The New Era of 'Wiretapping': California Courts Continue to See Rise in CIPA Litigation Involving Tracking Technologies and Website Usage

The California Invasion of Privacy Act (CIPA) was originally passed in 1967 to curb unlawful telephone wiretapping. Now, in the age of website tracking technologies, this outdated law is being wielded by plaintiffs' attorneys in a new wave of consumer privacy litigation.

CIPA prohibits the installation of a "pen register" or a "trap and trace device" without first obtaining a court order or without the consent of the user. The statute defines pen register as: "a device or process that records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, but not the contents of a communication." A trap and trace device is defined as: "a device or process that captures the incoming electronic or other impulses that identify the originating number or other dialing, routing, addressing, or signaling information reasonably likely to identify the source of a wire or electronic communication, but not the contents of a communication." Traditionally, these devices were used by law enforcement to record outgoing and ingoing telephone numbers from a specific telephone line. Now, California courts are tasked with determining whether website analysis and tracking tools such as cookies, session replay and chatboxes fall within CIPA's prohibition of pen registers and trap and trace devices.

This onslaught of recent CIPA litigation largely stems from the United States District Court for the Southern District of California's decision last year in *Greenley v. Kochava, Inc.* In *Greenley*, plaintiff (filing a class action suit on behalf of similarly situated California residents) alleged that the defendant was a "data broker" providing software development kits to third-party software application developers. In return, the application developers allowed the defendant to intercept data from application end users which could be sold to the defendant's clients for advertising purposes. According to the complaint, the software development kit allowed defendant to "fingerprint" each unique device and application user, and connect end users to certain devices and devices to certain end users, thereby allowing defendant and its clients to create targeted advertising without the knowledge or consent of the end user. Plaintiff alleged that this practice violated several laws, including CIPA. Defendant filed a motion to dismiss the plaintiff's complaint.

The Court, turning to the definition of pen register provided by the statute, noted that it "could not ignore" the legislature's expansive definition. Accordingly, the Court determined that a pen register "process" could take many forms, *including* software that identifies consumers, gathers data, and correlates that data through unique "fingerprinting." The Court therefore denied the motion to dismiss the CIPA claim, and in doing so opened the floodgates for class action lawsuits alleging violations of CIPA relating to webpage tracking software. The parties in *Greenley* are currently in settlement negotiations.

The *Greenley* decision left California courts with more questions than answers regarding what constitutes a "pen register" for purposes of the CIPA claim, and without clarification from an appellate court or an amendment from the legislature, the legal landscape remains murky at best. Given the emergence

of new and expansive technology, there is significant concern about the potentially expansive consequences these lawsuits can have on any California-based business operating an online webpage. Many websites now include cookies and other tracking technologies that function in ways that could lend to even more CIPA litigation.

A decision last month from a Los Angeles Superior Court provides hope that CIPA will not be subject to as expansive an interpretation as recent claims have attempted to imply. In *Licea v. Hickory Farms*, plaintiff alleged that IP address tracking software on the defendant's website constituted an illegal pen register. The Court disagreed and distinguished the circumstances from those in *Greenley*, finding that the complaint did not establish IP address tracking as equivalent to the "unique fingerprinting" relied upon by the Court in *Greenley*. The Court granted the plaintiff leave to amend the complaint, but included a cautionary warning in dicta that plaintiff's intended broad interpretation of CIPA could "potentially disrupt a large swath of internet commerce."

While the *Licea* decision provided a small comfort to California-based businesses and website operators, it is only a trial-level state court decision and has little precedential value. The legal landscape regarding these new CIPA claims is everchanging at this juncture and businesses should focus on mitigating risk and exposure. Obtaining *prior* consent from users provides the strongest defense to claims of this type. Best practice may include, for example, a pop-up window requiring that users affirmatively acknowledge data collection practices. Additionally, businesses should ensure that all privacy policies and website terms of use are up-to-date and include proper disclosures regarding the types of technologies leveraged by your websites or applications. The policies should include clearly defined terms that put users on notice of what information is being collected and shared, and the extent to which any collected information is shared with third parties.

The attorneys in Bond's litigation and cybersecurity and data privacy practices are monitoring the developments in CIPA litigation and can assist in drafting policies, notices, and alerts to mitigate CIPA and other wiretapping risks. Please contact Amber Lawyer, CIPP/E, CIPP/US or Michaela Mancini if you have any questions regarding these notices or CIPA and its potential impacts.

BOND SCHOENECK & KING ATTORNEYS