Documents show cops making up the rules on mobile surveillance

By Timothy B. Lee
April 3, 2012

Documents newly obtained by the ACLU reveal the extent of surveillance conducted by state and local law enforcement agencies with the assistance of cell phone companies. Most notably, they show that location-based tracking has become ubiquitous, with cell phone companies offering "tower dumps" of everyone who used a particular cell phone tower during a particular time period. At least one police department, worried about public backlash if the extent of such tracking became widely known, has barred officers from disclosing the use of such tracking capabilities to the media.

The documents were revealed by an ambitious ACLU project to use open-records laws to obtain a deeper understanding of police department practices with regard to cell phone surveillance around the country. ACLU affiliates submitted information requests to dozens of law enforcement agencies; while many refused to provide documents, the ACLU was able to assemble more than 5,500 pages of documents from numerous state and local agencies.

The documents paint a picture of a surveillance free-for-all. While departments seem to have avoided warrantless access to phone calls themselves—which would likely run afoul of wiretapping laws—police departments have sought access to a wide variety of other user information.

The legal standards used for cell phone tracking requests vary widely by police department. Some law enforcement agencies do not track cell phones, or have concluded that the Fourth Amendment requires them to obtain a warrant in order to track user locations. But many more reported obtaining location information with a simple subpeona—which is available without meeting the Fourth Amendment's "probable cause" standard. The ACLU says that "a number of law enforcement agencies report relying on cell phone providers to tell them what legal process is necessary to obtain location records."

A New York Times report on the documents says that many departments keep their use of cell phone tracking capabilities secret, fearing the backlash that could be generated if the public learned how often they are used. For example, a document published by the Iowa City police department admonishes police officers not to "mention to the public or media the use of cell phone technology or equipment used to locate the targeted subject." Officers are advised not to include "details of the methods and equipment used to locate the subject" in police reports.

A full menu

The documents also suggest that selling customer information to law enforcement has become a significant revenue source for cell phone companies. A particularly illuminating cache of documents comes from the Tucson, AZ, police department. It catalogs how much various wireless companies charge for a wide variety of surveillance services.

Telecom carriers have long been required to assist the government with surveillance efforts, and they have been permitted to charge for providing information. But as network providers have offered their users a growing menu of services, the menu of surveillance capabilities offered to law enforcement has grown accordingly.

For example, a July 2009 price list indicates that Sprint charged $120 per target number for "Pictures and Video," $60 for "E-Mail," $60 for "Voicemail," and $30 for "SMS Content." Verizon Wireless charged $50 for "picture content." Verizon Wireless could not "preserve voicemail, but can reset pass code to give access to law enforcement," according to the documents. Resetting a user's voicemail password cost $50. AT&T charged $150 for voicemail, but did not offer "SMS Content" or "Picture Content."

Probably the most troubling service offered by wireless companies are "tower dumps." Law enforcement agencies ask for a download of "all activities" on a particular tower. As of 2009, Alltel, AT&T, Verizon, T-Mobile, and Sprint all offered "tower dump" services, with prices ranging from $50 to $500 per tower. Only one carrier—Cricket—was refusing to provide such information in 2009.

Cato Institute privacy researcher (and *Ars Technica* alum) Julian Sanchez wrote on Monday that, until he read these documents, he had been aware of only one instance in which "tower dumps" had been used in an investigation. But the fact that all the major wireless companies have standard list prices for the service suggests that it has become a relatively routine investigative technique.

It's not clear if the "activity" disclosed in a "tower dump" is limited to phone calls placed through that tower or whether it includes all phones that merely came within range of the tower during the requested time period. Either way, the practice raises serious constitutional issues.

Sanchez writes that the use of "tower dumps" is "in serious tension with our constitutional tradition of 'particularity' in searches. If it were to be permitted under *any* circumstances, it would require extraordinary safeguards, ideally established by a clear legislative framework—not a patchwork of agencies making up the rules as they go."

Unfortunately, a "patchwork of agencies making up the rules" is what we're stuck with for now.