SPRING 2017 E-NEWSLETTER

At Digital Mountain we assist our clients with their cybersecurity, computer forensics and e-discovery needs. For this E-Newsletter, we discuss Internet cookies and the data security, privacy and legal impact it has on organizations and their employees.

The Regulatory Kerfuffle over Cookies and Internet Security

The clear connection between internet security and HTTP cookies makes discussion of one without inclusion of the other incomplete. The Yahoo! forged cookie hack in 2015 that exposed over 32 million accounts clearly illustrates the potential for damaging security breaches launched via cookies. As innocuous as the moniker "cookie" sounds, when we understand the function and deployment of cookies, the recent outrage over the idea that Internet Service Providers (ISPs) legally install cookies, collect data, and, again legally, sell that data may pale in comparison to what it might reasonably be. With all of the attention on government regulation, legal review, and emphasis on network security, is there anything stopping ISPs, application developers, and websites from selling data collected via cookies on the open market?

It's not Good Cop – Bad Cop. It's which Cop?

On March 27, 2017, the US House of Representatives passed a joint resolution that mirrored a Senate joint resolution disapproving of Federal Communications Commission rules relating to "Protecting the Privacy of Customers of Broadband and Other Telecommunications Services" (81 Fed. Reg. 87274 (December 2, 2016)). The joint resolutions annulled enforcement of certain cybersecurity protections that the FCC could have enforced with regard to cookies. Predictably, in our hyper-charged political climate when the news of the joint resolutions broke loose, so did all heck; and not without good reason. When we put the latest thriller novel in our online shopping cart, or check out the website of that dynamic speaker whose session we attended at a professional conference, we're probably not too concerned that a cookie is employed to keep that novel in our cart for later purchase, or that we can zip back to that speaker's website when we want to email the link to colleagues. However, if you want to go out and look at those pictures of a certain celebrity, you may not want your browsing history recorded. The internet is an exercise in free speech, for better or worse. We want that exercise to extend to us on an individual basis

without fearing the repercussions of our curiosity. Hence, when the House and the Senate rolled back those FCC regulations, the public was infuriated.

Despite the rhetorical swirl, an argument has arisen that makes some sense in support of the joint resolutions. That argument is that the FCC is not the appropriate agency to take up this fight, and the enforcement of rules and regulations that protect the consumer's internet privacy belongs to the Federal Trade Commission (FTC). This isn't to say that the two agencies don't work in conjunction, because a quick search on both agencies' websites reveals clear collaboration. However, the missions of the two agencies are disparate enough to support discussion of proper regulatory venue. In brief, the logic behind this argument is that the FCC is industry-centric, regulating and encouraging the development of the nation's communication infrastructure, while the FTC's mission is, "…to protect consumers by preventing anticompetitive, deceptive, and unfair business practices, enhancing informed consumer choice and public understanding of the competitive process, and accomplishing this without unduly burdening legitimate business activity" (FTC.gov). The resulting theory is that regulation preventing harm to internet users is consumer protection, and therefore, falls under the purview of the FTC, not the FCC. This boiled down explanation may beg the question why not just do a search and replace to swap FCC with FTC and shift the regulations to the appropriate agency? Because the answer is never that simple, and the waters are never that clear.

In March 2016, the FCC announced it had reached a settlement with Verizon Wireless for inserting "supercookies" into customers' mobile internet traffic without disclosure (AT&T suspended a similar practice in 2014). The FCC pursued the case as a violation of "the FCC's 2010 Open Internet Transparency Rule and Section 222 of the Communications Act." Section 222 "imposes a duty on carriers to protect their customers' proprietary information and use such information only for authorized purposes." (Both citations https://apps.fcc.gov/edocs_public/attachmatch/DOC-338091A1.pdf) In plain language, Section 222 of the Communications Act is consumer protection, which as discussed above is supposed to be FTC territory, thus muddying the enforcement waters, and not for the first time. The first instance of FCC enforcement under the Open Internet Transparency Rule resulted in a proposed $100 million fine against AT&T for throttling back speeds on unlimited data plan users. This again seems to encroach upon the FTC's mission of consumer protection.

A Fine Line on a Level Playing Field

In an Op-ed for The Hill written prior to the Congressional Joint Resolution vote, Terrell McSweeny, a commissioner at the FTC, argued for the preservation of the FCC's rules by drawing attention to a difference in the enforcement jurisdictions between the FTC and the FCC (http://thehill.com/blogs/pundits-blog/technology/322312-fcc-should-not-leave-broadband-privacy-rules-to-ftc). According to McSweeny, the FTC cannot police broadband cable or wireless carriers with regard to data security and privacy practices, as the FCC does. Where the FTC's jurisdiction lies is over edge providers, such as Amazon, Apple iTunes, and YouTube. The disparity between the FCC's regulation of ISPs and the FTC's oversight of edge providers is seen by some as creating different rules for different players in the same game.

McSweeny contends that the FTC has advocated for data security legislation which would allow for joint enforcement by the FCC and the FTC. The arguments which oppose this level of regulation center on the differing missions of the two agencies and redundant bureaucratic operations, although Rep. Mary Bono (R-CA) and former FTC Chairman Jon Leibowitz hailed the

resolution as a chance to “develop a holistic approach to privacy for the entire internet ecosystem that benefits consumers (http://thehill.com/policy/technology322812-sen-jeff-flake-introduces-measure-to-reverse-the-fccs-broadband-privacy). In the absence of regulations covering data protection and breaches at ISPs, what remains are current FCC practices which place the responsibility of understanding data collection and sale, as well as opt-out consent, on the consumer.

Irrespective of which side of the regulatory debate is supported, there are some conclusions that can be drawn. Interestingly, the FCC and the FTC may be proxies in a competition that in fact ISPs versus edge providers. The drive to own customer information and monetize that information has evolved from “if there is no product for sale, you are the product,” to “you are one of the many products sold.” Cookies are one method by which internet activity is collected and converted into sellable data. Without appropriate regulation and enforcement, the unchecked sale of cookie-based data could very well be the subject of a thriller in your online shopping cart.

Please direct questions and inquiries about cybersecurity, computer forensics and electronic discovery to info@digitalmountain.com.

UPCOMING INDUSTRY EVENTS

Internet of Things World
Santa Clara, CA: May 16-18, 2017

ISSA 9th Annual Information Security Summit
Los Angeles, CA: May 18-19, 2017

ENFUSE 2017
Las Vegas, NV: May 22-25, 2017

"The Exchange" Data Privacy and Cybersecurity Forum
New York, NY: May 23-24, 2017

Click here to see more upcoming events and links

Digital Mountain, Inc. Founder and CEO, Julie Lewis, will be presenting at various upcoming industry events. Please send requests for speaker or panel participation for her to marketing@digitalmountain.com.

DIGITAL MOUNTAIN, INC.
4633 Old Ironsides Drive, Suite 401
Santa Clara, CA 95054
866.DIG.DOCS

www.digitalmountain.com

Contact us today!

FOLLOW US AT: