Proskauer

Now Trending: The TikTok Dox

Proskauer on Privacy on **December 10, 2024**

Key Takeaways:

- Plaintiffs are persistently crafting creative legal theories to target tracking technologies.
- One new approach is to characterize tracking technologies as "pen registers" or "trap and trace devices" used in violation of CIPA § 638.51.
- The TikTok Analytics software is at issue in many of these new claims, and a number have survived motions to dismiss and demurrers.

Now Trending: The TikTok Dox

Another TikTok trend has gone viral this year. But it's not what you think. Since the beginning of the year, the Plaintiffs' bar has filed over a hundred California Invasion of Privacy Act ("CIPA") class actions centered on the TikTok Analytics software, and many more cases have undoubtedly been threatened and resolved out of the public sphere.

These claims target companies, both big and small, that have integrated TikTok Analytics into their websites, with plaintiffs arguing that the tracking technology functions as a "trap and trace" device used in violation of CIPA § 638.51. Plaintiffs allege that use of the software allows TikTok to connect web user behavior with existing TikTok data, a process called "fingerprinting" or, in internet-speak, "doxing."

What are "trap and trace" claims?

You've probably seen trap and trace devices in action while watching your favorite crime dramas – historically, these devices have been used by law enforcement to acquire phone call data, with the intention of identifying the parties on a call. CIPA § 638.51 is the statute that regulates use of this technology, and it prohibits the installation or use of these devices by individuals or companies without a court order.

A “trap and trace device” is defined under § 638.50 as “a device or process” that captures the identification information transmitted *to* a device. While trap and trace devices do not collect a communication’s content, they can be used to gather information that could “reasonably identify” the communication’s source (e.g., data about *incoming* phone calls). Note that § 638.51 also prohibits the installation or use of “pen registers,” which collect identification information transmitted *from* a device (e.g., data about *outgoing* phone calls).

Violations of § 638.51 run the risk of a $2,500 fine or even imprisonment. But there are exceptions to § 638.51’s prohibitions. For example, use of these devices is permitted when consent is obtained from the subject whose information is captured. Similarly, these devices can be used to “operate, maintain, and test a wire or electronic communication service,” protect “rights or property of the provider,” or protect “users of the service from abuse of service or unlawful use of service.”

This provision of CIPA received little attention until the Southern District of California’s decision in *Greenley v. Kochava, Inc*. In *Kochava*, plaintiff alleged that Kochava “surreptitiously intercept[ed] location data” from smartphone application users and purportedly sold that data to third parties. Despite its acknowledgment that “pen registers” are traditionally physical machines used by law enforcement to record numbers called from telephones, the Court eschewed this practical view, opting to stretch what it described as a “vague” definition. The Court reasoned that the “expansive language” of § 638.51 “indicate[d] courts should focus less on the form of the data collector and more on the result” because “[a] process can take many forms [and] [s]urely among them is software that identifies consumers, gathers data, and correlates that data through unique ‘fingerprinting.’” Thus, the Court rejected Kochava’s contention “that a private company’s…embedded software installed in a telephone cannot constitute a ‘pen register.’”

The Court’s decision in *Kochava* has emboldened plaintiffs’ attorneys to pursue § 638.51 claims alleging that software used to collect user information, including smartphone applications, pixels, and cookies, constitutes a trap and trace or pen register device under CIPA.

The TikTok Claims

TikTok Analytics is at the center of many of these increasingly popular claims. Plaintiffs allege that the sole purpose of the software is to identify the source of incoming communications to a website; thus, TikTok Analytics purportedly functions as a trap and trace device because it's capable of matching web user activity to existing TikTok data.

For example, in these largely copy-and-pasted complaints, plaintiffs assert that TikTok Analytics engages in "fingerprinting" to collect "as much data as it can about an otherwise anonymous visitor to the Website and matches it with existing data TikTok has acquired and accumulated about hundreds of millions of Americans." *See e.g.,* *Jurdi v. Massage Envy Franchising, LLC*. The software then, allegedly "in collaborat[ion] with the Chinese government…", "effectively 'dox[es]' [p]laintiff[s] to America's most formidable geopolitical adversary." *See e.g.*, *Sanchez v. J. Crew Group LLC*; *Sanchez v. Jo-Ann Stores, LLC*; *Sanchez v. Tractor Supply Co.*.

The Central District of California's July decision in *Moody v. C2 Education Systems* followed *Kochava*. In *Moody*, the Court denied defendant's motion to dismiss, permitting plaintiff's § 638.51 TikTok claim to proceed and determining that the "software *may* qualify as a pen register or trap and trace device under California law[.]" (emphasis added). The *Moody* Court quoted *Kochava* in support of its holding, noting that "*Greenley* [*v. Kochava, Inc.*] concluded that tracking software could plausibly constitute a pen register under §§ 638.50 and 638.51."

Similarly, the Los Angeles Superior Court has denied a number of defendants' demurrers, approving the theory that TikTok Analytics *may* qualify as a trap and trace device. *See Price v. Entravision Communications Corporation*; *Heiting v. IHOP Restaurants, LLC*; *Jurdi v. MSC Cruises (USA) LLC*; *Heiting v. Taylor Fresh Foods, Inc.*. Similar claims based on other tracking technologies have survived motions to dismiss and demurrers, as well. *See e.g.,* *Shah v. Fandom, Inc.*; *Levings v. Choice Hotels International, Inc.*.

But not all of these claims have been successful. The Central District of California dismissed a TikTok trap and trace claim for an inadequate showing of injury-in-fact but provided plaintiff the opportunity to amend the complaint to cure this deficiency. *See* *Hughes v. Vivint, Inc. et al*. The Los Angeles Superior Court has also dismissed similar tracking technology claims. *See* *Casillas v. Transitions Optical, Inc.* (dismissal for failure to allege: 1) the technology trackers at issue qualify as trap and trace devices; and 2) a lack of consent); *Licea v. Hickory Farms LLC* (dismissal for failure to allege: 1) the information collected was of the type prohibited; and 2) a lack of consent).

No court has affirmatively held that TikTok Analytics is, in fact, a trap and trace device. Instead, these decisions have simply allowed TikTok fingerprinting claims to proceed past the pleading stage. Defendants have successfully thwarted a number of CIPA tracking technology claims on alternative bases. Successful defenses include challenges to personal jurisdiction and punitive damages, as well as the existence of consent language in company policies and motions to compel arbitration. *See* *Palacios v. Lolliprops Inc.* (granting motion to quash for failure to establish personal jurisdiction in tracking technology trap and trace case); however, compare *Palacios v. Wilson Sporting Goods Company* (denying motion to quash for failure to establish personal jurisdiction on complaint almost identical to *Lolliprops*); *see also* *Sanchez v. Unite Eurotherapy, Inc.* (granting motion to strike request for punitive damages in tracking technology trap and trace case); *Gennaro v. Avvo, Inc.*, No. 18-CV-2213-WQH-BLM, 2019 WL 13488559 (S.D. Cal. May 6, 2019) (granting defendant's motion to compel arbitration in CIPA case).

What next?

Plaintiffs are seizing upon this new frontier, and tracking technology fingerprinting claims are being filed each week. And it's not just the TikTok software facing scrutiny – similar CIPA claims have been filed against companies using other third-party trackers like Google Analytics and Meta Pixel, as well as smartphone applications.

Companies should take steps to mitigate risk and prepare for potential fingerprinting claims, especially if they employ the TikTok Analytics software or any other third-party tracker. If your organization needs assistance assessing its risk posture with respect to these technologies and guidance on risk mitigation, please reach out to our Privacy & Cybersecurity Practice Group lead Leslie Shanklin. Organizations may also reach out to our litigation partners Baldassare Vinti, David Fioccola and Jeff Warshafsky for class action litigation defense strategies.

View original.

Related Professionals

- **Aaron M. Francis**
  Associate
- **Jeff H. Warshafsky**
  Partner