advertisers) that is assigned to every person who buys a particular devise, such as an Apple iPad or iPhone that can be used by the Apple's advertising network to track what ads that user is viewing with that devise.
- ETags, which are cached by the browser.
- Web storage capabilities used by a particular browser to remember browser history and favorites, including browser plug-ins that store user data.
- a browser fingerprint, which is information collected about a browser's configuration that allows that devise or user to be identified.
- planting a web beacon, which is an object embedded in a web page or email that is typically invisible to the user and that sends a "signal" when a user has accessed certain content.
- pixel tags, which is a type of beacon in an image embedded on a website.

Software (e.g., Adware, Malware, and Spyware)

Software may also be used to collect personal information and track online consumer behavior. Special software programs are called "applications" (apps). Software is a series or package of instructions that directs a computer to perform specific tasks or operations. For example, software allows a computer to receive and play movies (e.g., Windows Media Player 12), assists business accounting (e.g., QuickBooks), and allows individuals to send and receive e-mail (e.g., Microsoft Outlook).

Adware - Software that performs certain functions for advertisers, such as serving an ad to a specific website that is being visited by a certain consumer who has been identified as part of a particular consumer group, is called "adware". Adware may be installed on a computer as part of a bundle of software that a consumer purchases or it may be embedded into a free download.

Malware - Unwanted or maliciously installed software is called "malware". A computer virus is a type of malware that replicates itself and spreads within the user's computer like an infection.

Spyware - Spyware is a type of software that gathers personal information without the individual's knowledge or consent. Some spyware may even assert control over a computer without the consumer's knowledge.

Who is Tracking Us?

Legitimate online tracking is done at every level and by a variety of different organizations:

- Companies or organizations with a product, service, or responsibility, ranging from small business owners to multi-national corporations, and from media companies to government agencies.

- Companies that host websites, such as iPage and GoDaddy.

- Companies that provide browsers and search engines, such as Google Chrome, Internet Explorer, Yahoo, and Firefox.

- Companies that specialize in advertising.

- Companies that specialize in buying and selling consumer data (e.g., data brokers).

- Analytics companies, such as those that specialize in analyzing website traffic and consumer behavior.

Unfortunately, hackers seeking to steal personal information use the very same tools and technologies used by legitimate businesses.

How can we block or limit online tracking?

A variety of tools are available to Internet users to manage or block online tracking. Some of these tools are mentioned in a video by MonkeySee, a company that produces free online instructional videos arranged into 23 categories covering topics ranging from auto mechanics to parenting and from city guides to safety. The following is a link to a video entitled *How to Protect Yourself From Online Tracking.* (Note the MonkeySee privacy policy before viewing this video.)
https://www.youtube.com/watch?feature=player_detailpage&v=ISjH6gbEb-Y

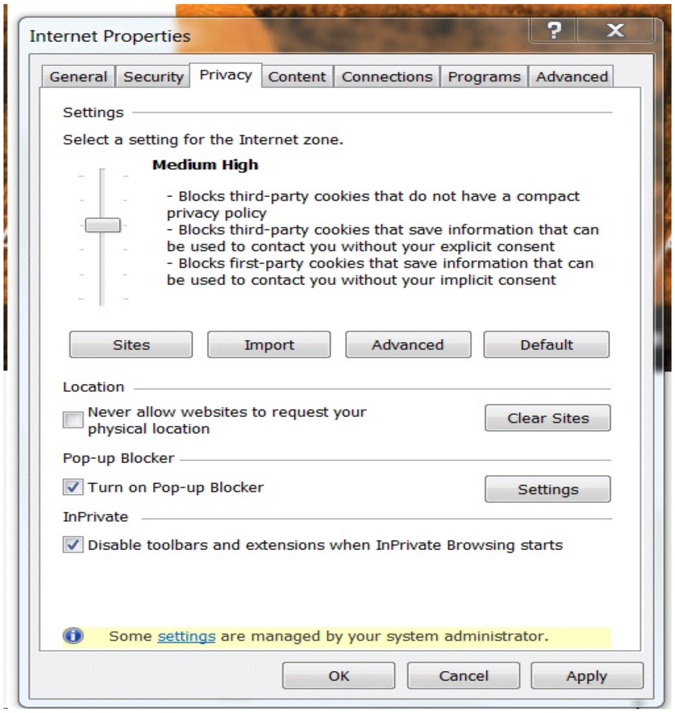
> [This section includes watching the video and then an online demonstration about MonkeySee's website terms and conditions and privacy policy. The demonstrates starts at http://www.monkeysee.com.]

To recap some of the tools mentioned in the MonkeySee video, there are several tools available to Internet users to may manage tracking cookies. These tools are outlined below.

[go to next page]

Browser tools

- Delete the browsing history
- Enable "private browsing", which prevents the browser from storing some data
- Enable a "do not track" option, which sends a signal to websites you visit, but which may not be honored by the website
- Change the browser's privacy settings



Internet Properties

General | Security | Privacy | Content | Connections | Programs | Advanced

Settings

Select a setting for the Internet zone.

Medium High

- Blocks third-party cookies that do not have a compact privacy policy
- Blocks third-party cookies that save information that can be used to contact you without your explicit consent
- Blocks first-party cookies that save information that can be used to contact you without your implicit consent

Sites | Import | Advanced | Default

Location

□ Never allow websites to request your physical location

Clear Sites

Pop-up Blocker

☑ Turn on Pop-up Blocker

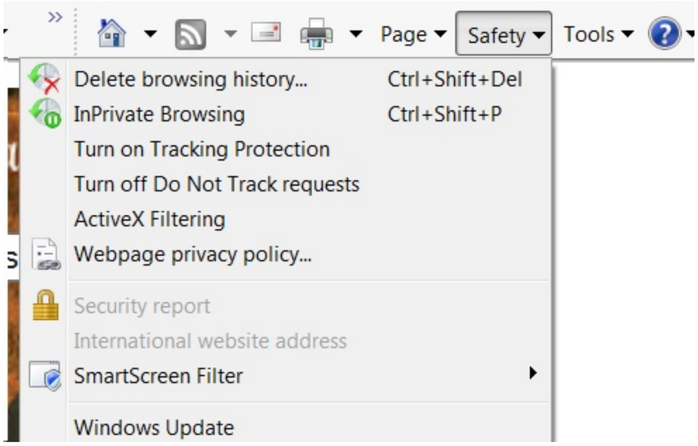
Settings

InPrivate

☑ Disable toolbars and extensions when InPrivate Browsing starts

Some settings are managed by your system administrator.

OK | Cancel | Apply


Page
Safety
Tools
Delete browsing history... Ctrl+Shift+Del
InPrivate Browsing Ctrl+Shift+P
Turn on Tracking Protection
Turn off Do Not Track requests
ActiveX Filtering
Webpage privacy policy...
Security report
International website address
SmartScreen Filter
Windows Update

Search engine tools

Users may change their privacy settings related to their browser's search engine. Some require a download of "add-on" software to the search engine.

[This section includes an online demonstration of Google's privacy policy and how this process works. The demonstration starts at https://www.google.com.]

E-mail tools

E-mail programs, whether free (Gmail or Yahoo!) or purchased (Outlook in Microsoft Office) have privacy settings that customers may use to control some aspects of tracking.

Yahoo!'s Privacy Center:
https://policies.yahoo.com/us/en/yahoo/privacy/index.htm

Gmail - Google Safety Center:
https://www.google.com/safetycenter/everyone/start/gmail/

Outlook: [staff demonstration on Legislative Services Division account.]

Tools on the visited website

An individual website/business owner may offer a user the opportunity to manipulate user preferences.

[This section includes an on online demonstration of Amazon's website tools. The demonstration starts at https://www.amazon.com.]

Software packages

Various tech companies offer special software designed to block or limit online tracking. Some software is offered as a free download, others must be purchased. Also, the software available may be available as a stand alone package or as an add-on or enhancement to an existing program.

The following are some examples of this specialized software:

- Ad blockers, such as from Adblock Plus - https://adblockplus.org/

- Cookie blockers, such as the TrackerBlock add-on for the Firefox search engine https://addons.mozilla.org/en-US/firefox/addon/trackerblock/

- Encryption services, such as AxCrypt, a free tool for Windows http://www.axantum.com/AxCrypt/

- Deletion of personal information from the Web, such as DeleteMe https://www.abine.com/deleteme/landing.php

- Firewalls, such as SpyShelter Firewall - https://www.spyshelter.com/spyshelter-firewall

- Password managers - such as compared by PCMag.com

Conclusion

Online tracking is conducted using a variety of technologies for a variety of reasons. Tracking is necessary if consumers wish to participate in the online ecosystem. Unfortunately, bad actors use the same tracking technologies that are necessary for legitimate businesses to operate.

Consumers have access to a vast array of tools for blocking and managing certain types of online tracking. However, navigating this online tracking ecosystem takes time, technical saavy, and strong motivation. And, some of these tools may not be sufficient safeguards against hackers.

Informed policymaking concerning online tracking requires at least a basic understanding of this ecosystem and appreciation for dynamics involved:

- Various local, national, and international businesses that have built their businesses relying on online tracking.

- A vast array of developing technologies for online tracking, not just cookies.

- Consumer interests that range from expectations for functional websites, access to information, and smooth transactions, to an expectation of privacy and control over their own personal information.

Hopefully this research brief has helped map some of the basics that will help inform the committee's further examination of specific issues under HJR 21.