Bloomberg BNA

Privacy and Security Law Report®

California Privacy

In this article, the author explores six high tech cases involving California's constitutional privacy right. The cases provide valuable insight into the California right to privacy, such as that California constitutional right to privacy cases are highly fact dependent and unpredictable and that some courts are comfortable recognizing traditional privacy interests while other aren't, the author writes.

Six Modern Technology Cases Involving the California Constitutional Right to Privacy

By Helen Trac

Over 40 years ago, when the citizens of California made privacy a constitutional right, the internet was in its infancy, web browsers would not exist for another 20 years, social networks existed in Rolodexes and location tracking personal devices existed exclusively in the realm of science fiction. The tremendous technological progress of the past few decades has transformed the ways in which we work, live and interact with each other. Yet despite the myriad of changes, privacy advocates have used California's constitutional right to privacy as a tool for protecting some areas of our lives from being monitored and monetized.

Helen Trac is an associate at Hogan Lovells LLP in San Francisco where she represents leading technology companies.

The phrase ''and privacy'' was added to California Constitution, article I, section 1 by an initiative adopted by the voters on Nov. 7, 1972 (the Privacy Initiative). *Hill v. Nat'l Collegiate Athletic Assn.*, 7 Cal. 4th 1, 15 (1994) (Article I, Section 1 of the California Constitution provides: ''All people are by nature free and independent and have inalienable rights. Among these are . . . privacy.''). The California Supreme Court has held that the Privacy Initiative is to be interpreted ''in a manner consistent with the probable intent of [] the voters of the State of California,'' which has led California courts to the (perhaps counter-intuitive) conclusion that citizen's constitutional right to privacy applies not only against public actors, but against ***private*** actors as well. *Hill*, 7 Cal. 4th at 17-20.

A claim under the California Constitutional right to privacy requires three elements: (1) a legally protected privacy interest; (2) a reasonable expectation of privacy under the circumstances; and (3) conduct by the defendant that amounts to a serious invasion of the protected privacy interest. *Hill*, 7 Cal. 4th at 35–37. Even if a plaintiff establishes the three elements, however, the ''diverse and somewhat amorphous character of the privacy right'' may still be balanced with the ''legitimate and important competing interests'' of the defendant. *Id.* at 37-38.

Against this backdrop, this article will explore six high tech cases involving California's constitutional privacy right. The first three cases explore individuals' constitutional right to privacy in the context of three common online activities: web browsing, e-mailing and using social networking sites. The next two cases both

 ISSN 1538-3423

involved location tracking, but had divergent outcomes. The final case involved the assertion, not of a constitutional right to privacy claim, but of an unfair competition law claim premised upon California's public policy on privacy, as evidenced by the constitutional right—a move which allowed the plaintiff to proceed under a Unfair Competition Laws (UCL) ''balancing test'' rather than establishing the three elements of a constitutional privacy claim.

1. *In re Cookie Placement Consumer Privacy Litig.*, 806 F.3d 125 (3d Cir. 2015)

Web browsing and the right to conduct personal activities without being observed. In *Cookie Placement*, plaintiffs alleged that defendants (internet advertising businesses) were surreptitiously exploiting loopholes in the ''cookie blockers'' of leading web browsers. ''Cookies'' are trackers used by companies to monitor an individual's web activity on any website on which those companies feature ads. Leading web browsers had built-in features called ''cookie blockers,'' which prevented the installation of cookies by third-party servers. According to an online report, one of the defendants used hidden forms to trigger an exception to the cookie blocker, which enabled the broad placement of cookies on the browser notwithstanding the blocker.

The phrase ''and privacy'' was added to California Constitution, article I, section 1 by an initiative adopted by the voters on Nov. 7, 1972.

The trial court dismissed the plaintiffs' California constitutional right of privacy claim on the grounds that the defendant's alleged practices ''did not rise to the level of a serious invasion of privacy or an egregious breach of social norms.'' The appellate court reversed, stating that the alleged conduct raised ''different issues than tracking or disclosure alone'' and was distinguishable from cases cited by defendant, due to *how* it accomplished its tracking—*i.e.*, by allegedly overriding user's cookie blockers while concurrently representing in its Privacy Policy that internet users could set their browser to refuse all cookies.

The appellate court then held that the California Constitution protected an individual's interest in ''conducting personal activities without observation,'' and that the reasonableness of a user's expectation of privacy was dependent upon their opportunity to be notified in advance and consent to the intrusion. In its view, an activated cookie blocker equated to an ''express, clearly communicated denial of consent for installation of cookies.'' Thus, the appellate court found that by contravening the cookie blockers, the defendant intruded upon users' reasonable expectations of privacy. As a result, the court held that a reasonable fact finder could deem the alleged conduct to be highly offensive and an egregious breach of social norms.

2. *In re Yahoo Mail Litig.*, No. 5:13-cv-04980-LHK, 3/15/16

E-mails and the right to protect only sensitive or confidential information. In *Yahoo Mail*, the plaintiffs alleged that Yahoo! Inc. scanned and analyzed the contents of e-mails to collect and store user information, including information of non-Yahoo Mail users (who therefore had not agreed to Yahoo Terms and Privacy Policy) with whom Yahoo Mail users communicated. Plaintiffs further alleged that roughly 75 percent of Yahoo's revenue in 2013 came from advertising, and that Yahoo was able to charge more for targeted advertising, which used the user information collected from e-mails. The court held that plaintiffs failed to state a claim under the California constitution, because individuals do not have a legally protected privacy interest and reasonable expectation of privacy in e-mail generally. Rather, the court recognized only a privacy interest in confidential and sensitive content within e-mails. The court further rejected the argument that protecting the public from the ''stockpiling of personal information'' was one of the purposes of the Privacy Initiative.

3. *Low v. LinkedIn Corp.*, 900 F. Supp. 2d 1010 (N.D. Cal. 2012)

Social networks and the right to remain anonymous. In *Low*, the plaintiffs alleged that LinkedIn Corp. provided third parties with their users' LinkedIn browsing history, but with an anonymized LinkedIn ID. The plaintiffs further alleged that third parties could de-anonymize a user's LinkedIn ID number by associating a LinkedIn user ID with the Uniform Resource Locator (URL) of the user's profile page using cookies. The court dismissed plaintiffs' constitutional privacy claim, reasoning: ''[a]lthough Plaintiffs postulate that these third parties could, through inferences, de-anonymize this data, it is not clear that anyone has actually done so, or what information, precisely, these third parties have obtained.'' Accordingly, the court held that LinkedIn's disclosure of a numeric code associated with a user and the URLs of the profile pages viewed was insufficient to establish a serious invasion of a protected privacy interest.

4. *Goodman v. HTC Am., Inc.*, No. C11-1793MJP (W.D. Wash. June 26, 2012)

GPS location tracking and the right to conduct personal activities without being observed. In *Goodman*, the plaintiffs alleged that weather applications on certain HTC smartphones violated users' constitutional right to privacy by transmitting ''fine'' location data, accurate to identify a customer's location within a few feet, rather than ''coarse'' data about a person's location sufficient to provide accurate local weather information. The application transmitted their fine GPS location data every three hours, whenever a user tapped the weather icon, or whenever a device user switched from another application or refreshed the screen.

The court held that because conducting personal activities without observation, intrusion or interference was a protected privacy interests, the plaintiffs adequately alleged a legally protected privacy interest in

  PVLR ISSN 1538-3423

their fine location data and location history. The court further recognized that information about where individuals ''live, work, park, dine, pick up children from school, worship, vote, and assemble, and what time they are ordinarily at these locations'' constituted sensitive personal information. ''GPS data invariably may disclose trips, the indisputably private nature of which takes little imagination to conjure: trips to the psychiatrist, the plastic surgeon, the abortion clinic, the AIDS treatment center, the strip club, the criminal defense attorney, the by-the-hour motel, union meeting, mosque, synagogue or church, the gay bar and on and on.''

California constitutional right to privacy cases are highly fact dependent and unpredictable.

Finally, the court rejected defendants' argument that plaintiffs did not have a reasonable expectation of privacy because of their admission that they expected their smartphones to transmit GPS location data for some apps: ''While Plaintiffs may have expected their phones to transmit fine GPS data occasionally for certain reasons, they did not expect their phones to continually track them for reasons not related to consumer needs.''

5. *Cahen v. Toyota Motor Corp.*, 147 F. Supp. 3d 955 (N.D. Cal. 2015)

GPS location tracking and the right to conduct personal activities without being observed. Despite similar allegations, the court in *Cahen* dismissed plaintiffs' constitutional privacy claim. In *Cahen*, the plaintiffs alleged that the defendants collected vehicle owner data, specifically geographic location, driving history and vehicle performance and then shared that data with third parties without securing the transmission. Plaintiffs further alleged that while defendants disclosed data collection practices in owners' manuals, online privacy statements and the terms and conditions of specific feature activations, drivers could not opt-out of the data collection without disabling the relevant feature.

The court dismissed the plaintiffs' constitutional privacy claim, stating that the ''tracking of a vehicle's driving history, performance, or location at 'various times,' is not categorically the type of sensitive and confidential information the [California] constitution aims to protect.'' The court further noted that plaintiffs did not allege the frequency with which data was being tracked, and that ''[w]ithout more robust allegations,'' it could not infer that defendants were constantly collecting, aggregating and disseminating data about plaintiffs' personal travel locations.

6. *In re Carrier IQ, Inc.*, 78 F. Supp. 3d 1051 (N.D. Cal. 2015)

Litigating constitutional privacy rights under California's unfair competition law framework. Last but not least, in *Carrier IQ*, the defendant marketed a software network diagnostics tool for cell phone service providers, which plaintiffs alleged would collect and transfer sensitive personal data off of a user's mobile device. Moreover, the software allegedly operated in the background, such that the typical user had no idea that it was running and could not turn it off.

Notably, the plaintiffs did ***not*** allege violation of their constitutional right of privacy. Rather, they claimed a violation of the unfairness prong of the California's UCL on the basis that California public policy, as embodied in the California Constitution, recognizes an interest in ensuring that private communications or data are not intercepted. Since a claim under California's UCL unfairness prong is subject to a ''balancing'' test, plaintiffs were able to ''side-step'' the three pronged analysis set forth in *Hill*.

Applying the UCL balancing test, the court held that plaintiffs alleged conduct—i.e., interception and transmission of private and confidential communications and data—could plausibly outweigh the utility of such conduct to defendants. The court further explained that the cost-benefit analysis required ''is not properly suited for resolution at the pleading stage.'' Accordingly, the court denied defendants' motion to dismiss plaintiffs' UCL claim.

Conclusion

Although there are relatively few cases involving California's constitutional privacy right as it applies to online intrusions, the above cases hold some valuable insights. For example, these cases demonstrate that California constitutional right to privacy cases are highly fact dependent and unpredictable. These cases further show that some courts are comfortable recognizing traditional privacy interests, such as one's interest in ''conducting personal activities without observation,'' in non-traditional contexts while others are not. Finally, these cases reveal that combining California's UCL with the constitutional right to privacy may be a powerful strategy for protecting privacy interests that do not fit well under the traditional *Hill* framework.