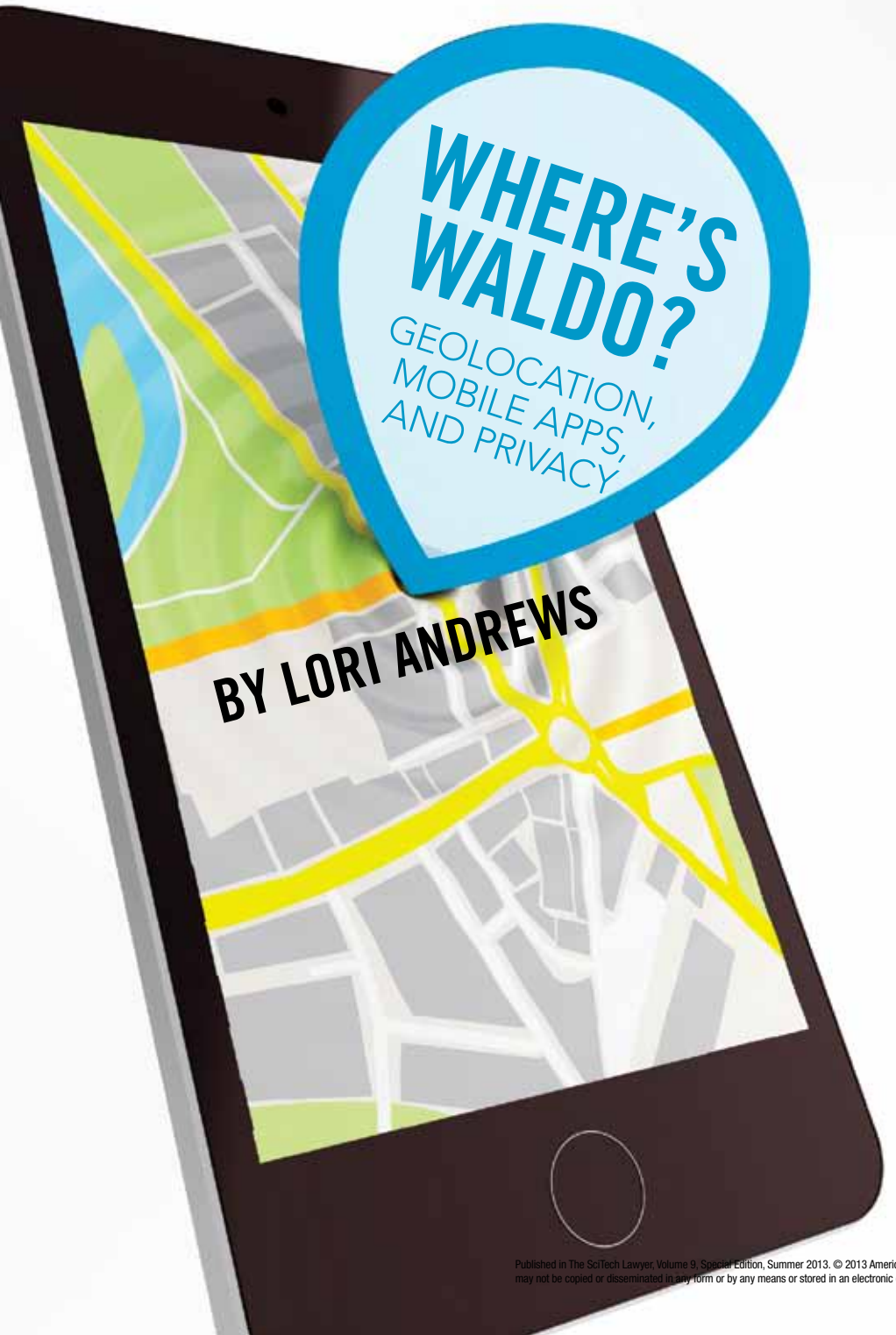
7-1-2013

Where's Waldo?: Geolocation, Mobile Apps, and Privacy

Lori Andrews
IIT Chicago-Kent College of Law, landrews@kentlaw.iit.edu



WHERE'S WALDO?

GEOLOCATION, MOBILE APPS, AND PRIVACY

BY LORI ANDREWS

Where in the world is Carmen Sandiego? Well, if she's got a Droid, Google knows where she is. If she checks in on Foursquare or posts a picture on the mobile version of Facebook, her friends know where she is. Even the games she plays on her phone—such as Angry Birds—collect information about her location.

Where's Waldo? If his parents have downloaded the PhoneSheriff app to his smartphone, they can track his location. Or they can use any number of apps to keep a digital eye on him. With WebWatcher Mobile, they can see what he is texting to friends and what he is looking at online. And with AirCover Family Locator, they can create an electronic fence around their child and get an alert if he and his smartphone leave a particular perimeter.

Virtually all of us are carrying devices that collect or record our location and that transmit data about our calls, our texts, and our searches. The vast majority of US adults (87%) own a cell phone, and more than half of cell phone owners (52%) have a smartphone. Many of us cram our cell phones with apps. Back in 2008, Apple and Google offered a total of 600 apps; now they offer more than a million.

According to a February 2013 Federal Trade Commission Staff Report, data collected via a mobile device can reveal habits and patterns that expose a person's way of life. FTC Chairwoman Edith Ramirez has indicated that mobile devices pose unique privacy problems because they:

1. are personal, as opposed to a shared computer;
2. are portable and often carried to different locations;
3. can collect a variety of information on users, from contact information to geotag locations to installed mobile apps;
4. are popular with younger people, such as teens and children, who may not be as aware of or concerned with personal privacy;
5. are capable of being payment devices; and

Published in The SciTech Lawyer, Volume 9, Special Edition, Summer 2013.

6. have smaller screens, which make it harder to convey privacy notices and other relevant information.

People Don't Realize What They're Disclosing

People often do not realize what they are disclosing when they use mobile apps. A 2008 *Consumer Reports* poll found that "61% of Americans are confident that what they do online is private and not shared without their permission" and that "57% incorrectly believe that companies must identify themselves and indicate why they are collecting data and whether they intend to share it with other organizations." Yet a study by *The Wall Street Journal* in 2010 found that more than half of 101 popular apps transmitted users' unique identifiers to third parties without consent; 47 apps transmitted phone location; and Pandora, a music app, transmitted each user's age, gender, and the device ID location to advertisers. A 2011 joint report by TRUSTe and Harris Interactive found that only 19 percent of the top 340 free mobile apps contained a link to a written privacy policy.

In a 2012 study of 400 mobile apps for kids, the FTC found that nearly 60 percent (235) of the reviewed apps transmitted the device ID to the developer or a third party, such as a data aggregator. Fourteen of these apps also transmitted geolocation information or phone numbers. Despite these practices, only 20 percent (81) of the apps had an accessible privacy policy that disclosed what information they shared with third parties. Consequently, parents and children cannot adequately determine which apps can be safely downloaded. Adults posing as teens were able to use a geolocation app to lure a 12-year-old girl, a 13-year-old boy, and a 15-year-old girl into settings where they raped the children.

Data aggregators turn our personal information into their profit. Acxiom has data on half a billion people from around the world. The company has an average of 1,500 pieces of data on each person ranging from credit scores to medication purchases. Google collects information from its 60 products and services—Google scans Gmail messages, stores search engine queries, tracks which websites a person visits while signed into his or her Google account, assesses what a person watches on YouTube, tracks location information from Android phones, and gathers information from its own social network Google+.

Nielsen is a global marketing and information research company that is active in more than 100 countries and serves more than 20,000 clients. Nielsen boasts that its "Online Measurement" service provides clients with "a 360 degree view of how consumers engage with online media." The company explains that, "Our approach doesn't stop at the computer screen because we understand that online audiences don't just consume digital 'cookies'—they're a shopper, a car-pooling power mom, a TV watcher, a tweeter and a texter." Nielsen collects information from 130 million blogs, 8,000 message boards, Twitter, and other social networks.

Why Location Data Can Be Problematic

Whole businesses are being created around linking mobile device location information to other data about our activities, desires, and purchases. Algorithms can be applied to that data set to make assumptions about us in ways that could benefit—or disadvantage—us. If I enter a particular store, I might receive a coupon on my phone for a discount in that store (a near-term benefit). But other entities might use that information against me. Kevin Johnson, a condo owner and businessman, held an American Express card with a $10,800 limit. When he returned from his honeymoon, he found that the limit had been lowered to $3,800. The switch was not based on anything Kevin had done but on information about where he shopped. A letter from the company told him: "Other customers who have used their card at establishments where you recently shopped have a poor repayment history with American Express."

At first glance, the disclosure of

PEOPLE OFTEN DO NOT REALIZE WHAT THEY ARE DISCLOSING WHEN THEY USE MOBILE APPS.

THE FTC STAFF REPORT ENTITLED MOBILE PRIVACY DISCLOSURES:

Building Trust Through Transparency (February 2013) recommends the following for mobile platforms:

"Consider obtaining affirmative express consent for content that consumers would find sensitive in many contexts, such as contacts, photos, calendar entries, or the recording of audio or video content."

"Consider developing a one-stop 'dashboard' approach to allow consumers to review the types of content accessed by the apps they have downloaded."

"Consider developing icons to depict the transmission of user data."

"Promote app developer best practices. For example, platforms can require developers to make privacy disclosures, reasonably enforce these requirements, and educate app developers."

"Consider offering a Do Not Track (DNT) mechanism for smartphone users. A mobile DNT mechanism, which a majority of the Commission has endorsed, would allow consumers to choose to prevent tracking by ad networks or other third parties as they navigate among apps on their phones."

location information might not seem that troublesome. After all, if we're out at a bar or on a boat on a lake, that's a public space where we seem to have already given up our privacy. But location data is problematic. Where we are can reveal sensitive information about us. Are we at a synagogue, a mosque, or a church? Are we meeting with a competitor of our current employer? Are we at an AIDS or abortion clinic, or perhaps at a lover's apartment? As Justice Sotomayor pointed out in *U.S. v. Jones*, "GPS monitoring generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations."

People use mobile devices to transmit ever more personal information as they look up and hook up. People live their most intimate lives digitally these days. They may sext a nude photo to a lover or do a Google search for a divorce lawyer. They may schedule a doctor's appointment or enter health information into one or more of the 40,000 available medical apps.

According to a 2013 study released by the Pew Research Center's Internet and American Life Project, more than half of smartphone owners (52%) use their devices to get health information, and roughly one-fifth of smartphone owners (19%) have health apps. On the positive side, mobile health apps not only help people obtain information about and monitor their condition, but they also can be used to study health patterns and determine public health policies. In the Asthmapolis study, the city of Louisville is using data from asthma sufferers' GPS-equipped inhalers to pinpoint which parts of the city are the most polluted.

Yet health information from mobile devices can also be used in ways that disadvantage people. An employer might turn down an applicant who "likes" the American Cancer Society or checks in on Foursquare at a doctor's office, because the employer wants to avoid hiring someone who might incur costly medical bills. A nursing home might deny admission to someone who had done a Google search for a particular disorder that the nursing home managers did not want to deal with. By aggregating data about people, social institutions may be creating more precise portraits of people that can be used for discriminatory purposes.

Life insurance underwriting has traditionally been based on urine and blood samples that provided indications about the person's health. But now some consultants are suggesting that those tests (which are expensive and time-consuming for companies to administer) should be replaced by information from social networks. Deloitte Consulting LLP reports that the predictive modeling approach could save insurance companies an estimated $2 to $3 million a year and can "shorten and reduce the invasiveness of the underwriting" process. Among the factors that have been delineated as possibly making a person ineligible for life insurance include the fact that the person is an avid reader, commutes to work, or has friends who are skydivers. A person may be denied life insurance because GPS places her at too many fast food places or because she has downloaded a diabetes-monitoring app.

Data aggregators' collection and use of mobile health information is an example of how paltry online privacy protections are in contrast to offline ones. Offline, personal health care information in the hands of doctors and hospitals is protected under the Health Insurance Portability and Accountability Act of 1996 (HIPAA). In addition, physical barriers in health care institutions prevent random strangers from looking at a person's records. But data aggregators can swoop up digital health care information without constraints. The promotional document for Nielsen's Pharma-Health data aggregation practice indicates that it collects individuals' digital data regarding "cancer, diabetes, mental illness, Multiple Sclerosis, high blood pressure, Alzheimer's, weight management, asthma, aging, ADD/ADHD, cholesterol, arthritis, allergies, over-the-counter treatments, HIV/AIDS, migraines, pain management and more."

Because health care privacy laws don't cover information from online searches or medical apps, it's up to individual companies to set their own guidelines. One marketing company, Healthline Networks, Inc., has adopted a policy that it will not use information about people's searches related to HIV, impotence, or eating disorders, but other companies have no such limits. And Healthline does use information about bipolar disorder, overactive bladder, and anxiety, which are arguably just as stigmatizing as those on its privacy-protected list.

What Policies Are Needed to Protect Privacy in the Mobile Market?

Sun Microsystems' Scott McNealy has said, "You have zero privacy anyway. Get over it." But people haven't gotten over it. People do care about privacy. A 2012 Pew Research Center study found that 57 percent of all mobile app users had either uninstalled or declined to install an app because they were concerned about sharing personal information. Fewer than one-third of respondents in a 2011 survey of US smartphone users felt in control of their personal information in mobile devices.

When people realize that data aggregators are collecting extensive information about them, many want legal change. A 2009 survey by Professor Joseph Turow and his colleagues at the University of Pennsylvania and the University of California, Berkeley, found that 68 percent of Americans opposed being "followed" on the web, and 70 percent of Americans supported the idea of requiring companies that collect or use someone's information without consent to pay hefty fines. Most people—92%—believe that websites and advertising companies should be required to delete all information stored about an individual if requested to do so. People's desires for privacy are also evidenced by the large number of complaints filed with the FTC alleging that the companies are engaged in "unfair or deceptive acts or practices" due to their deficient privacy standards. Over a four-year period from 2004 to 2008, the FTC received 1,230 complaints under the category "company does not provide any opportunity for consumer to opt out of information sharing;" 1,678 complaints that the "company fails to honor request to opt out/opt-out mechanism does not work;" and 534 complaints that the "company is violating its privacy policy." The agency also received 84 complaints that a "privacy policy is misleading, unclear, or difficult to understand;" 555 complaints that a "company does not have adequate security;" and 3,265 other complaints of privacy violations.

Certain legal trends suggest that the developers of mobile devices and mobile apps will ultimately be held more accountable. A California state law, the Online Privacy Protection Act, requires operators of websites and other online services to:

> identify the categories of personally identifiable information that the operator collects through the Web site or online service about individual consumers who use or visit its commercial Web site or online service and the categories of third-party persons or entities with whom the operator may share that personally identifiable information.

Under the law, the California Attorney General reached an agreement with six major mobile-device companies (Apple, Microsoft, Google, Amazon, Hewlett-Packard Co., and Research in Motion Limited), which agreed to disclose privacy policies on apps to individuals within the state of California.

The FTC has also pursued legal action against companies that did not meet proper mobile device privacy standards. Path, Inc. operates a social networking app that allows users to create and share journals with their networks of friends. Although Path made it appear that it would only collect personal information from a user's mobile device if the user agreed, the app collected users' address book information—including any available first and last names, addresses, phone numbers, email addresses, Facebook and Twitter user names, and dates of birth—without the user's consent. The app also obtained this data from the mobile address books of approximately 3,000 minors under the age of 13—with actual knowledge of their status as minors—without parental consent, in violation of the Children's Online Privacy Protection Act (COPPA).The FTC investigation resulted in a settlement agreement, which required Path to establish a comprehensive privacy program and to obtain independent privacy assessments each year for the next 20 years. Path was also required to pay $800,000 to settle charges that it illegally collected personal information from children without their parents' consent and was prohibited from making any future misrepresentations about the extent to which it maintains the privacy and confidentiality of consumers' personal information. Taking a more prospective approach, the FTC has recommended steps that mobile platforms can follow to take privacy seriously. (See Box.) In formulating policy, it is important to be cognizant of the financial, physical, and psychological harms that can result from mobile privacy breaches. It's also useful to think about what Samuel Warren and Louis Brandeis wrote back in 1890 in their classic *Harvard Law Review* article about technology and privacy. They wrote:

> The intensity and complexity of life attendant upon advancing civilization have rendered necessary some retreat from the world so that solitude and privacy have become more essential to the individual; but modern enterprise and invention have, through invasions upon his privacy, subjected him to mental pain and distress, far greater than could be inflicted by mere bodily injury. ◆

Lori Andrews is a professor at IIT Chicago-Kent College of Law and the author of I Know Who You Are and I Saw What You Did: Social Networks and the Death of Privacy *(Simon and Schuster, 2013). Lori can be reached at landrews@kentlaw.iit.edu.*