Washington Legal Foundation
Advocate for freedom and justice®
2009 Massachusetts Avenue, NW
Washington, DC 20036
202.588.0302

Critical Legal Issues: **WORKING PAPER SERIES**

NO CAUSE OF ACTION:
California's Pen/Trap Law Inapplicable to Web Ad Cookies and Pixels

Steven G. Stransky, Kip T. Bollin & Jennifer A. Adler
Thompson Hine LLP

Washington Legal Foundation
Critical Legal Issues WORKING PAPER Series

Number 228
March 2024

TABLE OF CONTENTS

ABOUT OUR LEGAL STUDIES DIVISION

Since 1986, WLF's Legal Studies Division has served as the preeminent publisher of persuasive, expertly researched, and highly respected legal publications that explore cutting-edge and timely legal issues. These articles do more than inform the legal community and the public about issues vital to the fundamental rights of Americans—they are the very substance that tips the scales in favor of those rights. Legal Studies publications are marketed to an expansive audience, which includes judges, policymakers, government officials, the media, and other key legal audiences.

The Legal Studies Division focuses on matters related to the protection and advancement of economic liberty. Our publications tackle legal and policy questions implicating principles of free enterprise, individual and business civil liberties, limited government, and the rule of law.

WLF's publications target a select legal policy-making audience, with thousands of decision makers and top legal minds relying on our publications for analysis of timely issues. Our authors include the nation's most versed legal professionals, such as expert attorneys at major law firms, judges, law professors, business executives, and senior government officials who contribute on a strictly *pro bono* basis.

Our eight publication formats include the concise COUNSEL'S ADVISORY, succinct LEGAL OPINION LETTER, provocative LEGAL BACKGROUNDER, in-depth WORKING PAPER and CONTEMPORARY LEGAL NOTE, topical CIRCULATING OPINION, informal CONVERSATIONS WITH, balanced ON THE MERITS, and comprehensive MONOGRAPH. Each format presents single-issue advocacy on discrete legal topics.

In addition to WLF's own distribution network, full texts of LEGAL OPINION LETTERS and LEGAL BACKGROUNDERS appear on the LEXIS/NEXIS® online information service under the filename "*WLF*," and every WLF publication since 2002 appears on our website at www.wlf.org. You can also subscribe to receive select publications at www.WLF.org.

To receive information about WLF publications, or to obtain permission to republish this publication, please contact Glenn Lammi, Vice President of Legal Studies, Washington Legal Foundation, 2009 Massachusetts Avenue, NW, Washington, DC 20036, (202) 588-0302, glammi@wlf.org.

ABOUT THE AUTHORS

Steven Stransky, partner and co-chair of Thompson Hine's privacy and cyber security practice helps clients develop and implement data governance frameworks and internal policies and procedures to address evolving data privacy and digital marketing laws. As an authorized Data Breach Coach, he works with clients in responding to ransomware attacks, business email compromises, and other cybersecurity incidents. Prior to joining Thompson Hine, Steven served for over 10 years in the federal government, including as senior counsel at the U.S. Department of Homeland Security, Intelligence Law Division, and as a deputy legal advisor on the President's National Security Council.

Kip Bollin is a litigator and Partner in Charge of Thompson Hine's Cleveland office. His practice includes the defense of putative class actions, consumer claims, privacy claims, commercial claims, intellectual property claims, and other state and federal causes of action. Kip is a former national president of the 18,000+ member Federal Bar Association.

Jennifer Adler is counsel in Thompson Hine's Business Litigation group and advises businesses on privacy litigation strategies and represents them in a broad range of complex business disputes in federal and state courts nationwide, as well as in mediations and arbitrations.

Editor's Note:
This *Working Paper* is for informational purposes only and intended to serve as a resource for organizations seeking to understand the regulatory framework governing this issue and potential legal defenses that may be available in this context, and it does not, and is not intended to, constitute legal advice. Any changes to the laws, regulations, or legal opinions governing this area of law may require the conclusions herein to be reevaluated.

NO CAUSE OF ACTION:
California's Pen/Trap Law Inapplicable to Web Ad Cookies and Pixels

INTRODUCTION

Like many other states, California has enacted a statute regulating the use of pen registers and trap and trace devices. Cal. Penal Code § 638.50-55 (the "California Pen/Trap Law"). Pursuant to this law, "a person may not install or use a pen register or a trap and trace device" without first obtaining certain types of court orders or to the extent other statutory exceptions apply. *Id.* at § 638.51(a). As described in greater detail below, pen registers and trap and trace devices are surveillance tools used to identify telephone numbers and similar sources of communication, but from different perspectives: pen registers track *outgoing* telephone calls and communication sources, while trap and trace devices track *incoming* calls and communication sources.

Recently, there has been a rise in legal claims that argue website advertising cookies and pixels should be considered pen registers and/or trap and trace devices pursuant to the California Pen/Trap Law. Thus, a website end-user's privacy rights are violated each time an advertising cookie or pixel collects their data if no court has issued an order allowing such collection. To date, no judicial precedent supports this position. Instead, these claims appear to be based on a misunderstanding of a recent federal court decision.

The California Pen/Trap Law is a criminal statute and an individual who violates its terms can be subject to both monetary penalties and imprisonment. *Id.* at § 638.51(c). If a court were to adopt the position that a website advertising cookie or pixel is considered a pen register or trap and trace device, that absurd result could subject every organization with a public-facing website that uses this technology (without a court order or qualification for an exception) to criminal and civil liability.

This *Working Paper* explains why the use of advertising cookies and pixels does not violate the California Pen/Trap Law. That conclusion is supported by (i) the plain text and structure of the California Pen/Trap Law, (ii) the legislative intent behind the California Pen/Trap Law, (iii) the scope of court orders authorizing the use of pen registers and trap and trace devices, (iv) other California laws governing website cookies and pixels, and (v) the "user consent" provisions within the California Pen/Trap Law. After some important background information, the *Working Paper* offers a detailed discussion of each of these five points.

I. BACKGROUND

A. Website Tracking and Advertising Technologies

A broad range of online technologies facilitate and monitor internet-based communications. For purposes of the California Pen/Trap Law, there are four important areas to consider and understand: (i) website cookies, (ii) tracking pixels, (iii) digital fingerprinting, and (iv) software development kits.

1. Website Cookies

The term "cookie" refers to a small text file that a website server creates and transmits to a web browser (e.g., Google Chrome, Safari), which then stores the file in a particular directory on an individual's computer, phone, or other device. *See* Sara J. Nguyen, *What Are Internet Cookies and How Are They Used?*, All About Cookies (Jul. 28, 2023) (hereinafter, "What Are Cookies"). Essentially, when a website end user attempts to access a webpage, the end-user's browser transmits a communication to the website's server requesting the server to display the website's content for the end-user's browser to load, which then, if working properly, displays the webpage's content to the end user. *Id.*

While providing the requested content to the end user, the website's server also provides the cookies it would like the website end-user's browser to retain to facilitate the communication more efficiently and possibly for other purposes. *Id*. The U.S. District Court for the Southern District of California explains the cookie-deployment process as follows:

> For context, a cookie is a file on a user's computer. Cookies contain information that identifies the domain name of the webserver that wrote the cookie (e.g., hulu.com, comScore.com, or facebook.com). Cookies have information about the user's interaction with a website. Examples include how the website should be displayed, how many times a user has visited the website, what pages he visited, and authentication information. Each web browser on a computer (e.g., Internet Explorer or Chrome) stores the cookies that are created during a user's use of the browser in a folder on the user's computer that is unique to that browser. When a user types a website address into the browser, the browser sends (a) a request to load the page to the web server for that website address and (b) any cookies that are associated with the website (such as the cookies on the user's computer for 'hulu.com' or 'comScore.com'). The remote website server returns the requested page and can update the cookies or write new ones.

In re Hulu Priv. Litig., No. C 11-03764 LB, 2014 WL 1724344, at *4 (N.D. Cal. Apr. 28, 2014) (internal citations omitted).

Accordingly, "[c]ookies do contain data, and that typically includes a unique identifier and a site name" and it "could also include personally identifiable information such as your name, address, email, or phone number if you've provided that information to a website." Nguyen, *supra*. There are several types of cookies, but the two most relevant to this analysis are first-party cookies and third-party cookies.

A first-party cookie is implemented by the website the end user accesses, and the website "host" or "operator" uses its cookies for a variety of purposes, including authentication, monitoring user sessions, and collecting analytical data. *Id*. A third-party cookie (also called an "advertising cookie") is a cookie that belongs to a domain other than the one being displayed to an end user in their browser, and they are primarily used for cross-site tracking, retargeting, and ad-serving. *Id*. The key differences between first- and third-party cookies are who sets them (i.e., the website display host or a third party), whether and how they can be blocked by a web browser, and the availability of the cookie (i.e., first-party cookies are available to the domain creator and a third-party cookie is accessible on any website that loads the third-party server's code). *Id.*

2. Tracking Pixels

A pixel, also known as a "tracking pixel," "web bug," "clear GIF," or "web beacon," is like a website cookie. It is a small, essentially invisible image (pixel) embedded in a website or an email to track an end-user's activities. Patti Croft & Catherine McNally, *What Is a Web Beacon and Why Should You Care?*, All About Cookies (Sept. 26, 2023). In practice, a website host or operator embeds a tracking pixel therein, which itself contains code that links to its external server. *Id.* In turn, when a user accesses the website, the browser identifies and opens the code within the pixel, which records and transmits certain data about the user back to the pixel server. This data often includes the end-user's operating system, the type of website or email used, the time of website access, the user's Internet Protocol (IP) address, and whether the server hosting the pixel image previously set cookies. *Id.*

In 2003, the U.S. Court of Appeals for the First Circuit analyzed whether the use of cookies and pixels violated federal wiretapping laws. *Blumofe v. Pharmatrak, Inc. (In re Pharmatrak, Inc. Privacy Litig.*), 329 F.3d 9, 12 (1st Cir. 2003). The court provided a good example of how cookies and pixels can work in tandem. In the case, the court focused on Pharmatrak's cookies and pixels that it included in a service called "NETcompare" and that were deployed on the websites of pharmaceutical companies. This is how the court described the use of these online technologies:

> NETcompare operated as follows. A pharmaceutical client installed NETcompare by adding five to ten lines of HTML code to each webpage it wished to track and configure[ed] the pages to interface with Pharmatrak's technology. When a user visited

> the website of a Pharmatrak client, Pharmatrak's HTML code instructed the user's computer to contact Pharmatrak's web server and retrieve from it a tiny, invisible graphic image known as a 'clear GIF' (or a 'web bug'). The purpose of the clear GIF was to cause the user's computer to communicate directly with Pharmatrak's web server. When the user's computer requested the clear GIF, Pharmatrak's web servers responded by either placing or accessing a 'persistent cookie' on the user's computer. On a user's first visit to a webpage monitored by NETcompare, Pharmatrak's servers would plant a cookie on the user's computer. If the user had already visited a NETcompare webpage, then Pharmatrak's servers would access the information on the existing cookie.
>
> Each Pharmatrak cookie contained a unique alphanumeric identifier that allowed Pharmatrak to track a user as she navigated through a client's site and to identify a repeat user each time she visited clients' sites. If a person visited www.pfizer.com in June 2000 and www.pharmacia.com in July 2000, for example, then the persistent cookie on her computer would indicate to Pharmatrak that the same computer had been used to visit both sites. As NETcompare tracked a user through a website, it used JavaScript and a JavaApplet to record information such as the URLs the user visited. This data was recorded on the access logs of Pharmatrak's web servers.

Id. at 13-14.

As shown, pixels can also be programmed to deliver or "drop" their own cookies on the website end-user's device to gather, consolidate, and analyze additional data from the end user for marketing purposes.

3. Digital Fingerprinting

The term "digital fingerprinting" (or just "fingerprinting") may refer to two separate and distinct activities: device fingerprinting or browser fingerprinting. With respect to device fingerprinting, an end-user's device (e.g., computer, cellphone, tablet) transmits its system information to a website to ensure "site functionality on the device and, in essence, forming a 'fingerprint' of the device." Anokhy Desai, *The Half-Baked Future of Cookies and Other*

Tracking Technologies, IAPP (July 2023). This process helps ensure that the website is displaying content and operating appropriately, depending on the type of device utilized by the end user. *Id.* Browser fingerprinting, on the other hand, refers to the same type of identification process, but is based on an end-user's browser data. *Id.* For example, "[w]hen a user clicks on a link to visit a site, the site sends a request to the server along with information necessary to receive the requested content like IP address, browser type and version, and other information like time zone, battery level and CPU usage." *Id.* Although a browser or device does not transmit personal information about an end user, "most fingerprinting is performed via a third-party tracker," and therefore, this third party "can track an individual across multiple sites and form a profile about them." *Id.*

4. Software Development Kits

A software development kit (SDK) is a set of software programs and similar tools that developers and engineers can leverage to build applications for specific platforms. More specifically:

> An SDK, devkit, or software development kit is a program designed by manufacturers of operating systems, hardware platforms, program languages, software, or applications. It provides developers with a set of tools that help them build apps more efficiently and effectively. An SDK can accompany hardware or digital software to help developers create new apps that can integrate with existing programs or apps. It can also help users to better navigate these products. An SDK is designed for use within a specific system, on a certain operating system, or with a specific programming language. . . An SDK can contain a variety of components to help with application creation, providing a framework to work within.

What Is an SDK? Software Development Kits Explained, Okta, Inc. (June 30, 2022).

The SDK often includes, among other tools, the following: libraries (i.e., the collection of reusable code that performs specific functions), application programming interfaces (i.e., predefined pieces of code that allow application developers to perform common and routine programming), instructions, guides, directions, and tutorials. *Id.*

B. Recent Case Law on the California Pen/Trap Law

The increase in California Pen/Trap Law-related legal claims can largely be traced to a recent Southern District of California decision, *Greenley v. Kochava Inc.*, No. 22-cv-01327-BAS-AHG, 2023 U.S. Dist. LEXIS 130552, at *2 (S.D. Cal. Jul. 27, 2023). The defendant, Kochava Inc. ("Kochava"), is a software developer that designs SDKs and other products to assist companies in identifying and tracking existing or potential customers via mobile devices. *See About Us*, Kochava, https://www.kochava.com/company/?int-link=menu-about.

In his lawsuit, the plaintiff alleges that Kochava sold certain SDKs to mobile-application developers wherein Kochava secretly embedded code that allowed them to "surreptitiously" intercept personal data and other information from application end users. *Greenley,* at 2. This data and information potentially included an end-user's geolocation data, usernames and communications derived from other SDK apps installed on an end-user's device, and an end-user's activities within an application after installation. *Id.* Kochava then sold this data to third parties, such as retail companies and grocery stores, who could use the data for their own marketing and advertising purposes. *Id.* According to the complaint, Kochava is "able to deliver targeted advertising . . . by in essence 'fingerprinting' each unique device and user, as well as connecting users across devices and devices across users." *Id.*

The plaintiff alleged, *inter alia*, that Kochava's SDK was a "pen register" and Kochava violated the California Pen/Trap Law. *Id.* at 3. In response, Kochava filed a motion to dismiss on the grounds that the court lacked subject matter jurisdiction and the plaintiff failed to properly state a claim. *Id.* at 2.

Therefore, one of the key issues[1] in *Greeley* is the scope and meaning of a "pen register." The California Pen/Trap Law defines a "pen register," in relevant part, as "a device or process that records or decodes dialing, routing, addressing, or signaling ["DRAS"] information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, but not the contents of a communication." *Id.* at 38 (citing Cal. Pen. Code § 638.50(b)).

At the beginning of her analysis of whether Kochava's SDK was a pen register under the California Pen/Trap Law, Judge Cynthia Bashant indicated that there was "no caselaw" to support the defendant's position that its SDK was *not* a pen register because "no court has interpreted this provision" of the law at any point and it was a matter of first impression. *Id.* She also noted that while law enforcement agencies traditionally used pen registers on "physical machines" to "record all numbers called from a particular telephone," they now "take the form of software." *Id.* Judge Bashant further reasoned that "[a]s a result, private companies and persons have the ability to hack into a person's telephone and gather the same information as law enforcement." *Id.* at 38-39. Judge Bashant speculated that these technological advancements were the reason that the California legislature did not limit its prohibition on installing pen registers to only law enforcement agencies, but rather applied the prohibition to any "person." *Id.* at 39.

Judge Bashant then focused on the "expansive language" used to define a pen register. *Id.* She noted that the definition is specific as to the "type of data" collected (i.e., DRAS information), but it is "vague and inclusive as to the form" of the collection tool or method (i.e., a "device or process" that records data). *Id.* As a result, in her opinion, when analyzing whether an SDK is a pen

[1] The plaintiff also argued that Kochava is liable under the California Computer Data Access and Fraud Act, other California Invasion of Privacy Act provisions, the California Unfair Competition Law, and common law principles of unjust enrichment. *Id.* These issues will not be addressed herein.

register, the court "should focus less on the form of the data collector and more on the result." *Id.*

Further to this point, a "process" can, according to Judge Bashant, "take many forms," including software that identifies consumers, gathers data, and correlates that data through unique "fingerprinting." *Id.* at 39-40. Therefore, she held that a private company's "surreptitiously" embedding of software installed in a telephone used to secretly extract and sell personal data and communications can constitute a pen register for purposes of the California Pen/Trap Law. *Id.*

Kochava argued that its SDK was not a pen register because the data it collected did not implicate a legal requirement for law enforcement to obtain a court order or warrant to collect it. *Id.* at 40. Judge Bashant responded by noting that Kochava "misunderst[ood]" the plaintiff's claim. *Id.* According to the judge:

> CIPA extends civil liability to the installation of a pen register without a court order. Plaintiff has alleged each necessary element of this claim: Defendant installed a pen register without a court order. The fact that law enforcement can install a warrantless pen register without offending the Fourth Amendment is immaterial.

Id.

Judge Bashant concluded that the plaintiff "alleged enough to survive the motion to dismiss." *Id.* at 41. However, the *Greenley* decision did not, in any form or manner, address whether or otherwise hold that a website advertising cookie or pixel is or should be considered a pen register or trap and trace device under the California Pen/Trap Law.

II. LEGAL ANALYSIS

As noted above, plaintiffs are relying on the broad interpretation of a "pen register" in *Greenley* to argue that website advertising cookies and pixels should be considered pen registers or trap and trace devices under the California Pen/Trap Law. They often argue that such technologies capture certain types of DRAS information or similar electronic impulses (e.g., IP addresses, MAC addresses, port numbers) from devices used to access a website for the purpose of identifying the source of the communication and therefore fall within the scope of the law. However, no court decision holds that website advertising cookies and pixels should be considered pen registers or trap and trace devices pursuant to *any* federal *or* state law, including the California Pen/Trap Law. In addition, even if one assumes *arguendo* that website advertising cookies and pixels collect such DRAS-related information, there are at least five compelling reasons (set forth in greater detail below) why the California Pen/Trap Law does not prohibit the use of these technologies.

Were a federal or state court to conclude that website advertising cookies and pixels are considered pen registers or trap and trace devices within the meaning of the California Pen/Trap Law, such a holding could subject every organization that uses these common and ordinary technologies to **civil and criminal liability**. *Id.* at § 638.51(a) (emphasis added). Yet, "ambiguity concerning the ambit of criminal statutes should be resolved in favor of lenity." *United States v. Carr*, 513 F.3d 1164, 1168 (9th Cir. 2008) (quoting *Rewis v. United States*, 401 U.S. 808, 812 (1971)). This "rule is equally relevant in the civil context if the statute at issue" also contains criminal penalties. *LVRC Holdings LLC v. Brekka*, 581 F.3d 1127, 1134 (9th Cir. 2009). "The Supreme Court has long **warned against interpreting criminal statutes in surprising and novel ways** that impose unexpected burdens on defendants" and "no citizen should be held accountable for a violation of a statute whose commands are uncertain, or subjected to punishment that is not clearly prescribed." *Id.* at 1134–35 (internal quotation and citations omitted) (emphasis added). Courts must understand and consider this rule when analyzing whether website advertising cookies and pixels should be considered pen registers or trap and trace devices under the California Pen/Trap Law.

A. Plain Text and Structure of the California Pen/Trap Law Demonstrates that the Law Does Not Apply to Website Advertising Cookies and Pixels

The U.S. Supreme Court has stated that statutory construction is a "holistic endeavor" and a statutory clause or provision that seems "ambiguous in isolation is often clarified by the remainder of the statutory scheme—because the same terminology is used elsewhere in a context that makes its meaning clear, or because only one of the permissible meanings produces a substantive effect that is compatible with the rest of the law." *United Savings Ass'n v. Timbers of Inwood Forest Associates*, 484 U.S. 365, 371 (1988) (citations omitted). Although the California legislature used "expansive language" when defining key terms in the California Pen/Trap Law, expansive does not mean unlimited, and by examining the text and overall structure of the law, it is clear that it does not apply to website advertising cookies or pixels.

The California Pen/Trap Law defines a pen register as "device or process that records or decodes [DRAS] information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, but not the contents of a communication." Cal. Penal Code § 638.50(b). Similarly, a trap and trace device is a "device or process that captures the incoming electronic or other impulses that identify the originating number" or other DRAS information reasonably likely to identify the source of a wire or electronic communication, but not the contents of a communication. *Id.* at § 638.50(c). Thus, these tools both identify telephone numbers and transmission-related communications, but from different perspectives. A pen register tracks outgoing calls/communications, and a trap and trace device tracks incoming calls/communications.

Yet, the text and structure of the California Pen/Trap Law makes it clear that the types of devices and processes at issue are those that capture communications from **specific, targeted devices** and exclude common and ordinary website advertising cookies and pixels that facilitate internet communications to and from indiscriminate commercial website end users. For example, when granting a court the authority to issue an order authorizing the installation and use of a pen register or trap and trace device, the California Pen/Trap Law requires the order to specify, *inter alia*, the (i) identity, if known, of **the person** to whom is leased or in whose name is listed the telephone line to which the pen register or trap and trace device is to be attached, (ii) identity, if known, of the **person who is the subject** of the criminal investigation, and (iii) number and, if known, **physical location of the telephone line** to which the pen register or trap and trace device is **to be attached** and, in the case of a trap and trace device, the geographic limits of the trap and trace order. *Id.* § 638.52(d) (emphasis added). In addition, the California Pen/Trap Law requires the government to furnish, subject to certain procedures and exceptions, notice of its use of a pen register or trap and trace device to "identified **targets** of the order." *Id.* § 638.54(a) (emphasis added). Accordingly, although a pen register and trap and trace device may be defined broadly in terms of the form used to collect data (i.e., a "device or process"), the text and structure of the California Pen/Trap Law makes it clear that these terms are narrow with respect to the type of data collected (i.e., DRAS information) and the targets of the collection (i.e., targeted and identifiable devices).

As described in greater detail below, the state legislature primarily derived the California Pen/Trap Law from its federal counterpart, and the courts interpreting this federal law have also addressed the narrow scope of a pen register and trap and trace device.[2] The case of *In re Appl. U.S. for Order Authorizing Installation and Use of Pen Register and Trap and Trace Device*,

[2] A statute adopted from another jurisdiction is presumed to carry the construction given by the jurisdiction from which the statute was taken. *Jennings v. Alaska Treadwell Gold Min Co.*, (9th Cir. 1909). Therefore, the interpretation of federal courts and agencies with respect to how a pen register and trap and trace are defined under federal law are instructive to how they should be interpreted under the California Pen/Trap Law.

890 F. Supp. 2d 747 (S.D. Tex. 2012) is a good example of this. In this case, the government sought an order authorizing the use of a pen register and trap and trace device to support a narcotics investigation. However, the government did *not* know the actual cellphone number of its primary investigatory target. During a hearing on the government's application for the order, a federal agent indicated that it sought to use a StingRay[3] device "to detect radio signals emitted from wireless cellular telephones" that were in the common area of the investigatory target. *Id.* at 748. The agent would do this by driving a vehicle near the target's home, and then follow the target for a period of time as he travelled. *Id.* According to the government, this technique would enable a federal agent to identify the cellphone number of the target. *Id.*

Magistrate Judge Brian Owsley presided over the case and ultimately denied the order. *Id.* at 752. Specifically, he stated that although the PATRIOT Act "broadened" the definition of a pen register, courts still have determined that a pen register application must seek "information about a **particular** telephone." *Id.* at 750 (emphasis added). Importantly, Judge Owsley emphasized this point by citing several other cases that have reached the same conclusion:

- *United States v. Jadlowe*, 628 F.3d 1, 6 n. 4 (1st Cir. 2010): "A 'pen register' is a device used, *inter alia*, to record the dialing and other information transmitted by a **targeted phone**."
- *In re Application for Pen Register and Trap/Trace Device with Cell Site Location Authority*, 396 F. Supp. 2d 747, 752 (S.D. Tex. 2005): "A 'pen register' is a device that records the numbers dialed for outgoing calls made from the **target** phone."
- *In re Application of the United States for an Order Authorizing the Installation and Use of a Pen Register and a Caller Identification System on Telephone Numbers*, 402 F. Supp. 2d 597, 602 (D. Md.

[3] A "StingRay" device refers to cellular site simulators that replicate the signal of a cellphone tower to force cellphones located nearby to connect to it, which consequently could enable the user (i.e., a law enforcement officer) to download information from the phone or track its location. Department of Justice Policy Guidance: Use of Cell-Site Simulator Technology.

2005): “[A] pen register records telephone numbers dialed for outgoing calls from the **target** phone.”

- *In re Application of the United States for an Order for Disclosure of Telecommunications Records and Authorizing the Use of a Pen Register and Trap and Trace*, 405 F. Supp. 2d 435, 438 (S.D.N.Y. 2005): “Pen Register Statute is the statute used to obtain information on an ongoing or prospective basis regarding outgoing calls from a **particular** telephone.”
- *In the Matter of Applications of the United States of America for Orders (1) Authorizing the Use of Pen Registers and Trap and Trace Devices and (2) Authorizing Release of Subscriber Information*, 515 F. Supp. 2d 325, 328 (E.D.N.Y. 2007): “In layman’s terms, a pen register is a device capable of recording all digits dialed from a **particular** phone.”
- *United States v. Bermudez*, No. 05–43–CR, 2006 WL 3197181, at *8 (S.D. Ind. 2006): “A ‘pen register’ records telephone numbers dialed for outgoing calls made from the **target** phone.”

Id. (emphasis added).

Similarly, a trap and trace device, according to Judge Owsley, also seeks information about a particular phone:

- *In re Application of the United States for an Order Authorizing the Installation and Use of a Pen Register and a Caller Identification System on Telephone Numbers*, 402 F. Supp. 2d at 602 (“[A] trap/trace device . . . records the telephone numbers of those calling the **target** phone.”
- *In re Application for Pen Register and Trap/Trace Device with Cell Site Location Authority*, 396 F. Supp. 2d at 752: “A trap and trace device captures the numbers of calls made to the **target** phone.”
- *Bermudez*, 2006 WL 3197181, at *8: “[A] trap/trace device records the telephone numbers of those calling the **target** phone.”

Id. (emphasis added).

These cases demonstrate that the purpose of a pen register and trap and trace device “is to **track telephone numbers, not people**.” Brian L. Owsley, *TriggerFish, StingRays, and Fourth Amendment Fishing Expeditions*, 66 HASTINGS L. J., 183, 198 (2014) (emphasis added). However, the legal framework governing these surveillance tools does not apply to (and appears to be the exact opposite purpose of) website advertising cookies and pixels that are designed to facilitate internet communications to and from indiscriminate commercial website users. Such advertising cookies and pixels are not designed and are never deployed to target one particular individual like a pen register and trap and trace device. In other words, they are agnostic to the devices used to access the website on which they reside, and they are deployed regardless of whether the website end user is a first-time or repeat visitor. They are primarily used to build customer profiles for marketing purposes and analyze website usage, which simply is not applicable to the context in which pen registers and trap and trace devices are defined for specific, targeted purposes under the California Pen/Trap Law.

B. The Legislative History of the California Pen/Trap Law Reveals No Intention to Regulate or Criminalize Website Advertising Cookie and Pixel Use

In addition to analyzing a statute's plain text and structure, reviewing "[l]egislative history can be particularly helpful when a statute is ambiguous or deals with especially complex matters" and even when a statute's framework "can clearly be discerned from its text, consulting reliable legislative history can still be useful, as it enables [courts] to corroborate and fortify [their] understanding of the text." *Digit. Realty Tr., Inc. v. Somers*, 583 U.S. 149, 171 (2018) (Sotomayor, J., concurring). In turn, by examining the legislative history of the California Pen/Trap Law—and the federal counterpart from which it was derived—one can confirm that it was never intended to regulate or criminalize the use of website advertising cookies and pixels.

In 1968, the United States Congress enacted Title III of the Omnibus Crime Control and Safe Streets Act of 1968, which, *inter alia*, prohibits the interception of "any wire, oral or electronic communication," except in accordance with the strict procedures set forth therein. 42 U.S.C. § 3711, *et seq*. However, in 1977, the Supreme Court indicated that these prohibitions do not apply to pen registers or trap and trace devices, and that federal courts had the power to authorize the installation of these devices upon a finding of probable cause. *United States. v. New York Tel. Co.*, 434 U.S. 159 (1977). Two years later, the Supreme Court held that the installation and use of pen registers and trap and trace devices by law enforcement agencies does not constitute a "search" within the meaning of the Fourth Amendment because these devices do not collect the content of communications and there is no legitimate expectation of privacy in non-content-type of data. *Smith v. Maryland*, 442 U.S. 735 (1979).

Following these developments, Congress enacted the Electronic Communications Privacy Act of 1986 (codified as amended at 18 U.S.C. §§ 3121–3127) (the "Federal Pen/Trap Law"). The law provides that "no person may install or use a pen register or a trap and trace device without first obtaining" certain types of court orders or other government orders mandated by the statute, or during certain emergency situations outlined in the law, or when relevant to the provision of services by a communications provider. 18 U.S.C. § 3121(a). As explained below, the California legislature derived the text for the California Pen/Trap Law from the Federal Pen/Trap Law, and their similarities and key terms are set forth in Appendix A.

The Federal Pen/Trap Law sets forth a specific framework for how federal *and* state officials can submit applications for authorization to install a pen register or trap and trace device. More specifically, at the federal level, an "attorney for the Government" must make an application for authorization to install and use a pen register "in writing under oath or equivalent affirmation, to a court of competent jurisdiction." *Id.* at § 3122(a)(1). Such an application only needs to contain the following two elements: (i) the identity of the attorney or law enforcement officer making the application and the identity of the law enforcement agency conducting the investigation, and (ii) a certification by the applicant of the order that the information likely to be obtained from these surveillance tools is relevant to an ongoing criminal investigation. *Id.* at § 3122(b). Upon a finding that this burden has been met, the court "shall enter" such an order. *Id.* at § 3123(a).

At the state level, the Federal Pen/Trap Law provides that "[u]nless prohibited by State law, a State investigative or law enforcement officer may make" an application for authorization to install and use a pen register "in writing under oath or equivalent affirmation, to a court of competent jurisdiction of such State." *Id.* at § 3122(a)(1). The application must contain the same two aforementioned elements. *Id.* at § 3122(b). Similarly, a "court shall enter an ex parte order" authorizing a pen register or trap and trace device "within the jurisdiction of the court, if the court finds that the State law enforcement or investigative officer has certified to the court that the information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation." *Id.* at § 3123(a)(2).

Under the terms of the Federal Pen/Trap Law, a court receiving an application for a pen register or trap and trace device "is merely to determine whether the applicant had made the necessary certification," and such a review does not require "an independent judicial review of whether the application meets the relevance standard." *In re U.S. Ord. Authorizing Installation and Use of Pen Reg. and Trap and Trace Device*, 846 F. Supp. 1555, 1563 (M.D. Fla. 1994) (internal quotation omitted). Because "it is virtually impossible to botch the simple certification, the court . . . seemingly provides nothing more than a rubber stamp" to a government's application. *Id.*

The Federal/Pen Trap Law sets forth separate procedures for how a pen register or trap and trace device may be installed in emergency situations by federal *and* state officials. More specifically, it provides that, notwithstanding the law's other procedural requirements, any investigative or law enforcement officer specially designated by certain federal officials or "by the **principal prosecuting attorney of any State** or subdivision thereof **acting pursuant to a statute of that State**, who **reasonably determines** that an emergency situation exists" may have a pen register or trap and trace device installed without a prior court order only if an order approving the installation or use is issued within 48 hours after the installation has occurred or begins to occur. 18 U.S.C. § 3125 (emphasis added). The provision for "Emergency Pen Register And Trap And Trace Device Installation" narrowly defines a covered "emergency" to involve specific circumstances, such as immediate danger of death or serious bodily injury to any person, organized crime-related activities, national security threats, and cyberattacks. *Id.* In these circumstances, the official may have a pen register or trap and trace device installed if, within 48 hours, a formal order approving the installation or use is issued in accordance with the law's regular procedures. *Id.*

The California legislature enacted Assembly Bill (AB) 929—the California Pen/Trap Law—in 2015 to create a comprehensive framework governing the use of pen registers and trap and trace devices, including during emergency circumstances.[4] For instance, California Penal Code § 638.51 sets forth the procedures under which a state official can apply for and the standards in which a court grants a pen register or trap and trace device application. The California Pen/Trap Law mirrors the Federal Pen/Trap Law in many respects. *See* Appendix A. However, one key difference between the two laws is the standard used to determine whether the use of a pen register or trap and trace device is appropriate. Here, California Penal Code § 638.52 authorizes magistrates to approve the installation and use of a pen register or trap and trace device if they find that the information likely to be obtained from its use "is relevant to an ongoing investigation and that there is **probable cause** to believe" that it will lead to the discovery of certain types of

[4] After AB 929 was passed, California enacted the California Electronic Communications Privacy Act, which incidentally related to signal information and thus created confusion as to which governed the use of pen registers and trap and trace devices. Thereafter, California enacted S.B. 1121 and A.B. 1924, which reconciled the two laws and did not alter the legislative intent of AB 929.

information defined in the law. *Id.* (emphasis added).

Prior to AB 929, California did not have a statutory framework addressing any of these issues. In fact, the primary reason California enacted the California Pen/Trap Law was to create a framework that authorizes state and local law enforcement officers to use a pen register and trap and trace device under routine and emergency circumstances, and, in doing so, they created a more stringent standard than what is required by federal law. As is clear from the legislative history, the California Pen/Trap Law was intended to address this narrow area and was not intended in any way to regulate the use of website advertising cookies and pixels.

For example, the California Assembly Committee on Privacy and Consumer Protection explained AB 929's purpose in a report as follows:

> Federal law allows law enforcement agencies to use pen register and trap and trace devices, but they must obtain a court order from a judge prior to the installation of the device [which cannot exceed 60 days in duration]. However, during an emergency situation, they may use these devices without a court order if they obtain the court order within 48 hours of the use of the device. Law enforcement agencies must demonstrate that there is reasonable suspicion that the use of the device is relevant to an ongoing criminal investigation and will lead to obtaining evidence of a crime for a judge to authorize the use. . . . However, there is a legal complication with the use of emergency orders. The Los Angeles District Attorney's Office writes, '[t]hough federal law authorizes states and local law enforcement officers to use pen register and trap and trace devices by obtaining a court order first, **it does not allow them to obtain an emergency order unless there is a state statute authorizing and creating a process for states and local law enforcement officers to do so.' California does not have such an authorizing statute, although six other states do** . . . As a result of the lack of an authorizing statute, the Los Angeles District Attorney's Office suggests that some law enforcement agencies have utilized warrantless emergency declarations without proper authorization, which is technically a federal misdemeanor. In response, **AB 929 would explicitly authorize state and local law enforcement officers to use pen register and trap and trace devices, including during emergency situations.**

Pen Registers: Authorized Use: Hearing on AB 929 Before the Assembly Comm. on Priv. and Consumer Protection, 2015-2016 Sess. 5 (Ca. 2015) (emphasis added).

In addition, the California Assembly Committee on Public Safety issued a formal report on AB 929 and focused almost exclusively on the law's emergency provisions. According to the Committee, the California Pen/Trap Law allows magistrates to "grant oral approval for the installation and use of a pen register or a trap and trace device, without an order, if [they] determine all of the following" apply: (i) there are grounds upon which an order for a pen register or trap and trace device could be issued under Section 638.52, (ii) there is *probable cause* to believe that a criminal-related emergency situation exists, and (iii) there is *probable cause* to believe that a substantial danger to life or limb exists, provided all procedural requirements are satisfied. *AB 929: Hearing on AB 929 Before the Assembly Comm. on Public Safety,* 2015-2016 Sess. 4 (Ca. 2015). When discussing AB 929, the California Assembly Committee on Public Safety report repeated the following statement from the Los Angeles County District Attorney's Office: AB 929 would authorize "state and local law enforcement officers to use pen register and trap and trace devices under state law" and "the issuance of emergency pen registers and trap and trace devices." *Id.* at 10. "Under the provisions of AB 929," according to the Los Angeles County District Attorney's Office, "a California court could issue a court order authorizing the use of a pen register and/or a trap and trace device upon a showing of probable cause which is a higher standard than the reasonable suspicion standard required under federal law." *Id.* at 17.

Similarly, the corresponding California Senate Committee on Public Safety held a hearing on AB 929 on June 16, 2015, and specifically indicated that the "**purpose of this bill is to authorize state and local law enforcement to use pen register and trap and trace devices under state law, and to permit the issuance of emergency pen registers**

and trap and trace devices." *Pen Registers: Authorized Use: Hearing on AB 929 Before the S. Public Safety Comm.*, 2015-2016 Sess. 1 (Ca. 2015) (emphasis added).

Further, the primary author of the bill, Edwin Chau, made several formal statements on the scope and purpose of the law. According to Assembly Member Chau:

> AB 929 would authorize state and local law enforcement officers to use pen register and trap and trace devices, including during emergency situations. The bill will require law enforcement officers to obtain a court order before using such devices by providing a judge with information that the use of information is relevant to an ongoing criminal investigation, and that there is probable cause to believe that the pen register or trap and trace device will lead to obtaining evidence of a crime. This higher standard of proof (probable cause vs. reasonable suspicion) is more restrictive than under federal law and is more consistent with California law governing search warrants.

Id. at 10.

These and other legislative records clarify that the legislature primarily enacted AB 929 to create a framework governing how California law enforcement officials could obtain and use a pen register or trap and trace device, including in emergency circumstances. **It was never intended to regulate the use of website cookies and pixels, let alone apply criminal penalties to organizations that deploy these technologies on their websites. There simply is no evidence to support such a conclusion**. Accordingly, for a court to hold that these online technologies are now within the scope of the California Pen/Trap Law would substantially undermine and deviate from the purpose and intent of the California General Assembly.

C. The Scope of Previous Court Orders Authorizing the Use of Pen Registers and Trap and Trace Devices Demonstrates that the Law Does Not Apply to Website Advertising Cookies and Pixels

Both the California and Federal Pen/Trap Laws provide that a court order authorizing a pen register or trap and trace device may require that a provider of wire or electronic communication service, landlord, custodian, or another person furnish law enforcement officials executing the order with "all information, facilities, and technical assistance necessary to accomplish the installation" of the device. *See* Cal. Penal Code § 638.52(h-i); 18 U.S. Code § 3124(a)-(b). This is important because internet service providers routinely assist law enforcement agencies by installing pen registers and trap and trace devices on the internet service accounts and programs they administer.

Yet, given the constitutional concerns with these "assistance" demands, especially because they can result in the "overcollection" of data, both the federal courts and the U.S. Department of Justice (DOJ) have issued rulings and guidance on the scope of pen register and trap and trace device orders and the types of data collected thereunder. *See In re Appl. U.S. for Ord. Authorizing Use of Pen Reg. & Trap*, 396 F. Supp. 2d 45, 49 (D. Mass. 2005); U.S. Dep't of Just., *Policy Regarding Avoidance of "Overcollection" in the Use of Pen Registers and Trap and Trace Devices* (2002). Such rulings and guidance are instructive when interpreting the California Pen/Trap Law.

A pen register or trap and trace device may only obtain any non-content information utilized in the processing and transmission of wire and electronic communications. This requirement applies not just to traditional telephones, but to online activities as well, including email communications and web browsing. According to the DOJ, such non-content information "includes IP addresses and port numbers, as well as the 'To' and 'From' information contained in an e-mail header," but not the "content of a communication, such as words in the 'subject line' or the body of an e-mail." U.S. Dep't of Just., *Electronic Surveillance Manual Procedures and Case Law* (2005).

This DOJ guidance mirrors a Ninth Circuit which concluded that computer surveillance tools that enabled the government to learn the to/from addresses of the defendant's email messages, the IP addresses of the websites he visited, and the total volume of information transmitted to or from his account was "analogous to the use of a pen register." *United States v. Forrester*, 512 F.3d 500, 504 (9th Cir. 2008). The Ninth Circuit provides an extensive analysis on this issue:

> First, e-mail and Internet users, like the telephone users in *Smith,* rely on third-party equipment in order to engage in communication. *Smith* based its holding that telephone users have no expectation of privacy in the numbers they dial on the users' imputed knowledge that their calls are completed through telephone company switching equipment. Analogously, e-mail and Internet users have no expectation of privacy in the to/from addresses of their messages or the IP addresses of the websites they visit because they should know that this information is provided to and used by Internet service providers for the specific purpose of directing the routing of information. . .
>
> Second, e-mail to/from addresses and IP addresses constitute addressing information and do not necessarily reveal any more about the underlying contents of communication than do phone numbers . . . Like IP addresses, certain phone numbers may strongly indicate the underlying contents of the communication; for example, the government would know that a person who dialed the phone number of a chemicals company or a gun shop was likely seeking information about chemicals or firearms. Further, when an individual dials a pre-recorded information or subject-specific line, such as sports scores, lottery results or phone sex lines, the phone number may even show that the caller had access to specific content information. Nonetheless, the Court in *Smith* and *Katz* drew a clear line between unprotected addressing information and protected content information that the government did not cross here.

Id. at 510.[5]

These conclusions are important, as they describe the types of targeted, individualized data that are derived from a pen register or trap and trace device and further distinguish them from website advertising cookies and pixels. *See supra I(A)*. In other words, this framework demonstrates that a pen register and trap and trace device focus on capturing specific types of limited communications from specific, targeted individuals. They clearly were never intended to include common and ordinary website advertising cookies and pixels that facilitate internet communications to and from indiscriminate commercial website users to assist in marketing programs.

D. California Enacted Laws Specifically Designed to Regulate Website Cookies and Pixels

After it enacted the California Pen/Trap Law, the California Legislature enacted the California Consumer Privacy Act of 2018 (CCPA), which was amended by the California Privacy Rights Act of 2020 (CPRA) (codified, as amended, at Cal. Civ. Code § 1798.100-1798.199.100) (the "CCPA/CPRA"). These more recent consumer privacy laws are specifically intended to regulate the use of website advertising cookies and pixels, and courts should refrain from interpreting these two separate legal frameworks as being in conflict as it could require the statute enacted later-in-time to supersede the former. *See Davis v. Hutchinson*, 36 F.2d 309, 312 (9th Cir. 1929) (holding that statutes "should be construed in harmony with the prior legislation" and avoid interpretations creating "direct and unavoidable inconsistency" that may result in "repeals by implication," which "are not favored").

As background, in 2018, the California Legislature enacted the CCPA and, in doing so, expanded the state's already extensive privacy and

[5] Interestingly, *Forrester* speculated (in a footnote) that information related to a Uniform Resource Locator (URL) may be considered the "content" of a communication. *Id.* at n. 6. If true, it could also render the use of such devices outside the scope of the California Pen/Trap Law.

information security legal framework. The law regulated how covered businesses can collect, retain, and sell the personal information of California residents. In November 2020, California voters passed the CPRA in a ballot initiative (known as Proposition 24), which expanded the privacy rights and privileges of California residents and created additional obligations on businesses and service providers that collect and process personal information on Californians.

The CCPA/CPRA defines "personal information" in a complex and expansive manner, and it clearly was intended to regulate the use of, and data derived from, website advertising cookies and pixels. *See* Steven G. Stransky, et. al., *The New CCPA Draft Regulations: Defining the Scope of Personal Information*, Int'l Assoc. of Priv. Pro. (May 7, 2021). Specifically, the term "personal information" means "information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household." Cal. Civ. Code § 1798.140(v)(1). The CCPA/CPRA identifies several categories of data that are considered personal information, including the following:

- Identifiers such as a real name, alias, **unique personal identifier**, online identifier, Internet Protocol address, email address, account name.
- Internet or other electronic network activity information, including, but not limited to, browsing history, search history, and information regarding a consumer's interaction with an internet website application or advertisement.
- Geolocation data.
- Inferences drawn from these (and other) types of personal information to create certain consumer profiles.

Id. (emphasis added).

Further, the CCPA/CPRA broadly defines a "unique personal identifier" as

> [A] persistent identifier that can be used to recognize a consumer, a family, or a device that is linked to a consumer or

> family, over time and across different services, including, but not limited to, a device identifier; an Internet Protocol address; ***cookies, beacons, pixel tags, mobile ad identifiers, or similar technology*** . . . .

Id. at §1798.140(a)(j) (emphasis added).

These terms are significant because they regulate how organizations can disseminate or disclose (i.e., "share") this type of personal information for "cross-context behavioral advertising," which is defined as the "targeting of advertising to a consumer based on the consumer's personal information [e.g., personal data derived from advertising cookies and pixels] obtained from the consumer's activity across businesses, distinctly-branded websites, applications, or services, other than the business, distinctly-branded website, application, or service with which the consumer intentionally interacts." *Id.* at § 1798.140(k).[6] The CCPA/CPRA set forth a framework for **when covered businesses can deploy advertising cookies and pixels on their websites** and when consent for such activities is needed:

- Californians have the right, at any time, to direct a business that shares personal information about them to not engage in such activities (known as the "right to opt out of sharing"). *Id.* at § 1798.120(a).
- A business is prohibited from sharing the personal information of Californians if they have actual knowledge that the consumer is less than 16 years of age unless they are at least 13 years of age and have affirmatively authorized/consented to the sharing of their personal information. *Id.* at § 1798.120(c).
- A business is prohibited from sharing the personal information of Californians if they have actual knowledge that the consumer is less than 13 years of age unless their parent or guardian has affirmatively authorized/consented to the sharing of their personal information. *Id.*

[6] The CCPA/CPRA defines "sharing" as the disclosure or release of a Californian's personal information by an organization "to a third party for cross-context behavioral advertising, whether or not for monetary or other valuable consideration." *Id.* at § 1798.140(a)(h).

The CCPA/CPRA filled a void in California law for regulation of website advertising cookies and pixels. The California Department of Justice emphasized this point in its enforcement action against Sephora USA, Inc. ("Sephora"). *See* Complaint at 2, *People v. Sephora United States*, No. CHC-22-601380, 2022 Cal. Super LEXIS 79250 (Ca. Super. Ct. Aug. 23, 2022) ("Sephora Complaint"). More specifically, the Sephora Complaint alleged that Sephora installed third-party tracking software on its website and in its online application so that it can (through these third parties) monitor individuals who access their online services. *Id.* The Complaint alleged that Sephora failed to properly disclose this activity and provide end users with the ability to opt out from it. Germane to this analysis, the Complaint summarized one of the key purposes of the CCPA as follows:

> Consumers are constantly tracked when they go online. Sephora, like many online retailers, installs third-party companies' tracking software on its website and in its app so that these third parties can monitor consumers as they shop. The third parties track all types of data; in Sephora's case, third parties can track whether a consumer is using a MacBook or a Dell, the brand of eyeliner that a consumer puts in their 'shopping cart,' and even the precise location of the consumer. Some of these third-party companies create entire profiles of users who visit Sephora's website . . . For example, the third party might provide detailed analytics information about Sephora's customers and provide that to Sephora, or offer Sephora the opportunity to purchase online ads targeting specific consumers, such as those who left eyeliner in their shopping cart after leaving Sephora's website . . . Moreover, when a company like **Sephora utilizes third-party tracking technology without alerting consumers and giving them the opportunity to control their data**, they deprive consumers of the ability to limit the proliferation of their data on the web. **California's landmark privacy law, the CCPA, sought to prevent this**.

Id. at 2 (emphasis added).

The California legislature never intended that the California Pen/Trap Law regulate the use of website advertising cookies and pixels. This conclusion is supported by both (i) the plain text of the CCPA/CPRA, which created a specific framework for regulating the use of and consent concerning website advertising cookies and pixels, and (ii) formal legal documents filed by the California Attorney General, who is vested with authority to enforce the California Pen/Trap Law and with certain authority to enforce the CCPA/CPRA. If the California Pen/Trap Law regulated the use of advertising cookies and pixels and by default prohibited such activities without a court order or other exception, then the CCPA/CPRA's legal framework governing the use and consent for advertising cookies and pixels would not be needed. However, as noted above by the California Attorney General, neither the California Pen/Trap Law nor any other California privacy law regulated these activities; accordingly, it was the CCPA—California's "landmark privacy law"—that sought (for the first time) to regulate use of website advertising cookies and pixels. *Id.*

Further, if courts were to ignore this evidence and conclude that website advertising cookies and pixels are also pen registers and trap and trace devices, then it would place the California Pen/Trap Law and the CCPA/CPRA in direct conflict as they set forth different frameworks governing the use of these technologies. In such circumstances, the courts would be forced to nullify the former because the latter entered into force at a later date and was specifically intended to regulate the use of website advertising cookies and pixels. *See Davis*, 36 F.2d at 312. However, just as the plain text, overall structure, and legislative history of the California Pen/Trap Law make it clear that it was not intended to regulate advertising cookies and pixels, the plain text and purpose of the CCPA/CPRA indicate that it was not intended to supersede and modify the California Pen/Trap Law. The two laws can be interpreted harmoniously, with the CCPA/CPRA specifically regulating website advertising cookies and pixels and the California Pen/Trap Law excluding such activities from its scope.

E. Even if Website Advertising Cookies and Pixels Are Pen Registers and Trap and Trace Devices, the California Pen/Trap Law's "User Consent" Exception Permits Their Use

As described above, the California Pen/Trap Law and the Federal Pen/Trap Law are almost identical in their language and scope. S*ee* Appendix A. Importantly, both laws have a similar exception to the prohibition on installing a pen register or trap and trace device: user consent. Specifically, California law provides that a provider of electronic or wire communication service may use a pen register or trap and trace device where "the consent of the user of that service has been obtained." Cal. Penal Code § 638.51(b). The federal law similarly provides that the prohibition on using these devices without a court order does not apply when they are used by a provider of electronic or wire communication service and "where the consent of the user of that service has been obtained." 18 U.S.C § 3121(b). Federal courts have analyzed the scope and meaning of the "user consent" exception in analogous circumstances, as has the DOJ in dealing with trap and trace devices specifically.

In 2001, a group of internet users brought class actions alleging several violations against DoubleClick Inc. ("DoubleClick"), an internet advertising corporation. *In re DoubleClick Inc. Privacy Litig.*, 154 F. Supp. 2d 497 (S.D.N.Y. 2001). DoubleClick embedded its cookies on its clients' websites (i.e., third-party cookies) to assist its clients with targeted advertising. The plaintiffs argued that DoubleClick's storage of cookies on computer hard drives of internet users who accessed websites that featured its advertising violated federal surveillance laws, including (most germane to this issue) the Stored Communications Act (SCA).

The SCA "aims to prevent hackers from obtaining, altering or destroying certain stored electronic communications" and "[i]t creates both criminal sanctions and a civil right of action against persons who gain unauthorized access to communications facilities and thereby access electronic communications stored incident to their transmission." *Id.* at 507 (internal citations omitted). However, the SCA contains an exception to its general prohibition, which mirrors the exception in both the California and Federal Pen/Trap Laws. *Id.* Specifically, the SCA provides that its prohibitions "do[ ] not apply with respect to conduct authorized . . . (2) by a user of that [wire or electronic communications] service with respect to a communication of or intended for that user." *Id.* at 508 (citing 18 U.S.C. § 2701(c)). According to the court, this exception has three parts: (i) identifying the relevant electronic communications service, (ii) determining who are the "users" of this service who can provide the relevant authorization, and (iii) confirming whether these users in fact gave (in this case) DoubleClick sufficient authorization to access plaintiffs' stored communications "intended for" those users. *Id.*

On the first issue, the court summarily determined that an internet service provider "is an entity that provides access to the Internet" and "[a]ccess to the Internet is the service an [internet service provider] provides." *Id.* Therefore, "the 'service which provides to users thereof the ability to send or receive wire or electronic communications' is 'Internet access'." *Id.*

Next, the court noted that federal law defines a "user" as "any person or entity who (i) uses an electronic communication service; and (B) is duly authorized by the provider of such service to engage in such use." *Id.* (quoting 18 U.S.C. § 2510(13)). According to the **court, it is DoubleClick's clients (i.e., the websites that include DoubleClick's third-party cookie on their websites) who are the "users" for purposes of this exception**. *Id.* at 508-9 (emphasis added). According to the court, these website hosts "are (1) entities that (2) use Internet access and (3) are authorized to use Internet access by the [internet service providers] to which they subscribe." *Id.* at 509. Importantly, the court specifically **rejected the plaintiffs' argument that they (the class of internet website end users) are the users who**

must provide the authorization for purposes of the law's exception, and instead found it was the website and their servers that were the users. *Id.* In fact, the court emphasized it was these servers and not the individual owners of the servers who are the "users" for purposes of this exception. *Id.* (emphasis added).

Last, the court found that the "users" provided sufficient authorization to allow DoubleClick to access cookie data stored on an end-user's device. *Id.* at 510. According to the court, this presents two issues: whether the DoubleClick-affiliated websites authorized DoubleClick to access plaintiffs' communications to them and, if so, whether such authorization is sufficient under the law. *Id.* The court found "it implausible to infer that the Web sites have not authorized DoubleClick's access." *Id.* The court then provided the following analysis:

> In a practical sense, the very reason clients hire DoubleClick is to target advertisements based on users' demographic profiles. DoubleClick has trumpeted this fact in its advertising, patents and Securities and Exchange filings. True, officers of certain Web sites might not understand precisely how DoubleClick collects demographic information through cookies and records plaintiffs' travels across the Web. However, that knowledge is irrelevant to the authorization at issue—Title II in no way outlaws collecting personally identifiable information or placing cookies, qua such. All that the Web sites must authorize is that DoubleClick access plaintiffs' communications to them. As described in the earlier section 'Targeting Banner Advertisements,' the DoubleClick-affiliated Web sites actively notify DoubleClick each time a plaintiff sends them an electronic communication (whether through a page request, search, or GIF tag). The data in these notifications (such as the name of the Web site requested) often play an important role in determining which advertisements are presented to users. Plaintiffs have offered no explanation as to how, in anything other than a purely theoretical sense, the DoubleClick-affiliated Web sites could have played such a central role in the information collection and not have authorized DoubleClick's access.

Id.

In conclusion, the court found that all of the plaintiffs' communications accessed by DoubleClick fall within the SCA's "user consent" exception (or outside the scope of the law in general) and, therefore, granted the plaintiffs' motion to dismiss. *Id.* at 513.[7]

In 1994, the DOJ issued a formal opinion on the "user consent" exception within the Federal Pen/Trap Law, and its analysis and conclusions mirror those set forth in the *DoubleClick* litigation. *See* 9 FCC Rcd. 1764, *In re Rules and Policies Regarding Calling Number Identification Service - Caller ID* (1994), *available in* 1994 FCC LEXIS 1858 (1994). Although the DOJ's opinion is in the context of caller identification ("caller-ID") services, its rationale can be applied to website advertising cookies and pixels.

In the 1990s, the Federal Communications Commission (FCC) drafted regulations governing the use and implementation of caller-ID services, which were still in their nascent phases of development. *Id.* at the time, the FCC referred to caller-ID services as a "relatively new telephone service offering which identifies the calling number to the called party" and "a telephone subscriber's number identification device—which is either separately installed or incorporated into the subscriber's telephone—displays the calling party's telephone number between the first and second ring via common channel signaling technology." *Id.* at *86 (Part I of Appendix D) (internal quotations omitted). The DOJ was responsible for determining whether such caller-ID services would, among other issues, fall within the purview of any federal surveillance statute, including the Federal Pen/Trap Law. *Id.* at *85 (Part I of Appendix D).

[7] The court also found that DoubleClick is authorized to access plaintiffs' cookie-related submissions to the DoubleClick-affiliated websites because they are all "intended for" those websites. *Id.* at 511. However, this issue presents an "extra" requirement in the SCA that is not relevant to the Federal and California Pen/Trap Laws and therefore will not be further addressed. *Id.*

At first, the DOJ concluded that a caller-ID service (i) *cannot* be considered a pen register because it does not record or decode numbers dialed from a telephone line, and (2) *can* be considered a trap and trace device because it captures the incoming electronic pulses transmitted by the carrier that identify the originating number of the calling party's telephone line. *Id.* *93-4 (Part III of Appendix D).

However, the DOJ acknowledged that not all uses of trap and trace devices and processes without a court order are illegal, and these restrictions do not apply with respect to the use of "a trap and trace device by a provider of electronic or wire communication service . . . where the *consent* of the user of that service has been obtained." *Id.* at *94 (Part III of Appendix D) (citing 18 U.S.C. §3121). As noted above, this is essentially the same exception as the one set forth in the California Pen/Trap Law. *See* Appendix A. The DOJ then states:

> We conclude that a telephone carrier obtains the 'consent' of the user to have incoming calls trapped and traced when that user subscribes to the carrier's caller ID service, often by agreeing to pay a fee for it . . . **We conclude that the relevant 'user' of the wire communication service with respect to a trap and trace device is the subscriber whose incoming calls are being trapped and traced, not those subscribers whose outgoing calls happen to be identified by such device**. [The Federal Pen/Trap Law] contemplates that a trap and trace device will be 'attached' to just one telephone line. Logically, this can only be the line to which the trapped and traced calls are made. The statute also contemplates that there will be only one 'party with respect to whom the installation and use is to take place.' This can only be the person whose incoming calls are trapped and traced, not the many different persons whose calls happen to be tracked when they call a caller ID subscriber.

Id. at *94 (Part II of Appendix D) (emphasis added).

Therefore, according to the DOJ, the called party (i.e., the caller-ID service subscriber) is considered the "user" referred to in the consent-exception section of the Federal Pen/Trap Law. *Id.* at 96-7. This is the same logic used in *DoubleClick* and can be applied with respect to website advertising cookies and pixels. If one presumes, for the sake of argument only, that these online technologies are trap and trace devices because they can potentially identify end users, such as through an IP address or a social media account identifier captured from a tracking cookie or pixel, then the provision within the California Pen/Trap Law authorizing the use of this technology when "the consent of the user of that service has been obtained" also applies. Cal. Penal Code § 638.51(b).

In other words, for purposes of the California Pen/Trap Law, the applicable internet service providers obtain the "consent" of the website operator to have incoming network communications from website end users "trapped and traced" when the operator subscribes to their services and installs and deploys online tracking technologies whose very purpose is to target their own website end users. *See* 9 FCC Rcd. 1764, 1994 FCC LEXIS 1858, at *95 (1994) (Part III of Appendix D). By following DOJ's reasoning (and by the *DoubleClick* court), one can presume that the California Pen/Trap Law contemplates that a trap and trace device "will be 'attached' to just one" website and this can be the only website to which the trapped and traced communications are made. *Id.* at *96 (Part III of Appendix D). The statute also contemplates only one "party with respect to whom the installation and use is to take place" and "[t]his can only be the person who" has their incoming website communications trapped and traced, "not the many different persons whose" website communications happen to be tracked when they visit a website. *Id.* at *95 (Part III of Appendix D). In all these circumstances, it is the website host/operator that installs the advertising cookie or pixel, and therefore it is this website host/operator that consents to its use.

In addition, the DOJ analyzed whether the "use" of a trap and trace device (i.e., the caller-ID service) was by the subscriber who installed and used the services or the electronic or wire communication service and found it was the latter, and therefore the caller-ID service was within the "user consent" exception of the Federal Pen/Trap Law. According to the DOJ:

> On its own, a subscriber's own number identification device is literally 'useless,' for the device will not 'trap and trace' anything. It is only effective to the extent that an SS7–equipped telephone carrier, at the customer's specific request, uses its own 'devices' to track a subscriber's incoming calls and then deliberately transmits calling party numbers to the subscriber. Thus, a **number identification device can be viewed as a passive recipient of information generated by the carrier and in the form chosen by carrier** . . . The hardware/software of the phone company captures the number and transmits it to an otherwise inert box under the subscriber's ownership and control . . . Moreover, in providing caller ID service to subscribers, a telephone carrier deliberately chooses which 'electronic pulses' to capture and pass along . . . A subscriber's number identification device will be powerless to 'trap and trace' any calling party numbers withheld by the carrier . . . Therefore, the user-consent exception . . . makes it lawful for the telephone carrier, at the request of a subscriber, to capture the telephone numbers of incoming calls on the subscriber's line.

Id. at *99-100 (Part III of Appendix D) (emphasis added).

If a court were, for the sake of argument only, to hold that a website advertising cookie or pixel is considered a pen register or trap and trace device for purposes of the California Pen/Trap Law, then it should also apply the reasoning articulated by the *DoubleClick* court and the DOJ and determine that the use of such technologies is permitted by the "user consent" exception with the law. First, organizations using advertising cookies and pixels on their websites are clearly "users" of the internet service offered by a wire or an electronic communications service provider. It would be "implausible" to infer that the organizations that embed advertising cookies and pixels on their websites have not authorized the internet service provider to enable communications to and from their websites in the exact way they configured them. Second, the internet service provider is ultimately the party "using" the advertising cookie or pixel, just like it is the telephone company that is the party "using" the caller-ID service. In other words, on its own, a website operator's deployment of an advertising cookie or pixel is "literally useless" by itself because it will not and could not "trap and trace" any information or data by itself. *Id*. Rather, these technologies are only effective to the extent that an internet service provider makes information on the website end user (e.g., IP address) available for the website operator and marketing service provider to collect and retain. For purposes of the California Pen/Trap Law, a cookie or pixel can be viewed as a "passive recipient of information generated by the [internet service provider] and in the form chosen" by the provider. *Id*. at *100 (Part III of Appendix D). Accordingly, the user-consent exception also applies to the use of such technologies.

CONCLUSION

The practice of targeting companies for litigation based on how they operate their public-facing websites is not new. These lawsuits are often attractive to plaintiffs because the privacy statutes on which they rely upon as the bases for their legal claims include monetary damages for which an aggrieved party is able to recover. They also require courts to apply archaic privacy frameworks to novel forms of technology. In many circumstances, it is more cost effective for companies to settle these lawsuits out of court instead of pursuing litigation and risk incurring large legal fees or court-ordered damages. The recent surge of legal claims relying on the California Pen/Trap Law align with this framework. If a court were to adopt the position that a website advertising cookie or pixel is considered a pen register or trap and trace device, it would lead to an absurd result that could subject every organization with a public-facing website that uses this technology (without a court order or other exception) to criminal and civil liability, and open the floodgate for more lawsuits. Fortunately, as described above, there are several reasons courts do not have to—and should not—reach such a conclusion.

Appendix A:
Textual Comparison of the California and Federal Pen/Trap Laws

	California Pen/Trap Law	Federal Pen/Trap Law
Pen Register Definition	Means 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, but not the contents of a communication. "Pen register" does not include a device or process used by a provider or customer of a wire or electronic communication service for billing, or recording as an incident to billing, for communications services provided by such provider, or a device or process used by a provider or customer of a wire communication service for cost accounting or other similar purposes in the ordinary course of its business.	Means a device or process which records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, provided, however, that such information shall not include the contents of any communication, but such term does not include any device or process used by a provider or customer of a wire or electronic communication service for billing, or recording as an incident to billing, for communications services provided by such provider or any device or process used by a provider or customer of a wire communication service for cost accounting or other like purposes in the ordinary course of its business.
Trace and Trap Device Definition	Means 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, but not the contents of a communication.	Means a device or process which captures the incoming electronic or other impulses which identify the originating number or other dialing, routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication, provided, however, that such information shall not include the contents of any communication.

	California Pen/Trap Law	**Federal Pen/Trap Law**
Prohibition	Except as provided in subdivision (b), a person may not install or use a pen register or a trap and trace device without first obtaining a court order pursuant to [certain sections of law].	(a) Except as provided in this section, no person may install or use a pen register or a trap and trace device without first obtaining a court order under [certain provisions of law] or an order from a foreign government that is subject to [certain procedures].
Exceptions	A provider of electronic or wire communication service may use a pen register or a trap and trace device for any of the following purposes: (1) To operate, maintain, and test a wire or electronic communication service. (2) To protect the rights or property of the provider. (3) To protect users of the service from abuse of service or unlawful use of service. (4) To record the fact that a wire or electronic communication was initiated or completed to protect the provider, another provider furnishing service toward the completion of the wire communication, or a user of that service, from fraudulent, unlawful, or abusive use of service. (5) If the consent of the user of that service has been obtained.	The prohibition of subsection (a) does not apply with respect to the use of a pen register or a trap and trace device by a provider of electronic or wire communication service— (1) relating to the operation, maintenance, and testing of a wire or electronic communication service or to the protection of the rights or property of such provider, or to the protection of users of that service from abuse of service or unlawful use of service; or (2) to record the fact that a wire or electronic communication was initiated or completed in order to protect such provider, another provider furnishing service toward the completion of the wire communication, or a user of that service, from fraudulent, unlawful or abusive use of service; or (3) where the consent of the user of that service has been obtained.