

3Qs: Mobile tracking in criminal investigations

April 16 2012, By Lauren Dibble



Credit: AI-generated image (disclaimer)

Last week, the American Civil Liberties Union released a new report revealing that law-enforcement agencies frequently use cell-phone tracking data provided by wireless carriers — often without a warrant. Northeastern University news office asked Sharon Fray-Witzer, a lecturer in the School of Criminology and Criminal Justice and a



practicing criminal defense attorney, to analyze the use of wireless tracking data in criminal investigations and whether it infringes on users' privacy.

Is using cell-phone data for tracking purposes a violation of privacy? Does it violate any constitutional requirements?

The short answer is: We don't know. The Supreme Court hasn't decided yet, though police are clearly doing it all the time. The basic test of what violates the Fourth Amendment is whether the government action is "unreasonable" search and seizure. The Supreme Court has just decided, in the United States v. Jones case, that it's unreasonable for police to attach a GPS tracker to someone's car in order to remotely monitor that car's movements full time for a month, without first getting a warrant.

But the majority opinion in the Jones case seemed to be tied closely to the concept of "trespass." The court thought it was unreasonable to attach a GPS monitor to the car without a warrant because the act interfered with a property right. Many commentators noticed that that reasoning left open the question of whether it would violate the Fourth Amendment simply to get signals coming from someone's <u>cell phone</u>, without attaching anything to their cell phone. If someone is already carrying something around, and they know full well that it is giving off signals about where they are, how can it be a trespass simply to collect those signals? Though the Court also thought the monitoring in Jones went on too long, the government will make the no-trespass argument about cell phones, and that is an argument that the <u>American Civil</u> <u>Liberties Union</u> is very concerned about.

This is part of a much bigger reality about our modern rights of privacy. The biggest threats to our privacy nowadays are probably those we create for ourselves, by giving out information to make our lives easier. Through the use of credit cards, email and mobile devices, we allow



many private entities to collect all kinds of information about us, and, where it isn't protected by some statute, those entities can sell that information to anyone willing to pay for it. The Constitution can't protect us very well against giving our information away.

What obligation do service providers have to give tracking data to law-enforcement agencies, particularly when no warrant has been obtained?

The government can get a warrant by showing a court that it has probable cause to believe that a certain service provider has evidence of a crime; then the service provider must turn over the information described in the warrant. The government can also subpoena data in certain investigations, or get court orders to turn it over. A <u>service</u> <u>provider</u> is not otherwise required to turn over tracking information to the government. But it may be willing to sell that information, if the price is right, and if it thinks that its customers won't care, or won't notice.

How has the pervasiveness of digital content and growing digital footprints influenced law-enforcement practices? In general, does it complicate or aid criminal investigations?

It complicates work, but also aids investigations. It has changed law enforcement dramatically. Though I work in criminal defense rather than law enforcement, I know that, in addition to GPS tracking (which can be performed by police with a warrant), the government is likely to collect all the electronic information it can get in order to help prove its case: cell-phone data, hard drives, emails, credit card, bank transactions, etc. Digital-evidence collection has vastly increased the amount of data that must be processed, and it requires entirely new kinds of expertise. The courts are still sorting out just how far police can go in looking



through someone's hard drive if they have probable cause to believe that they'll find incriminating <u>information</u>.

Provided by Northeastern University

Citation: 3Qs: Mobile tracking in criminal investigations (2012, April 16) retrieved 26 April 2024 from <u>https://phys.org/news/2012-04-3qs-mobile-tracking-criminal.html</u>

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.