Hashed & Salted | A Privacy and Data Security Update
March 2024

Teenage Mutant Privacy Class Action Theories

Sometimes, privacy law can seem like an unruly teenager. We can see this wildness in the emergent state, federal and international privacy regulations. We can also see it in the froth and change that we see in privacy litigation. The plaintiffs' bar articulates a theory and then it quickly (and opportunistically) mutates.

The first mutation of these privacy lawsuits alleged that advertising technology constituted an illegal wiretap.

California Wiretaps and Privacy Lawsuits—a Brief Romance

In 2021, businesses faced hundreds of class action demands alleging violations of the California Invasion of Privacy Act (CIPA). CIPA is a 1994 privacy law aimed at protecting California residents from illegally recorded conversations. Recording telephonic and electronic conversations, unless everyone involved in the conversation consents, constitutes an illegal "wiretap" under CIPA. Victims of a CIPA wiretap can sue for statutory damages.

A "wiretap" classically means a device or process that secretly monitors telephone conversations. Under Title III of the Omnibus Crime Control and Safe Streets Act of 1968, that amended definition includes "wire, oral, and electronic" communications such as telephone conversations and emails. Under CIPA, the definition was usually construed much more narrowly. These claims did not gain much legal traction until May 2022, when the Ninth Circuit reversed a district court's dismissal of a CIPA claim in *Javier v. Assur. IQ,* LLC. Smelling an opportunity, plaintiffs' firms sent out thousands of pre-suit demand letters threatening CIPA class action litigation under CIPA Section 631(a) and Section 632.7.

These cases argued that this old state wiretap law constituted new privacy violations due to the deployment of certain technologies on commercial websites. Some examples of these purported CIPA violations included (1) websites using chat boxes, whether live or automated, and (2) web session analytics technologies. The "chat box" theory centered on the idea that, since nearly every website uses third-party vendors to run their chat boxes, the chats were being recorded and shared with that third party in violation of law. The web session analytics theory (also known as the "session replay" theory) similarly argued that sharing the visitors' movements on the site (along with certain other indicators) constituted an illegal recordation of their electronic communications in violation of CIPA.

These wiretap claims gained another early victory in *Byars v. Goodyear Tire & Rubber Co.,* in which a California federal court decided that a chat box theory could constitute an illegal CIPA wiretap. After this decision, plaintiffs' attorneys raced to send hundreds more demand letters. The victory was short-lived, however.

Less than two weeks after *Byars v. Goodyear*, a different judge issued a contrary decision in *Byars v. Hot Topic.* This decision, which involved the same plaintiff's attorney and putative class representative, found that a chat box theory

could not constitute a CIPA wiretap. Since Feb. 14, 2023, many more courts have adopted the analysis utilized in *Byars v. Hot Topic*. As a practical matter, by the end of 2023, the CIPA wiretap theory was dead.

Love Reborn—What About Pen Registers?

A recent decision from the Southern District of California has prompted plaintiffs' firms to change their claims to invoke an obscure provision of CIPA—Section 638.51. These mutated claims advance a new theory for civil liability: What if these website features are pen registers instead of wiretaps?

CIPA Section 638.51 prohibits the installation or use of a pen register or a trap and trace device without first obtaining a court order. A "wiretap" is understood by the layperson: You are using technology to listen in on or otherwise intercept private communications. Such wiretaps constitute a lawful law enforcement tool with proper court approval. The definition of a "pen register or a trap and trace device" is less obvious.

CIPA Section 638.50(b) defines a "pen register" as a device or process that records or decodes dialing, routing, addressing or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted. Similarly, Section 638.50(c) defines a "trap and trace" device as a device or process that captures the incoming electronic or other impulses that identify the originating number or other dialing, routing, addressing or signaling information reasonably likely to identify the source of a wire or electronic communication. To put these definitions more simply, a "pen register" records all phone numbers called from a specific phone and a "trap and trace" device records all phone numbers coming in to a specific phone. Neither a "pen register" nor a "trap and trace" records the content of the communications, merely to whom they were directed. Thus, with a properly obtained pen register or a trap and trace device, law enforcement would have a written log of the devices contacting or contacted by a specific phone or device. Unlike a wiretap, which allows real-time interception of the content of the communications, pen registers and trap and trace devices are limited to the collection of these logs of dialing, routing, addressing or signaling information.

In *Greenley v. Kochava,* the plaintiff claimed that session replay software installed in third-party mobile applications constituted an illegally installed pen register. The defendant moved to dismiss, arguing that its software was not a pen register. After noting that no other court had interpreted CIPA's pen register provision, the court concluded that "software that identifies consumers, gathers data, and correlates that data through unique 'fingerprinting' is a process that falls within CIPA's pen register definition." Accordingly, the court denied *Kochava's* motion to dismiss.

The *Greenley* court's interpretation causes significant problems. All phones and internet-linked devices compile lists of the other devices contacted and that contact them. These lists are the backbone of caller ID and the back button in a web browser. Indeed, such lists are a backbone of the Internet Protocol that makes the entire internet work. Under *Greenley,* these ubiquitous functions fall within CIPA's definition of a pen register or a trap and trace device. We already see that the opportunistic demand letters have gone out. Expect many more.

The *Greenley* interpretation is so unworkable that it is unlikely to stand. However, for now, we are in a frothy cycle, wherein companies can expect many more *Greenley* demand letters. Like the *Byars* cases, contrary authority will likely develop as soon as more companies fight. When the fight forecloses this pen register theory, expect these young privacy claims to mutate again.

Related Professional

Christopher A. Ott . . . . . cott@loeb.com