Cybersecurity implications of Google cookie placement

November 30, 2015

The Third Circuit Court of Appeals recently issued an opinion in In re: Google Inc. Cookie Placement with a couple of interesting cybersecurity angles. The most relevant holding had to do with standing. According to the court, the violation of a statutory right is enough to give plaintiffs standing, regardless of whether or not a potential plaintiff suffered monetary damage. This is relevant insofar as standing-related arguments tie to other federal statutes that could (or, down the road with potential future legislation, might) relate to cybersecurity and insofar as potential plaintiffs live in states covered by the Third Circuit (Delaware, New Jersey and Pennsylvania). The remainder of the opinion is important for its examination of three federal statutes related to the internet and cybersecurity concerns (the Wiretap Act, the Stored Communications Act, and the Computer Fraud and Abuse Act), particularly for companies engaged in large-scale data mining and online advertising.

Background

First, a little background helps provide context for the opinion's discussion of some relatively technical aspects of Internet advertising. Third-party advertisers have created an extensive operation to track internet users' online habits. To do so, they have set up cookies on first-party websites for which they are the third-party advertising vendor. The cookie functions like a tracking device, collecting data on who goes to what sites. Joining multiple cookies together provides even more data for the advertisers, which allows for more targeted ads; more targeted ads are more valuable to all of the non-consumer players in the advertising operation. Safari and Internet Explorer both have built in mechanisms to provide more privacy and circumvent this operation — what could be called cookie blockers, for example — which, in theory, made it much harder to track an internet user's history on the web. According to the allegations, Google surreptitiously employed a code that automatically circumvented Safari's and Internet Explorer's built-in cookie defense mechanisms.

Based on all of this, the plaintiffs brought a putative class action suit against Google (and a number of other defendants) on behalf of themselves and anyone in America who has used Safari or Internet Explorer, and also Google, to search the internet. They alleged violation of several California laws, as well as several federal laws — namely, the Wiretap Act, the Stored Communications Act, and the Computer Fraud and Abuse Act. The Court of Appeals affirmed the dismissal of the plaintiffs' complaint and provided a couple of interesting holdings relevant to cybersecurity in doing so.

1) Third Circuit held that the plaintiffs did have standing to bring suit.

The defendants argued the opposite, pointing to the fact that, so far as anyone knew, the defendants didn't suffer any economic harm. The court disagreed, holding that defendants don't necessarily need to show actual monetary harm for standing and that the violation of a statute (like the Wiretap Act, for example) that creates a legal right is enough for standing. Stated in practical terms, if Google violated the statute, then that was enough for standing regardless of whether the defendants suffered monetary harm because of the violation.

2) The court addressed three federal statutes that deal with internet security, online advertising, and big data.

- One of the statutes at play was the Wiretap Act. The Wiretap Act bars a third party from intercepting "the content" of an electronic communication. According to the Third Circuit, URL information — which is historically viewed as a mere

location identifier outside of the "content" category (and thus not subject to protection from the Wiretap Act) — could be "content" worthy of protection from the Wiretap Act. Whether it is so depends on context, specifically whether the URL demonstrates the type of information an internet user is seeking, the type of documents looked at, or anything beyond basic metadata-like or pen-register-like identifying information. The Third Circuit also explained the defendants' Wiretap Act count failed nonetheless because of the Act's safe harbor for claims based on communications to those who were "party to the communication" at issue. Here, because users are trying to access a given site, they would send the tracking information and URL content at issue to a company like Google no matter what. And regardless of what Google did with that information, that rendered Google an original party to the communication shielded by the Act's safe-harbor provision.

- The court also addressed the Stored Communications Act (the SCA). The SCA prohibits a third party from accessing communications and related data stored at a facility through which an electronic communications service is provided. Here, the defendants' claim failed because, according to the court, "a personal computing device is not a facility through which an electronic communication service is provided." To this end, the SCA applies to centralized communication suppliers, such as telephone and email companies, but not personal computers.

- Finally, the court addressed the Computer Fraud and Abuse Act (the CFAA). The CFAA prohibits a third party from intentionally accessing a computer without authorization and then obtaining information from a protected computer. The statute requires a plaintiff to show "damage or loss." The plaintiffs argued that they properly pleaded loss given that their information, which is used as a currency or commodity, was impermissibly seized by Google's cookie operation. The court disagreed, noting that the plaintiffs didn't suffer loss, specifically because they failed to plead any intention to participate in a market where they could monetize their internet-usage information.

Authors