Jan 29th, 2:00 PM - 2:45 PM

Just Because I'm Paranoid Doesn't Mean I'm Not Being Followed: Using Tracking or Rather Do Not Track Features

Sharon Bradley
University of Georgia School of Law, bradleys@uga.edu

2016

Just Because I'm Paranoid Doesn't Mean I'm Not Being Followed:

USING TRACKING OR RATHER DO NOT TRACK FEATURES

SHARON BRADLEY, UNIVERSITY OF GEORGIA SCHOOL OF LAW, ATHENS, GA

➤ There is an online research guide that supplements this paper with additional information and web links: **libguides.law.uga.edu/cle2016**

_____

Just Because I'm Paranoid Doesn't Mean I'm Not Being Followed: Using Tracking or Rather Do Not Track Features

Sharon Bradley, J.D., M.L.S.
Special Collections Librarian
Alexander Campbell King Law Library
University of Georgia School of Law
Athens, Georgia

Table of Contents

In 2013 the American Bar Association formally approved a change to the Model Rules of Professional Conduct making it clear that lawyers have a duty to be competent not only in the law and its practice, but also in technology. More specifically, the ABA's House of Delegates voted to amend Comment 8 to Model Rule 1.1, which pertains to competence, to read as follows:

> **Rule 1.1 Competence - Comment**
>
> **Maintaining Competence**
>
> [8] To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, *including the benefits and risks associated with relevant technology*, engage in continuing study and education and comply with all continuing legal education requirements to which the lawyer is subject. (Emphasis added.)

By the end of 2015, 20 states had made changes to their own rules of conduct to reflect the importance of technical competence. See the list on the research guide.

Every office should have an information/data security plan and a program for training employees, including continuing education. How much or how complex such a plan needs to be depends on the office itself. But common elements include:

- Protection of personal identification information, which includes institution of a complex password policy
- A social media policy governing all employees, to avoid voluntary or involuntary disclosure of sensitive information
- Document security, in-house and/or with cloud computing
- General internet use

A part of the discussion of internet use is that everyone in the office understands tracking and how to protect individual employee privacy and client privacy.

Generally when people think "tracking" they picture the efforts of marketers and retailers to get you to see their ad, click on it, and buy something. This is referred to as

➤ There is an online research guide that supplements this paper with additional information and web links: **libguides.law.uga.edu/cle2016**

_____

targeted advertising.[1] Every company that advertises online wants to know what sites you visit, what you buy, who your friends are, and what you like. By gathering information about your online activities they can serve you targeted ads that are more likely to entice you to buy something. It's about attracting customers who will buy what they're selling. It's annoying, boxes get in the way, but it's also what makes much of the internet free.

For instance, the Facebook, Twitter, and Google+ buttons you see on just about every site allow those networks to track you even if you don't have an account or are logged into them. Information collection companies also rely on embedded code in banner ads that track your visits, preferences, and demographic information.

The darker aspects of tracking deal with attempts to gain private information, to access bank accounts, and to steal identities. Attorneys are in a unique position, not only do they need to be concerned about their personal privacy but also that of their clients. The best suggestion is to use a layered approach to protecting personal and client privacy. You might follow higher level and more complex techniques for your office than for home. There are a number of tools and the more tools you use the tighter your protection becomes. I'll discuss a few techniques in this paper/presentation but there is more information in the research guide.

[1] Also referred to as behavioral targeting. Website publishers and advertisers want to increase the effectiveness of their advertising using user web-browsing behavior information. The web sites and individual pages you visit, the amount of time you view each page, the links you click on, and the things you interact with are collected and analyzed and a profile is created. Factors like geography, demographics, or contextual web page content can also be included to further flesh out your profile. It's this profile that determines what ads are pushed at you.

➤ There is an online research guide that supplements this paper with additional information and web links: **libguides.law.uga.edu/cle2016**

_____

Tracking

Tracking refers to the way third–parties like advertising companies, online marketers, market researchers, affiliate marketers, analytics services, etc., learn about how you interact with websites. Your online activity, which includes clicks, searches, sites you visit, products you buy, your location (estimated by your IP address), is tracked by various third-parties. This helps these sites offer personalized (targeted) content like ads or recommendations, but it also means that your browsing activity is being collected. It is often shared with or sold to other companies. We've all had the experience of browsing on sites and seeing ads from online stores we patronize. They're not guessing, they know what we buy, even what we covet. It's one thing to deal with your personal privacy but lawyers have the additional ethical responsibility to protect the privacy of their clients.[2]

Rule1.6 Confidentiality of Information

(c) A lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client.

Is there really a risk? The easy answer is probably the bigger you are the more at risk you are. Cybersecurity firm Mandiant, a division of FireEye, reports at least 80 of the 100 biggest firms in the country, by revenue, have been hacked since 2011.[3]

---

[2] See the *ABA Cybersecurity Handbook* which discusses the lawyer's duty to gain and maintain competence about the technology they use so as to be able to protect their client's confidential information. Continued learning is needed to keep up with technology advances and it may be necessary to get help from an outside information security expert.

[3] Susan Hansen, *Cyber Attacks Upend Attorney-Client Privilege: Security experts say law firms are perfect targets for hackers*, Bloomberg Businessweek, Mar. 19, 2015,

➤ There is an online research guide that supplements this paper with additional information and web links: **libguides.law.uga.edu/cle2016**

_____

Information security experts believe law firms are increasingly popular targets for cybercrime for two primary reasons

One, cyber criminals are thinking laterally and using third-parties to gain access to their real target, corporations and financial institutions. Analysis of security breaches, like those at Target and Home Depot, are revealing the connections with third-party service providers. This includes outside law firms because of the data with which they are entrusted. Two, law firms handle sensitive data which generally contains personal data. This can include patent or trademark filings (intellectual property), corporate transactions and reports, mergers and acquisitions, and lawsuit data.

Cookies

The first level of any security efforts involve your web browser. Blocking or deleting computer cookies is basic. A cookie is the information given to a Web browser by a Web server. Its main purpose is to identify users and possibly prepare customized Web pages or save site login information for you. There are two types of cookies:

Session cookie

- Also called a transient cookie
- Erased when you close the Web browser
- Stored in temporary memory and not retained after the browser is closed
- Does not collect information from your computer
- Typically store information in the form of a session identification that does not personally identify the user

Persistent cookie

- Also called a permanent cookie or a stored cookie

---

http://www.bloomberg.com/news/articles/2015-03-19/cyber-attacks-force-law-firms-to-improve-data-security

➤ There is an online research guide that supplements this paper with additional information and web links: **libguides.law.uga.edu/cle2016**

_____

- Stored on your hard drive until it expires or deleted
  - Cookie creator sets the expiration date
- Collect identifying information about the user
  - Web browsing behavior
  - Preferences for a specific Web site

In and of themselves cookies are not dangerous. They generally make surfing more seamless, and help websites operate more efficiently and therefore with greater profitably. There are legitimate concerns about the ways cookies can be used to follow users from one site to another, forming profiles. Many believe this is a privacy violation, and in the wrong hands the information could be exploited for questionable purposes. Every user has the power to decide for themselves whether to accept cookies, whether to block certain types, and how often to purge them. Most browsers, as well as many Internet security products, give users relatively easy and flexible control over all of these decisions.

Supercookies

Ad companies have a way to track you, even if you delete cookies, using Local Shared Objects (LSO), also known as supercookies.

A supercookie is designed to be permanently stored on a user's computer. Super cookies are generally more difficult for users to detect and remove from their devices because they cannot be deleted directly in the browser (though some plugins may work).

The research guide has instructions on blocking cookies for the most popular browsers.

Do Not Track

Do Not Track (DNT) is an HTTP header that asks a web application to not track you. DNT was proposed in 2009 and first implemented in Microsoft's Internet Explorer, later followed by Mozilla Firefox, Apple's Safari and Opera. It is much like the Do Not

➤ There is an online research guide that supplements this paper with additional information and web links: **libguides.law.uga.edu/cle2016**

———————————————————————

Call registry, which allows people to opt out of marketing calls.[4] When you enable DNT in your browser, it sends a DNT header in the web request. When this header is processed by websites, they learn that you do not want to be tracked.

The DNT header supports three values:

1. 1 (DNT : 1) for Tracking Prohibited (User rejects being tracked)
2. 0 (DNT : 0) for Tracking Allowed (User accepts being tracked)
3. null, if user has not set any preference (User not choosing)

DNT tells third-parties (not first-party) not to track you. When you visit a website, various third-parties (ad networks, analytics services) will try to learn about your activities. With DNT enabled in your browser, they'll be notified that you do not want to be tracked. If the third-party honors the DNT system, then it will not track you or place cookies in your browser for tracking purposes.

DNT will not stop ads. You'll continue to see ads on websites but the ads will be more generic and less behavioral. You'll still be tracked by first-parties like Google when you visit their web services, GMail, Google Search, etc. It also will not stop tracking from social plugins that pull in content or controls from services like Twitter, Facebook, Google+, Pinterest, etc. If you have an account with them, they will consider themselves as 'first-party' and still track users with DNT enabled. Also, DNT will not stop companies like Facebook from tracking their members through 'Like' buttons and other methods.

[4] https://www.donotcall.gov/. The registry was created by the Do-Not-Call Implementation Act of 2003 (Public Law No. 108-10, was H.R. 395 of the 108th Congress, and codified at 15 U.S.C. § 6101 et. seq.)

➤ There is an online research guide that supplements this paper with additional information and web links: **libguides.law.uga.edu/cle2016**

_____

Currently, DNT is a proposed technology standard based on an honor system. If the third-party honors the system, they will not track you once you have enabled the option. If they do not honor the standard then you will be tracked. Unlike the Do Not Call registry, DNT is not backed by any regulatory or legislative authority. It is a purely voluntary effort from the technology community comprising the online advertising industry, web developers and, privacy advocates. Also, users who do not want to be tracked must enable DNT in every browser and device they use, in smartphones, tablets, laptops, or desktop computers.

At this point in time privacy is still be in the marketers' hands until DNT is supported by most companies in the technology community. It is more likely that legislative action will be required before we can expect a broad application of Do Not Track.

Incognito Browsing

The term incognito browsing, also referred to as private browsing, covers a wide array of precautions that internet users can take to ensure that their activity on the Web cannot be traced. It differs from non-private browsing because the history of an incognito session is not saved to the hard drive. When browsing incognito, cache or cookies are not left behind to provide footprints of where you have been.

For purposes of this paper/presentation I want to distinguish between private or incognito browsing and online anonymity. The first, incognito browsing, is a feature that is utilized through your web browser. The second, anonymity, allows you to hide your IP

➤ There is an online research guide that supplements this paper with additional information and web links: **libguides.law.uga.edu/cle2016**

_____

address. This can be done by using a web proxy, a Virtual Private Network (VPN) or Tor, a free open network that routes your activity through a series of world-wide servers, operated by volunteers, before sending it to your destination.

No doubt privacy and safety are the most important reasons to consider incognito browsing but avoiding personal embarrassment probably ranks high with many users. Bottom line there many reasons to consider browsing privately including:

- Multiple people use the same computer
    - Prevent personal information footprints such as passwords, web history, downloads, autofill, and dialog box information from being stored on another computer at home, while traveling, at school, or at work
- Testing and debugging websites
- Make management of multiple Google Apps accounts easier
- Prevent Facebook from tracking page and person views
    - Activity such as comments, posts, likes, etc., will not be private and will appear in activity logs
- Planning surprises such as gifts or trips for people that share computers
- Hide viewing sites such as those with pornography or other risqué subject matter
- Using a public computer, like at the library

Incognito browsing only prevents the browser from storing information locally. It does not make you anonymous online or prevent your employer or internet service provider from seeing your traffic. Fortunately, most popular web browsers offer incognito browsing. See the research guide for instructions on enabling the feature and for more information about online anonymity.