CAN YOU HAVE YOUR COOKIES AND EAT (OR DELETE) THEM, TOO?

By John M. McNichols

Until recently, a "cookie" was just a popular baked treat. Since the dawn of the Internet, however, the term has taken on a different meaning, namely that of a small text file that is automatically stored on a user's web browser when viewing a particular website.

Although initially intended as a means to track transaction-specific information for short periods, there is nothing inherent in the technology that limits a cookie to mere transitory use. Cookies can remain on a user's computer for weeks or months and, in doing so, can enable the long-term tracking of the user's Internet browsing activity. This capability is of great commercial value to advertisers, but the fact that advertisers might be able to determine all the websites that one has visited in the previous month—or even the previous year—has drawn attention from certain regulators and lawmakers.

European law now requires that all websites targeting users in European Union (EU) countries must gain "informed consent" before storing "non-essential" cookies on a user's device. Although there is currently no federal law in the United States analogous to the EU's General Data Protection Regulation (GDPR), contemplated legislation would similarly limit the abilities of businesses to track consumer behavior through the use of cookies. Regardless of the legislation, some private businesses have already discontinued using cookies on a voluntary basis, raising the question of whether additional legislation is needed.

> GDPR'S CONSENT STANDARDS EFFECTIVELY APPLY IN NORTH AMERICA AND PERHAPS EVEN WORLDWIDE.

How do cookies work? In the early days of the Internet, web designers were faced with the problem of needing to preserve transaction information from one Internet screen to the next in order to save users the trouble of reentering the information with each new click. Cookies emerged as a solution to this problem, with designers preferring to store such "stateful" information on the user's device rather than on the website's server, thereby conserving data storage space for the website. Although the possibility of using user-embedded information as a means to assess user interests and behavior was immediately apparent, the fact that cookies were actually used to do so was largely unknown to the public for several years. That changed in the late 1990s when the Federal Trade Commission (FTC) noted the prevalence of cookies in public workshops and in its report to Congress.

As the FTC noted, not all cookies were intended to enhance the user's experience of the website being visited. Some cookies, in fact, did not even belong to that website at all. Such cookies were not "first party," but rather "third party," in that they had been placed on the user's browser by a domain other than the one of interest to the user. In most instances, the third party was a professional advertiser, and its cookies were intended to enable the advertiser to identify the user as the same person—or, at least, the same IP address—if he or she later visited a different website that also happened to contain the advertiser's code. If repeated often enough, serial identifications would enable the

John M. McNichols is an associate editor for *Litigation News*.

advertiser to assess the user's interests and enable the delivery of advertising tailored to the user's interests.

What laws govern cookies in the United States? Since May 2018, the EU's GDPR has imposed a continent-wide consent requirement for the placement of cookies on a user's browser. Most large U.S. businesses have adopted GDPR-compliant standards, given the possibility that European consumers will visit their websites. As a result, the GDPR's consent standards have, in some sense, effectively come to apply in North America and perhaps even worldwide.

The enactment of the GDPR in Europe has not deterred U.S. officials from independent action. In 2019, Senator Josh Hawley introduced the Do Not Track Act, which would require the FTC to create a Do Not Track system analogous to the existing Do Not Call list for telemarketing activity. Although the Do Not Track Act is not a prohibition on the placement of cookies, the act would require website operators to notify Internet visitors of their option to click on a link and thereby make themselves exempt from data collection for any purpose not strictly necessary for the provision of online services. And to avoid doubt, the act identifies "targeted advertising" as an unnecessary purpose.

At the state level, meanwhile, California has gone much further, passing data protection legislation in the form of the California Consumer Privacy Act of 2018 (CCPA). Like the Do Not Track Act, the CCPA allows Internet users to declare themselves exempt from tracking technologies. But unlike the federal act—and much more closely aligned to the European GDPR—the CCPA also requires covered entities to disclose what data is collected as well as what is done with the data. And even more importantly, the CCPA is not merely forward-looking in terms of consumer data rights but actually allows consumers to demand that personal data already collected be deleted.

What is next for cookies? Separate and apart from the changing legal requirements, web browsers and online advertisers have voluntarily begun to phase out their use of cookies, particularly third-party cookies. They have done so, in part, in response to the diminishing effectiveness of cookies as increasing numbers of consumers adopt ad-blocking applications or simply clear their browsers. But the discontinuation of cookies does not mean the end of advertisers' efforts to learn the shopping habits and preferences of potential customers. In addition to turning to obvious sources of consumer behavior information such as loyalty programs, companies have begun testing new technologies, such as "fingerprinting."

Like cookies, fingerprinting seeks to assign an identifier to persons browsing the Internet in order to assess individual behavior. Instead of placing a file on users' devices, however, fingerprinting seeks to assess the digital characteristics of the website visitor—e.g., IP address, operating system, browser type, and time zone—in order to determine his or her unique online signature. To be sure, the fingerprinting method is no less a form of tracking technology than cookie-based data collection, but because it relies on the inherent attributes of the web user rather than an externally placed "tag," it is harder to detect or block. As the use of cookies declines and consumer awareness grows, we may see an increased focus on this new type of technology. ■

ABA LITIGATION SECTION

This article is an abridged and edited version of one that originally appeared on page 2 of *Litigation News*, Fall 2022 (48:1).
For more information or to obtain a copy of the periodical in which the full article appears, please call the ABA Service Center at 800/285-2221.
WEBSITE: https://americanbar.org/litigation
PERIODICALS: *Litigation*, quarterly journal; *Litigation News*, online magazine; committee e-newsletters (all Section members may join any of 40 committees at no additional cost).
RECENT BOOKS: *The Trial Lawyer; Class Action Strategy & Practice Guide; Reinventing Witness Preparation; Opposing the Adverse Expert; Internal Corporate Investigations; Mass Torts in the United States; The Attorney-Client Privilege and the Work-Product Doctrine; International Aspects of U.S. Litigation; Infectious Disease Litigation: Science, Law, and Procedure.*
PODCAST: *Litigation Radio* (available on all podcast platforms).