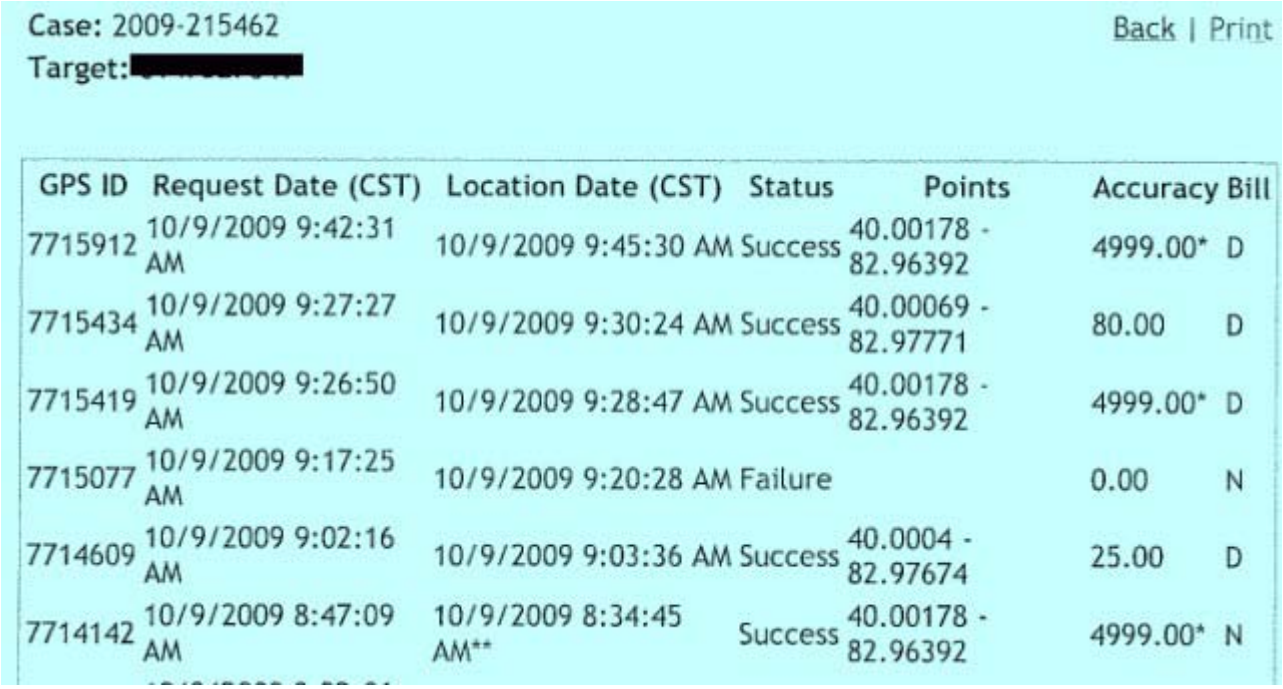
Feds ‘Pinged’ Sprint GPS Data 8 Million Times Over a Year

- Categories: Surveillance



Case: 2009-215462 Back | Print
Target: [redacted]

GPS ID	Request Date (CST)	Location Date (CST)	Status	Points	Accuracy	Bill
7715912	10/9/2009 9:42:31 AM	10/9/2009 9:45:30 AM	Success	40.00178 - 82.96392	4999.00*	D
7715434	10/9/2009 9:27:27 AM	10/9/2009 9:30:24 AM	Success	40.00069 - 82.97771	80.00	D
7715419	10/9/2009 9:26:50 AM	10/9/2009 9:28:47 AM	Success	40.00178 - 82.96392	4999.00*	D
7715077	10/9/2009 9:17:25 AM	10/9/2009 9:20:28 AM	Failure		0.00	N
7714609	10/9/2009 9:02:16 AM	10/9/2009 9:03:36 AM	Success	40.0004 - 82.97674	25.00	D
7714142	10/9/2009 8:47:09 AM	10/9/2009 8:34:45 AM**	Success	40.00178 - 82.96392	4999.00*	N

Sprint Nextel provided law enforcement agencies with customer location data more than 8 million times between September 2008 and October 2009, according to a company manager who disclosed the statistic at a non-public interception and wiretapping conference in October.

The manager also revealed the existence of a previously undisclosed web portal that Sprint provides law enforcement to conduct automated “pings” to track users. Through the website, authorized agents can type in a mobile phone number and obtain global positioning system (GPS) coordinates of the phone.

The revelations, uncovered by blogger and privacy activist Christopher Soghoian, have spawned questions about the number of Sprint customers who have been under surveillance, as well as the legal process agents followed to obtain such data.

But a Sprint Nextel spokesman said that Soghoian, who recorded the Sprint manager’s statements at the closed conference, misunderstood what the figure represents. The number of customers whose GPS data was provided to local, state and federal law enforcement agencies was much less than 8 million, as was the total number of individual requests for data.

The spokesman wouldn’t disclose how many of Sprint’s 48 million customers had their GPS data shared, or indicate the number of unique surveillance requests from law enforcement. But he said that a single surveillance order against a lone target could generate thousands of GPS “pings” to the cell phone, as the police track the subject’s movements over the course of

days or weeks. That, Sprint claims, is the source of the 8 million figure: it's the cumulative number of times Sprint cell phones covertly reported their location to law enforcement over the year.

The spokesman also said that law enforcement agents have to obtain a court order for the data, except in special emergency circumstances.

The information about the data requests and portal comes from Paul Taylor, manager of Sprint's Electronic Surveillance Team. He made the revelations at the Intelligent Support Systems (ISS) conference, a surveillance industry gathering for law enforcement and intelligence agencies and the companies that provide them with the technologies and capabilities to conduct surveillance.

The conference is closed to press, but Soghoian, who is a graduate student at Indiana University, obtained entry and recorded a couple of panel sessions, which he posted on his blog (see below). In one of the recordings, Taylor is heard saying that the automated web system was rolled out a year ago and that in 13 months it had processed more than 8 million requests for GPS data from law enforcement.

"We turned it on the web interface for law enforcement about one year ago last month, and we just passed 8 million requests," Taylor is heard saying. "So there is no way on earth my team could have handled 8 million requests from law enforcement, just for GPS alone. So the tool has just really caught on fire with law enforcement. They also love that it is extremely inexpensive to operate and easy."

Soghoian concluded on his blog that the quote provided proof that "location requests easily outnumber wiretaps, and … likely outnumber all other forms of surveillance request too."

He cites a telecom attorney named Al Gidari who claimed at a talk last year that each of the major wireless carriers received about 100 requests a week for customer-location data. At 100 requests a week for each of the top four wireless carriers, the total should be around 20,000 requests a year.

"I now have proof that he significantly underestimated the number of requests by several orders of magnitude," Soghoian writes.

But Sprint spokesman John Taylor (who is not related to Paul Taylor) says Soghoian had "grossly misrepresented" the 8 million figure, which doesn't refer to unique requests or to individual customers, but to the total number of "pings" made on every number for the duration of a law enforcement request.

"The figure represents the number of individual pings for specific location information, made to the Sprint network as part of a series of law enforcement investigations and public safety assistance requests during the past year," said spokesman Taylor. "It's critical to note that a single case or investigation may generate thousands of individual pings to the network as the law enforcement or public safety agency attempts to track or locate an individual."

There are four circumstances under which law enforcement agents can use the Sprint website and obtain GPS data: 1) under the authority of a court order; 2) to track the location of a

customer who has made a 911 call; 3) in an emergency situation, such as tracking someone lost in the wilderness or trying to locate an abducted child or hostage; 4) with a customer's consent.

In the case of court orders, Taylor said agents are required to provide Sprint with the order, after which the company provisions the law enforcement account to allow an agency to track the targeted phone number. Court orders cover a 60-day period, and agents can do automated pings to obtain real-time GPS data every three minutes throughout that 60-day period. Taylor says this accounts for the 8 million figure.

"If you can access the info every three minutes over 60 days, that adds up pretty quickly," he told Threat Level.

He added that the GPS data includes only latitude and longitude and the date and time of the ping.

The automated system was set up so that law enforcement agents wouldn't have to contact Sprint's electronic surveillance team each time they wanted to ping a phone number throughout the 60 days of a court order. Agents still have to obtain a subpoena to get historic call detail records, such as phone numbers called, the date, time and duration of calls and the cell site and sector from which the calls were made