Web privacy litigation – Where is it heading?

Google and Facebook may know more about us than we want them to, but have they violated any privacy laws?

By Ara Jabagchourian

With the rise of big data in Silicon Valley and beyond, a myriad of issues have arisen as to whether individuals' privacy rights are being trampled upon. These issues have arisen in the context of several litigated matters related to email scanning, click-wrap consent, sale of personal information to brokers, and scanning of unencrypted Wi-Fi. Despite the fact that there has been very little legislation to keep up with the new and expanding technologies being created related to nascent business involving the sale of personal information profiles, litigation has been growing in this area. However, much of the litigation has been driven through the use of statutes that were promulgated decades ago.

When looking at the new wave of privacy cases, some global questions arise. One is whether the laws being applied in these cases are properly suited to deal with the emerging technology. Another question that comes up is whether the rise of these new technologies began the contraction in the scope of privacy under the law. What this article seeks to do is to conduct a brief survey of four recent cases and set forth the issue for discussion on the future of privacy litigation during the rise of big data.

The Federal Wiretap Act

Several cases have been litigated for claimed violations of the Federal Wiretap Act in California. In 1986, Congress amended Title III of the Omnibus Crime Control and Safe Streets Act of 1968 ("Federal Wiretap Act") which sets forth the standards for the government to follow when seeking a wiretap on a private phone line. The purpose of the amendment was "to protect against unauthorized interception of electronic communications." (Senate Report No. 99-541.) The Wiretap Act also provides for a private right of action against a person who "intentionally intercepts . . .any wire, oral or electronic communication." (18 U.S.C. §§ 2511(1)(a) and 2520.) The term "intercept" is defined as "the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device." (*Id*. § 2510(4).) However, pursuant to the Wiretap Act, there is immunity for "intercepting" a communication if the device used is "being used by a provider of wire or electronic communication service in the ordinary course of its business . . ." (*Id*. § 2510(5)(a)(ii).)

Several cases have been brought or are ongoing alleging violations of the Federal Wiretap Act. Three will be discussed in this article: *Joffe v. Google*, *In re: Google Inc. Gmail Litigation*, and *In re Google, Inc. Privacy Policy Litigation*.

Joffe v. Google

Joffe v. Google (9th Cir. 2013) 729 F.3d 1262 involved Google's cars that not only took pictures for their Street View feature, but were also intercepting individuals' unencrypted Wi-Fi networks. The case went up on a writ challenging a denial of a

motion to dismiss. The core question in that case was whether Google's activity fell under one of the statutory exceptions to the Federal Wiretap Act that make it lawful to intercept an electronic communication that is readily accessible to the general public. The court ultimately held that unlike a radio communication that is readily accessible to the public, payload data contained on a Wi-Fi network is not a predominantly auditory broadcast. Nor is Wi-Fi readily accessible to the general public because such transmissions fail to go much further than the walls of a home and is only accessible with some difficulty.

The *Gmail Litigation* focused Google's information mining practice of scanning both outgoing and incoming emails of Gmail users for purposes of collecting individualized information for marketing purposes. (Northern District of California Case No. 13-MD-02430-LHK.) At the motion to dismiss stage, the argument centered on whether the scanning of emails fell under the Federal Wiretap Act's "ordinary course of business" exception. In issuing her decision to deny part of the motion, Judge Koh held "that the ordinary course of business exception is narrow." The Court held that the exception only offers protection from liability where the electronic communication service provider's interception facilitates the transmission. The court rejected the idea that the ordinary course of business equates to anything a company does, citing to *Watkins v. L.M. Berry & Co.* (11 Cir. 1983) 704 F.2d 577 to support the proposition. Given that the interception of the email content was not essential in the ability to provide email services, Google's argument was rejected.

The *Gmail* court also reviewed Google's own policies. The court found that Google's own policies were not clear as to whether or not users of Gmail were in fact consenting to have their emails scanned for creating individual profiles for marketing purposes. Therefore, the court had a second reason to deny the motion to dismiss.

Judge Koh also had to deal with the issue of whether both Gmail users and non-Gmail users (those who sent an email to one with a Gmail account from a non-Gmail account) consented to having their emails intercepted. The court rejected this argument in the motion to dismiss. First, the court held that Google's Terms of Service and Privacy Policies "did not explicitly notify Plaintiffs that Google would intercept users' emails for the purposes of creating user profiles or providing targeted advertising." Google's terms of service indicated that "advertisements may be targeted" based on the contents of information obtained from "Services." The court held that this was not consent, because it only indicated that Google had the "capacity to intercept communications, not that it will." Furthermore, the court indicated that the "Services" was ambiguous enough to mean Google's search engine, not content contained in email.

As for non-Gmail users, Google could not establish that all email users implicitly consented to having their emails scanned. Judge Koh held that Google failed to cite to one case that stands for the proposition that email users consented to having their emails scanned for purposes of third-party marketers. Rather, the cases cited by Google held that the sender of an email consents to the intended recipients' recording of the email.

The last major argument raised in the motion to dismiss was whether the plaintiffs had Article III standing. To establish Article III standing, a plaintiff must make a showing that he/she has suffered sufficient injury to satisfy the "case or controversy" requirement of the United States Constitution. To establish a "case or controversy," a plaintiff must allege (1) an injury-in-fact which is actual; (2) that the injury is traceable to the conduct of defendant; and (3) that it is likely that the injury will be redressed by a favorable decision. (*Friends of the Earth, Inc. v. Laidlaw Envtl. Servs.* (TOC), *Inc*. (2000) 528 U.S. 167, 180-81.)

The court starts its analysis on this point by indicating that in the Ninth Circuit, the injury required under Article III may exist by virtue of "statutes creating legal rights, the invasion of which creates standing." (*Edwards v. First Am. Fin. Corp*. (9th Cir. 2010) 610 F.3d 514, 517.) Since the plaintiffs alleged a Wiretap Act violation, they had properly pled standing under Article III. Under the Wiretap Act and its California counterpart, the California Invasion of Privacy Act ("CIPA") Cal. Penal Code section 630, *et seq*., both have statutory damages, which obviates the need to show actual injury.

With one hand the court giveth, with the other the court taketh away. Despite surviving the motion to dismiss, plaintiffs were not as successful at the class-certification stage. Plaintiffs sought the certification of four classes and three subclasses. The court held that none of the classes could satisfy the predominance requirement of Federal Rules of Civil Procedure, rule 23. The predominance analysis focuses on the relationship between common and individual issues in the case. The first problem the court raised regarding plaintiffs' proposed classes was that the issues of express and implied consent to the interception of the email are both fact intensive.

However, because consent can be implied based on the notice a putative class member may have had from Google directly, third-party disclosures, or the media, this factual inquiry necessarily becomes individualized. Since the inquiry regarding implied consent "requires a close examination of all circumstances," the court held that plaintiffs failed to meet the predominance prong of rule 23.

In re Google, Inc. Privacy Policy Litigation

The *In re Google, Inc. Privacy Policy Litigation* cut out the Federal Wiretap Act claims at the motion to dismiss stage. (Northern District of California Case No. C-12-01382-PSG.) This case centered on Google's change in policy. In Google's

new universal privacy policy, Google indicated that it will combine information from multiple Google products (e.g., Gmail, YouTube, Google Maps, etc.), which includes the user's physical address, IP address, list of contacts, etc. Plaintiffs contend that the universal policy violated Google's earlier policy which required Google to obtain the user's consent if it uses "this information in a manner different than the purpose for which it was collected . . ." The universal privacy policy no longer allows users to keep information gathered from one Google product separate from information gathered from other Google products.

Based on these changes in policy, plaintiffs sought to move forward on a wiretap claim based on the commingling of Gmail information with other Google services. Unlike the rationale in *Gmail*, Magistrate Grewal held in the *Privacy Policy Litigation* that the "ordinary course of business exception" to the Federal Wiretap Act is "broad." Ultimately, Magistrate Grewal held the meaning of the ordinary course exception to be a subjective one, turning on the actual conduct of the business. This ruling was made, knowing that the earlier *Gmail Litigation* decision held a much narrower interpretation of the "ordinary course" exception.

Despite the dismal outcome of the ruling, the court provided a favorable analysis to plaintiffs on the issue of Article III standing. One argument that obtained a favorable reception was the argument that plaintiffs suffered harm in fact by having to pay for the battery and bandwidth consumed by the unauthorized transmissions of information from their cellular telephones. A second argument raised under the injury-in-fact analysis was that one of the class representatives asserted that he would not have bought an Android phone (Google operating system-based phone) had Google disclosed its intention to use his information across all Google products.

The court noted that plaintiffs alleged every time an application was uploaded onto their phone, Google would conduct the unauthorized upload. The court stated that this was enough to establish more than a de minimus injury. As for not having purchased the phone, had one of the class representatives known about Google's change in policy, the court held that the overcharge he paid in purchasing a phone he believed would have more privacy was sufficient to establish Article III standing.

In addition, the court also noted that the violation of the Federal Wiretap Act was sufficient to establish Article III standing, just as in the *Gmail* case. The court held that although Article III always requires an injury, "the alleged violation of a statutory right that does not otherwise require a showing of damages is an injury sufficient to establish Article III standing." Thus, actual injury does not need to be shown under Article III because if statutory damages are set forth by the Legislature, then it is presumed that injury has occurred.

Video Privacy Protection Act

In re Hulu Privacy Litigation (N.D. Cal. June 17, 2014) 2014 WL 2758598 involved an alleged violation of the Video Privacy Protection Act ("VPPA"). The VPPA was a law that was promulgated after the Washington Post had published a story on Judge Bork's video rental history during his Senate confirmation hearing for the United States Supreme Court. The VPPA protects personal information of an individual who obtains video materials. (18 U.S.C. § 2710.) The information that is protected is that which identifies a person as having requested or obtained specific video material.

Hulu is an Internet video service provider which obtains licenses from studios, networks and other right holders to broadcast their shows. Hulu makes its money in two primary ways: through paid subscriptions and through advertising revenue. In order to market itself to advertisers, Hulu must obtain verified metrics from approved companies, such as comScore.

Facebook collects information and processes content shared by its users. It then provides that information to marketers when it sells them its products. Marketers then take this information and target their ad campaigns to specific users. Facebook makes its money from this advertisement revenue.

Plaintiffs alleged that Hulu transmitted their identifying information and the videos they watched to comScore and Facebook. The court granted summary judgment as it related to Hulu's transmissions to comScore because the information was provided as an aggregate, which did not identify a particular individual. However, the court held that there were material issues of fact as it related to Facebook's motion for summary judgment.

A class certification was brought against Facebook. Through the summary judgment motion and hearing, the class harm was narrowed to the transmission of Facebook ID cookies of users of Hulu who hit the Like button on Facebook. So the class members had to be both Hulu and Facebook users. The court presumed that the information between Hulu and Facebook can be cross-referenced to be able to tell which individual's information was transmitted from Hulu. However, the court held that this was not sufficient to satisfy the ascertainability prong.

The court delved into how, in this case, it can be determined whether someone's personal information was in fact transmitted from Hulu to Facebook. The case-specific issue was that a user cookie had to be sent by Hulu to Facebook. Whether this cookie was not only sent, but kept in one's browser, turned on numerous variables. These included whether a user stayed logged onto Facebook, whether they cleared cookies, or used ad-blocking software. Given these particularized issues, the court held that the class is not amendable to ready verification. However, the court denied the class motion without prejudice; providing plaintiffs with the opportunity to redefine the class and subclasses.

One additional argument was raised that was noteworthy in the class certification order involving the statutory damages sought. The argument raised by Hulu was that by certifying a class where, in this case, each violation has a statutory damages amount of $2,500, permitting such damages over the aggregate of a large class would violate Hulu's due process rights, as the damages can reach into the billions of dollars and are out of proportion to the "actual" harm. The court noted that the Ninth Circuit has refused to certify a class based on due-process grounds where the statutory treble damages involved $750 million, noting that each claim involved only minimal damages. (*Kline v. Coldwell Banker & Co.* (9th Cir. 1974) 508 F.2d 226, 234-235.) The court also discussed that the Second Circuit has held that a defendant may invoke the Due Process clause, "not to prevent certification, but to nullify the effect and reduce the aggregate damage award." (*Parker v. Time Warner Entertainment Co*. (2d Cir. 2003) 331 F.3d 13, 22.) The court acknowledged that this argument need not be addressed in full given the denial of the motion on ascertainability grounds.

New business models, old rules

As can be seen, these cases seek to take on new business models that did not exist at the time the laws that are being prosecuted were promulgated. However, the purposes of those laws have just as much validity to these new business practices as they did to the concepts of wiretaps and disclosure of who is watching what videos. Given that these privacy cases are still making their way up the appellate ladder, the issues of applicability, ascertainability, standing, and due process appear to be in the forefront. Until there are some decisions on these issues at the Ninth Circuit and beyond, it is not at all clear whether the privacy class action practice is one where a difference can be made for the public. It is further not clear whether any new legislation will come about dealing with these issues given that the decisions have not prohibited the business conduct of these high-tech marketers. Despite these cases, firms are still actively pursuing these actions and applying creative solutions to these legal problems.


Jabagchourian

Ara Jabagchourian of the Law Office of Ara Jabagchourian, *practices civil litigation in several areas, including financial fraud, injury and intellectual property. Prior to joining private practice, Jabagchourian served as a staff attorney for the Federal Trade Commission's Bureau of Competition in Washington, D.C.*