The Computer & Internet Lawyer

Volume 30 ▲ Number 10 ▲ OCTOBER 2013

Ronald L. Johnston, Arnold & Porter, LLP Editor-in-Chief

Intent-Based Advertising for Lawyers

By Randi W. Singer and Damien Kieran

In 2012, smartphones represented 18 percent of total global handsets and 92 percent of traffic.[1] Global smartphone usage grew 81 percent last year, and some industry analysts predict that the number of mobile-connected devices will exceed the number of people on earth by the end of 2013.[2] Staying connected no longer means just having a home or work-Internet connection; today, we are connected no matter where we are or what we are doing. This 24/7 connectivity poses opportunities for advertisers that were undreamed of even just a few years ago. Now, there is a constant window to serve advertisements and a treasure trove of data gathered from social media and from location-based technology through mobile devices to make these advertisements more relevant than ever.[3] These opportunities, however, also raise a host of legal issues, from privacy concerns to wire-tapping to outright fraud, which need to be evaluated against an evolving legal framework that simply cannot keep up with the technology.

Indeed, intent-based advertising is likely to become an even more integral part of daily life in the future. The advent of ever-increasingly-integrated mobile devices such as Google's Glass Project, which will be publicly available in late 2013, will place a display constantly within a user's field of vision no matter what he or she is doing.[4] Coupled with the endless potential for social media interaction that such devices create and the constant stream of data those interactions produce, advertisers will have the ability to serve customized advertisements specifically tailored to the particular user at the particular moment in time directly and seamlessly into the consumer's line of sight (or to his wrist *via* a smart watch[5]) at any given time.

This article briefly outlines some of the most interesting developments relating to intent-based advertising solutions including some recent high profile cases: Google settled with the Federal Trade Commission (FTC) for a record $22.5

Randi W. Singer is a litigation partner in the New York office of Weil, Gotshal & Manges LLP, where her practice focuses on copyright and Lanham Act false advertising and trademark litigation, and other intellectual property issues. **Damien Kieran**, a former litigation associate at Weil, is currently an associate at Paul, Weiss, Rifkind, Wharton & Garrison LLP in New York. This article was published originally in the Practising Law Institute course handbook *Hot Topics in Advertising Law 2013*.

Wolters Kluwer
Law & Business

million in 2012 over allegations relating to Google's misrepresentation of its use of tracking cookies in Apple's Safari browser; at the start of this year, UK users of the same Safari browser sued Google over the same secret tracking cookies; a class action was filed against Facebook seeking $15 billion in damages for wiretapping and privacy violations allegedly based on Facebook's use of cookies;[6] and KISSmetrics settled a class-action lawsuit by promising to avoid using ETags or other so called "supercookies" to track users online without first notifying them and giving them a choice.[7]

Caution: If you are contemplating using intent-based advertising or data mined from social media, search, or location based tools, you should consult an experienced attorney because there are myriad issues beyond the scope of this article that should be considered, including intellectual property concerns, broader data privacy issues, criminal concerns, and innumerable unknowns due to the differences between each advertising platform's functionality and the fact that the technology evolves faster than laws and policies adapt.

Evolving Uses, Conceptions, and Ideals of Data

Advertisers have long understood the value of using consumer data to make advertisements more relevant to the consumer. Historically, agencies set up focus groups to see how potential consumers would react to a product or advertisement and conducted surveys of consumers that had bought or used a product or seen an advertisement to refine products and advertising strategies. Today, it is possible to "observe" actual consumer behavior and to obtain such information without actually having to interact with consumers. Advertisers can easily obtain a user's likes, dislikes, length of time spent on a particular Web site or even a particular page, friends, social circles, and even the physical location of consumers to within a few feet. Together, these data points allow advertisers to effectively guesstimate where a consumer is going, what he or she is doing, and—importantly for the advertisers' purposes—what the consumer might want to do or need in the near future. It is possible to serve the perfect advertisement at the perfect time, customized to the individual consumer's needs.

But as users become more sophisticated and norms regarding privacy evolve, their conceptions and expectations of how data will be used changes faster than the policies and laws meant to protect both advertisers and users. Indeed, earlier this year during the annual World Economic Forum at Davos, considerable time was spent discussing how the world is changing with regards to the use of data.[8] For example, data traditionally were collected with user awareness, but today, data are traded passively between machines, making it difficult to notify individuals and acquire consent for collection. While the definition of data was historically predetermined or binary, today it is contextual and dependent on fast-changing social norms. Data used to be collected for specified uses, but now the economic value and innovation of data comes from the combining of data from multiple data sets and subsequent uses. Moreover, traditionally, a user was the data subject, but today, the user is the data subject, controller, and processor. Whereas individuals used to provide legal consent for use of data without being truly engaged in what that consent meant, today users engage and understand how data is used and the value created in it. Furthermore, traditional policy frameworks were designed to protect the user or minimize risk to the user, but today, policies are trying to protect the user and at the same time balance that protection with innovation and economic growth.[9]

What Is Intent-Based Advertising?

Picture Paul, an avid Facebook, Foursquare, and Twitter user. Paul has gone every third weekend to his favorite barbershop near his home. During his appointment, Paul checks in on Foursquare, alerting other Foursquare users and his friends to where he is. He sends a tweet or two about the great cut he is getting while tagging his location. Finally, Paul posts an arty picture of the barbershop floor to Facebook that his friends begin to comment on. Every one of these interactions can be logged and, over time, forms a web of useful analytical data.

Today, it is possible to "observe" actual consumer behavior and to obtain such information without actually having to interact with consumers.

A few months later, on the same day Paul always goes to the barber, he logs into Facebook and sees an ad for Joey's Barbershop, which just opened three blocks from Paul's house, much closer than his regular barbershop. Two of his friends have even been there and liked it. Next, Paul goes on Twitter and sees a direct message to Paul from Joey's Barbershop: "It's haircut day! Why don't you give us a try? Your friends Ross and Drew did and they loved us!" Paul goes to his Foursquare account and sees a message showing that his friends Ross and Drew used Joey's Barbershop recently and that it is currently only three blocks away. These advertisements or direct response campaigns can be viewed as intent-based advertising campaigns. They harness data about

Paul to effectively allow an advertiser to push the most relevant advertisements to Paul at the best time—when the advertisement will best match his desired intent.

But how do advertisers obtain the information to tailor these advertisements? There are numerous possibilities, but the two main ways data can be obtained without the user expressly supplying data (*e.g.,* by liking something on Facebook, or checking on Foursquare) to a service or advertiser are through the use of cookies and mobile device location awareness.

Cookies Everywhere, But Nothing to Eat

A cookie is a small piece of data sent from a Web site and stored in a user's Web browser.[10] Cookies originally were designed to allow Web sites to remember what state the Web site was in. For example, cookies remembered what buttons a user had pressed or links he had opened so that if the user ever came back to the Web site, those past interactions could be reflected. However, cookies have become far more intelligent and complicated, and, for advertisers, much more useful.

Tracking cookies have the same basic deployment as benign conventional cookies, but once embedded, they track a user's long-term habits to compile records of the individual's browsing histories, including information such as how long the user was on a given Web site, and the way the user interacted with that Web site. Cookies basically can be developed to target specific browsing habits. These long-term data promise tremendous rewards for advertisers and huge headaches when misused.

Indeed, concerns regarding cookie usage prompted the European e-Privacy directive, which requires explicit consent from users before a cookie can be embedded and used in a browser.[11] Although a bill containing similar restrictions for cookies in the United States was introduced, it died after referral to the Senate Commerce, Science, and Transportation Committee.[12]

Mobile Device Location Awareness

A recent *New York Times* article noted that there are "three things that matter with consumer data collection: location, location, location."[13] After all, for Joey's Barbershop to serve Paul its advertisement in the most efficient and effective way depends on knowing that Paul actually needs his haircut and is near the shop or on his way to another barbershop. How can Joey's Barbershop get that information? What governs its use of that information?

The first way for Joey's Barbershop to get the information is through cell-phone towers.[14] Cell towers can identify the localized area where a mobile device user is located. A Wi-Fi hotspot also can give up the location because Wi-Fi networks are local and generally tend to cover a relatively small area.[15] Third and most accurate, Global Positioning Systems (GPS) rely on satellites bouncing a signal to a user's mobile device to determine location.[16] Finally, crowd sourcing uses various Wi-Fi networks and cell tower locations to create a map and determine location based on the signals received by a mobile device.[17]

A 2012 report on Mobile Device Location Data by the US Government Accountability Office notes that there are considerable consumer privacy risks with this information: "[a]ccording to privacy advocates, when a user agrees to use a service that accesses location data, the user is unlikely to know how his or her location data may be used in ways beyond enabling the service itself."[18] Moreover, the report notes that third parties may vary in their own levels of security, so the richly-detailed profile of individualized consumer behavior that can be created by location tracking is open to exploitation through unwanted solicitation or other nuisances—not to mention identity theft and surveillance. Indeed, the Mobile Device Location Data report notes that companies currently do not take consistent steps to protect this information even though users are becoming more aware of the usage of their data.[19]

The richly detailed profile of individualized consumer behavior that can be created by location tracking is open to exploitation through unwanted solicitation or other nuisances.

For now, the Fair Information Practices Act, which was first enacted in 1973 and remains largely unchanged, the Communications Act of 1934 (Communications Act), and the Electronic Communications Privacy Act of 1986 (ECPA) basically are all that govern the tracking of users' locations based on their mobile devices.[20] These are beyond woefully out of date; the Senate has recently been working on a bill that would heavily regulate location data collection, but to date, nothing specifically on point exists.[21]

Recent Activity

Although there have been several lawsuits and FTC cases involving data in the privacy context, there has been a dearth of litigation concerning location-based services. But common sense and the issues highlighted in the US Government Accountability Office's Mobile

Device Location Data report suggest that it is only a matter of time before the synergy between location-based data and advertisers results in litigation.

Google Settles Privacy Misrepresentations with FTC

In late 2011, Google entered into a consent order with the FTC to settle charges stemming from allegations that Google had used deceptive tactics and violated its own privacy promise to Gmail users when it launched its Google Buzz social network. Among other provisions of the consent order, Google was required not to "misrepresent[] in any manner, expressly or by implication" the extent to which consumers could exercise control over the collection of their information.[22]

Fast-forward to 2012: In a second complaint against Google, the FTC alleged violations of §§ 5(i) and 16(a) of the FTC Act. The complaint alleged that, during portions of at least 2011 and 2012, Google placed advertising tracking cookies on the computers of Apple Safari browser users who visited Web sites within Google's DoubleClick advertising network despite the fact that Google's terms indicated that the default settings on Safari's browser would opt users out of such cookies. (Google found a workaround that, notwithstanding the default settings, allowed it to place a cookie on consumers' computers by exploiting an exception to the browser's default settings. Once that first cookie was embedded in the browser, it allowed the other DoubleClick cookies to operate on the user's computer including tracking cookies.) As its conduct violated its original consent order, Google agreed to pay a record settlement of $22.5 million to settle the charges against it.

Although it is not clear whether there was any intentional or even negligent conduct on Google's part, it is clear that privacy violations of this sort will not be tolerated any longer.

Google UK Sued Over Safari Browser Cookies

On the back of the FTC settlement in the United States, a group of British Safari browser users have sued Google in the UK courts. They have lodged the same allegations regarding Google's cookie practices that were asserted against Google in the United States. This lawsuit was just filed in January 2013 but is worth keeping an eye on to see how European courts view these practices and whether they are prepared to allow these activities.

KISSmetrics Settlement

In August 2011, UC Berkley researchers published materials demonstrating that some of the Internet's most popular Web sites were using a tracking service called KISSmetrics. These materials were widely circulated on the Internet. The most startling part of the reports claimed that KISSmetrics's tracking cookies—Etags—could not be blocked even if you manually did so in your browser settings, turned off your Flash storage, or even used incognito settings in your browser. Shortly after the report was published, a class action lawsuit was filed against KISSmetrics in the Northern District of California alleging, among other things, state law violations and violation of 18 U.S.C. § 1030 (the ECPA), which broadly prohibits the illegal access of computers or computer data without authorization.[23] In essence, the lawsuit claimed that KISSmetrics had surreptitiously tracked users through the use of tracking cookies.

KISSmetrics and the putative plaintiffs reached a settlement in October 2012. The two named plaintiffs received $5000, while the lawyers received approximately $500,000 under the settlement.[24] Although the amounts involved are small, this case may well be a test case to warm up for bigger things to come. In any event, it is clear that advertisers should exercise caution in collecting, purchasing or using user data.

Facebook Class Action

In May 2012, a class action lawsuit was filed against Facebook for among other things wiretapping and tracking its users through the use of cookies.[25] The lawsuit seeks $15 billion in damages. It is alleged that Facebook tracked the activities of its 150 million US users even when they had logged out of Facebook. Given the size of the claims involved and that the technology involved could affect all advertisers, developments in this case might be worth following.

Notes

1. Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2012-2017, *http://www.cisco.com/en/US/solutions/collateral/ns341/ns525/ns537/ns705/ns827/white_paper_c11-520862.html* (last visited August 21, 2013).
2. *Id.*
3. "Unlocking the Value of Personal Data: From Collection to Usage," *World Economic Forum*, February, 2013 at 7.
4. Google Glass, *http://www.google.com/glass/start/* (last accessed August 21, 2013).
5. Nick Bolton, "Disruptions: Where Apple and Dick Tracy May Converge," *New York Times*, February 10, 2013, *http://bits.blogs.nytimes.com/2013/02/10/disruptions-apple-is-said-to-be-developing-a-curved-glass-smart-watch/* (last accessed August 21, 2013).
6. In re Facebook Inc., Internet Tracking Litigation, No. 5:12-md-02314-EJD, May 17, 2012 (N.D. Cal.)

7. Kim v. Space Pencil, Inc., C 11-03796 LB, 2012 WL 5948951 (N.D. Cal. Nov. 28, 2012).
8. World Economic Forum, *supra* n.3.
9. *Id*.
10. PFMAG Encyclopedia, *http://www.pcmag.com/encyclopedia_term/0,2542,t=cookie&i=40334,00.asp* (last accessed August 21, 2013).
11. Directive 2002/58/EC.
12. Bill S.91(112TH), *http://www.govtrack.us/congress/bills/112/s913* (last accessed August 21, 2013).
13. Natasha Singer, "Their Apps Track You. Will Congress Track Them?," *New York Times*, January 5, 2013, *http://www.nytimes.com/2013/01/06/technology/legislation-would-regulate-tracking-of-cellphone-users.html* (last accessed August 21, 2013).
14. "Mobile Device Location Data: Additional Federal Actions Could Help Protect Consumer Privacy," *US Government Accountability Office* (September 2012) 11.
15. *Id*.
16. *Id*.
17. *Id*.
18. *Id*. at 16.
19. *Id*. at 20.
20. *See* "US Government Accountability Office Report on Mobile Device Location Data," September, 2012 at 6.
21. Information on Sen. Franken's draft bill S.1223 is available on his Web site. *http://www.franken.senate.gov/files/documents/121011_LocationPrivacyProtection.pdf* (last accessed August 21, 2013).
22. The Decision and Order are available at *http://www.ftc.gov/os/caselist/1023136/111024googlebuzzdo.pdf.*
23. *Kim*, C 11-03796 LB, 2012 WL 5948951.
24. *Id*. at Dkt#97-2.
25. In re Facebook Inc., Internet Tracking Litigation, No. 5:12-md-02314-EJD (N.D. Cal. May 17, 2012).