Cell Phone Companies Should not Use Confusing and Misleading Contracts

Imagine that somebody knows where you are at all times. How would you feel? Now, imagine that that person also keeps a record of your whereabouts for an unlimited amount of time. You'd probably feel rather uncomfortable, if not scared. Location data are sensitive, personal information that you may prefer to keep private. Unfortunately, this scenario is what is happening nowadays: if you possess and use a smart phone, you are at risk of being one of those individuals who is regularly followed day and night by the invisible eye of your phone company and any third parties that provide services you use on your phone. What is more troubling is that this is possible, for most part, because you consented to this practice, which is called geotracking, when you signed up for serviceóand it would be very hard for you to obtain the destruction of your data should you change your mind about your desire to be geotracked. Furthermore, the regulatory framework does not sufficiently protect users.[1] This is why we believe that, in the current regulatory and business climate, phone companies should have no right to keep data on a user's whereabouts.

Phone companies, location data, and privacy

Two types of company are primarily involved in tracking and storing location information through mobile devices. These are the company that provides data access (AT&T, Verizon, Sprint, T-Mobile, and Verizon) and the company that manufactures the operating system (the leaders in this industry are Apple (iOS) and Google (Android)). In addition to them, a multitude of third party companies offer applications that can be used on mobile devices and that can obtain your geographic location through downloaded applications (apps) or cookies from Web site visits.

All these companies have the capability of identifying your location. But, what are location data and why are they so important? Very simply, location data consist of information concerning the geographical location of a phone user. These data can be tracked by using any global positioning system (GPS) technology embedded in the phone or by beaming the unique hardware IDs of nearby Wi-Fi devices back to the phone company. The level of accuracy to acquire this information ranges from a few hundred feet or better with Wi-Fi to a few feet or better with GPS.

Location data can reveal very sensitive information about users. Location can reveal information about our medical status, our racial or ethnic origins, political or religious beliefs, or sexuality. Because of the sensitive nature of these data, we are often concerned with keeping them private. We care for secrecy not because we want to do something that is against the law or because we are ashamed of where we are; we care because we want to have control over our lives and over what people know about our whereabouts.

This is, however, not always possible. In fact, there is no expectation of privacy when we stand in public places where anybody can see us. Law enforcement authorities routinely requests access to this information, and obtain access.[2] In 2012, Peter Maass reported from the columns of the *New York Times* that "cell phone carriers responded 1.3 million times last year [in 2011] to law enforcement requests for call data."[3] Although courts have thus far been cautious, location data could also become public through discovery in civil litigation.[4]

However, we move in public space with the expectation that under normal circumstances their location will not be systematically and secretly recorded for later use. Andrew Blumberg and Peter Eckersley refer to this expectation as "localization privacy."[5] This form of privacy may be particularly important when we exercise our political rights.

Yet, geotracking may result in a curtailment of some of our freedoms. In 2012, the U.S. Patent and Trademark Office granted a patent application, to be assigned to Apple, of a technology that enables the maker of the iPhone to deactivate certain functions of our mobile phones depending on our locations.[6] While this may be useful under certain circumstancesówe would like for all phones to be turned off when we watch a movie at a movie theateróour phones could be blocked out if we tried to "take a photo of the police officer beating a man in the street because your oppressive government."[7] The fact that a phone company knows where we are at all times constitutes a new and unprecedented threat to our ability to control our lives.

The problem with privacy policies and "consent"

One of the problems with geotracking data is phone companies' policies. When you sign up for phone service or agree to the terms of use of an operating system or an application, you usually consent to some collection of personal information. In theory, this is not problematic because you, as a free and autonomous person, express your approval of the use of these data and accept the "inconvenience" of being tracked. Indeed, you can certainly gain some benefits from location data tracking: you can turn your mobile devices into GPS navigation systems, find nearby restaurants or gas stations, enjoy improved, personalized services based on location data, and even find your phone if it is ever lost or stolen. These policies however present several problems: they are purposely unclear; do not offer much choice at the time a user signs up for service; make it very difficult for a user to opt out; and often permit the sharing of geotracking data with third party companies.

First, agreements are drafted in a way such that it is very hard to understand to what exactly you consent and how to stop being tracked in the event you change your mind. Policies are purposely vague and convoluted to limit our understanding of what we agree to. How can we properly consent if the document that contains the terms of the agreement does not allow us to fully understand the implications of our choice? For instance, there is no definition of what actually constitutes "consent." AT&T takes great liberty with this: "The form of consent will be suited to the type of AT&T (location-based service) you utilize."[8] A user could theoretically show consent just by purchasing the phone or turning it on. Consent could even be the "default" setting on a new phone and may not require active participation at all. Sprint: "Our networks generally know the location of your Device when it is outdoors and/or turned on."[9] A litany of other exceptions are brilliantly hidden and disguised in their own respective User Agreements and Privacy Policies that make your decision moot. An example of this deceptive wording is best illustrated through an example used by Google in defining the type of information they collect: " . . . an IP address can often be used to identify the country from which a computer is connected to the internet."[10] This statement appears innocuous and although it is true that an IP address can identify the user's country, it fails to mention that each IP address is unique and can be used to determine a specific device. Often times the term "may" is present seemingly hundreds of times in each legal document. It allows companies to say that they can do something, without specifically stating that they are going to. From Verizon: "This type of information may be aggregated or anonymized for business and marketing uses by us or by third parties."[11] Now from AT&T: "...These data services (referred to as Location-Based ServicesÖ) are made available by AT&T and other companies via applications that may be pre-loaded."[12]

Second, not much choice is offered: if you want to use certain services, you must accept the term of use. You cannot negotiate them. Furthermore, "all or nothing" is all that is offered: you are frequently asked to consent to the tracking of all location data and only rarely are you offered a menu of options that allow you to craft data collection based on your preferences.

Third, even if you take the required steps to officially opt-out of services, any Web site or downloaded material retains the right to track the user's device. In April 2011, it was discovered that not only were both Apple and Google tracking users without their consent, they were tracking them even after the users opted out and the practice actively breached their own privacy policies.[13] To remove oneself from a location based service essentially requires a degree in computer engineering just to opt-out, not to mention the willpower required to forfeit the use of downloaded

apps and services forever. Since modern phones can access the Internet, nearly any action by the user, from checking the weather to visiting a Web site and checking the score of the big game, can result in cookies being uploaded. Location capabilities can even be turned on remotely when the battery is dead. The only way to ensure you are "off the grid" is to remove the battery. Opting out is practically impossible.

Fourth, these agreements contain an infinite number of exceptions, the most prominent of which is exempting any third party entity that does business with the phone companies from abiding by the user agreement, as discussed further below. Google adopted the following policy: "Our Privacy Policy does not apply to . . . sites that may include Google services."[14] Further, "Our Privacy Policy applies to all of the services offered by Google Inc. and its affiliates... but excludes services that have separate privacy policies that do not incorporate this Privacy Policy."[15] Similar third party exception clauses are endemic to the industry. Ultimately this leaves the door open to an infinite number of advertisers to attach tracking devices and cookies as they please. An excerpt from Verizon's Privacy Policy is typical for cell phone companies: "By enabling location settings you are permitting third party access to Location Information through software, widgets or peripheral components you choose to download, add or attach to your wireless device."[16]

The problem of dual use of data

A second major problem with phone companies' right to keep geotracking data is the dual use of data. On one hand, data are collected to deliver certain services that require location tracking and to improve service user experience. On the other hand, these data have a commercial value and are often shared with other business for a profit. This information is very valuable to advertisement companies, as it allows them to finely targeting consumer audiences when marketing a product. Search engines, email, or free games are there for a reason ñ to get you there to view advertisements and to keep you coming back. When you continue to return to the service, the website gets more hits and you now become a "user" that views an advertisement and provides personal information as payment for the costs to develop and provide the product. If you add to the mix tracking your location, the value of these data increases significantly. Here are some data to support this statement. Google, which manufactures the Android system, reported 96% of their revenue from advertisers in 2011, equating to $36 billion.[17] Moreover, the expense associated with mobile ads shows no signs of slowing down and is forecast to double every year to $20.6 billion in 2015.[18]

The ability to collect location data has indeed revolutionized the market. Before the prevalence of location technology in phones, companies had only been able to target advertisements based on your search history or email content. Now they can take into account where you live and like to hang out. No wonder they invest millions of dollars in a supposed "free" service because they are gaining that final piece of the puzzle to establishing an online identity. Since significant profits can be reaped, location data collection (and user data in general) has become a top priority. Take an excerpt from Verizon's policy: "Through web access, messaging capabilities or other means and you are authorizing Verizon Wireless to collect, use and disclose your Location Information."[19] This is the reason that cell phone companies must camouflage their actions in complex legal jargon that ensures their right to your personal data.

The way forward

Cell phones are devices that enable us to be connected with people and have access to various kinds of services on a regular basis in our daily lives. This technology has permanently shifted the way in which we live, work, and socialize. Yet, we also need to understand the limitations of this technology, and in particular become aware of the risk associated with the loss and consequential commercialization of our privacy. We often sign up for new services too often and too easily without reflecting on the consequences of our action. Indeed, phone companies often hide or minimize the loss of our privacy in the obscurity of terms of agreement that we accept. Despite societal contributions, we advocate for limiting the power of these corporate giants. Regulations constraining those who

create software and provide a service to us on a daily basis can and should be instituted by policy makers on Capitol Hill. Proper governmental policies must ensure not only accountability on behalf of the corporations but also must clearly state measures of evaluation that can be enforced. The privacy policies and user agreements that have been described take advantage of poorly written laws for the reason that they operate in a vacuum formed between policy that is too broad and too narrow. When too broad, policies allow for the mercurial wording of legal policies that make it impossible to prove they are doing anything wrong. Policy makers may not be able to control how a billion-dollar company operates internationally, but they can ensure that its citizens are protected and retain their right to control personal data shared for profit. We advocate for seeking a proper balance so that the playing field in which consumers and phone companies interact will become level.

The most pressing policy issue is to close the third party loophole. Companies that collecte data must guarantee to users that any third company with which location data are shared is bound by the terms of agreement between the user and the phone company. There should be no exemptions to allow a company to know your whereabouts. This policy could apply to every company, software, or technology that intends to track you and collect personal data. Users are only truly free if information concerning how their own information is shared is made available.

Second, phone companies should be prohibited from tracking location data after the user opts out, when users are not using an application or feature that must make use of location data to function properly, and needless to say when the phone are off. Opportunities for opting out fully should be made available. An individual should have the choice to decide who tracks them and who does not.

Enforceability is certainly problematic issue, especially when it comes to the international transmission of data. Currently, companies store some location data on servers that are located outside the United States. This adds another layer of vulnerability, considering that foreign governments could access data revealing the whereabouts of Americans. These problems do not have easy solutions, and they certainly highlight the need for phone users to be fully aware of the implications of using these powerful devices. On the other hand, phone companies must certainly do their part and fulfill their duties towards users because we cannot simply rely on governments to protect our privacy.

Works Cited

[1] Briana Schwandt, "Is the Government in My Pocket? An Overview of Government Location Tracking of Cell Phones under the Federal System and in Montana," *Montana Law Review* no. 72 (2011): 261-337.
[2] Peter Maas, "That's No Phone. That's My Tracker," *New York Times* (July 15, 2012) http://www.nytimes.com/2012/07/15/sunday-review/thats-not-my-phone-its-my-tracker.html.
[3] Eric Lichtblau, "Wireless Firms Are Flooded by Requests to Aid Surveillance," *New York Times*, (July 8, 2012) http://www.nytimes.com/2012/07/09/us/cell-carriers-see-uptick-in-requests-to-aid-surveillance.html?_r=2&ref=surveillanceofcitizensbygovernment.
[4] David K. Isom, "Location-Based Electronic Discovery in Criminal and Civil LitigationóPart 2," *Utah Bar Journal* no. 24 (2011) http://webster.utahbar.org/barjournal/2011/11/locationbased_electronic_disco.html.
[5] Andrew J. Blumberg and Peter Eckersley, *On Locational Privacy, and How to Avoid Losing it Forever*, (San Francisco CA: Electronic Frontier Foundation, 2011).
[6] Michael Bell and Vitali Lovich, "Apparatus and Methods for Enforcement of Policies upon a Wireless Device," U.S. Patent 8,254,902, filed June 26, 2008, and issued August 28, 2012.
[7] Zacharis Whttaker, "Apple Patent Could Remotely Disable Protesters' Phone Cameras," ZDNet, (September 4,

2012). http://www.zdnet.com/apple-patent-could-remotely-disable-protesters-phone-cameras-7000003640/.
[8] AT&T, *AT&T Privacy Policy*, (2012) http://www.att.com/Common/about_us/privacy_policy/print_policy.html.
[9] Sprint, *Terms and Conditions 2012* (2012)http://shop2.sprint.com/en/legal/legal_terms_privacy_popup.shtml?ECID=vanity:termsandconditions/.
[10] Google, *Key terms 2012b* (2012) http://www.google.com/policies/privacy/key-terms/.
[11] Verizon, *Privacy Policy Summary* (September 2011) from https://www22.verizon.com/about/privacy/.
[12] AT&T, *AT&T Privacy Policy* (2011) http://www.att.com/Common/about_us/privacy_policy/print_policy.html.
[13] Julia Angwin and Jennifer Valentino-Devries, "Apple, Google Collect User Data," *Wall Street Journal* (April 21 2011).
[14] Google, *Privacy Policy, July 27 2012c* (2012) [http://www.google.com/policies/privacy/.
[15] Ibid.
[16] VerizonWireless, *Wireless Location Based Services 2012* (2012) http://support.verizonwireless.com/clc/faqs/Wireless%20Issues/wireless_location_based_services.html?grp=1&faq=1.
[17] Google, *Financial Tables 2012a* (2012) http://investor.google.com/financial/tables.html.
[18] Gartner, "Gartner Says Worldwide Mobile Advertising Revenue Forecast to Reach $3.3 Billion in 2011," Press Release (June 16 2011) http://www.gartner.com/it/page.jsp?id=1726614.
[19] Verizon Wireless, *Wireless Location Based Services 2012*, http://support.verizonwireless.com/faqs/Wireless%20Issues/wireless_location_based_services.html.

About the Author

Joseph H. Robertson
Joseph H. Robertson graduated Summa Cum Laude from Bryant University with a B.A in politics and law and from The Maxwell School of Citizenship and Public Affairs in Syracuse, NY, with a dual masters degree in public administration and international relations.

Mr. Robertson also received a Certificate of Advanced Study in security studies. He is studying Russian language and culture in Irkutsk, Siberia. His interests are U.S. domestic policy, international policy, and diplomacy.

Andrea Boggio
Andrea Boggio is an associate professor of legal studies at Bryant University.

He earned a doctoral degree in legal studiesfrom Stanford University and completed his post-doctoral training at the University of Geneva. He taught at the Centre for Professional Ethics at Keele University in England before coming to Bryant. He is the author of *Compensating Asbestos Victims, Law and the Dark Side of Industrialization* (Ashgate 2013) and the co-editor of *Health and Development: Toward a Matrix Approach* (Palgrave-MacMillan, 2009).

Select Citation Style: MLA

MLA

Robertson, Joseph and Andrea Boggio. "Cell Phone Companies Should not Use Confusing and Misleading Contracts." *Issues: Understanding Controversy and Society*. ABC-CLIO, 2013. Web. 4 Feb. 2013.

back to top **Entry ID: 1766997**