ELECTRONIC FRONTIER FOUNDATION

December 1st, 2009

Surveillance Shocker: Sprint Received 8 MILLION Law Enforcement Requests for GPS Location Data in the Past Year

News Update by *Kevin Bankston*

This October, Chris Soghoian — computer security researcher, oft-times journalist, and current technical consultant for the FTC's privacy protection office — attended a closed-door conference called "ISS World". ISS World — the "ISS" is for "Intelligence Support Systems for Lawful Interception, Criminal Investigations and Intelligence Gathering" — is where law enforcement and intelligence agencies consult with telco representatives and surveillance equipment manufacturers about the state of electronic surveillance technology and practice. Armed with a tape recorder, Soghoian went to the conference looking for information about the scope of the government's surveillance practices in the US. What Soghoian uncovered, as he reported on his blog this morning, is more shocking and frightening than anyone could have ever expected

At the ISS conference, Soghoian taped astonishing comments by Paul Taylor, Sprint/Nextel's Manager of Electronic Surveillance. In complaining about the volume of requests that Sprint receives from law enforcement, Taylor noted a shocking number of requests that Sprint had received in the past year for precise GPS (Global Positioning System) location data revealing the location and movements of Sprint's customers. That number?

EIGHT MILLION.

Sprint received over 8 million requests for its customers' information in the past 13 months. That doesn't count requests for basic identification and billing information, or wiretapping requests, or requests to monitor who is calling who, or even requests for less-precise location data based on which cell phone towers a cell phone was in contact with. That's *just GPS*. And, that's not including legal requests from civil litigants, or from foreign intelligence investigators. That's *just law enforcement*. And, that's not counting the few other major cell phone carriers like AT&T, Verizon and T-Mobile. That's *just Sprint*.

Here's what Taylor had to say; the audio clip is here and we are also mirroring a zip file from Soghoian containing other related mp3 recordings and documents.

> *[M]y major concern is the volume of requests. We have a lot of things that are automated but that's just scratching the surface. One of the things, like with our GPS tool. We turned it on the web interface for law enforcement about one year ago last month, and we just passed 8 million requests. 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, so, just the sheer volume of requests they anticipate us automating other features, and I just don't know how we'll handle the millions and millions of requests that are going to come in.*

Eight million would have been a shocking number even if it had included every single legal request to every single carrier for every single type of customer information; that Sprint alone received eight million requests just from law enforcement only for GPS data is absolutely mind-boggling. We have long warned that cell phone tracking poses a threat to locational privacy, and EFF has been fighting in the courts for years to ensure that the government only tracks a cell phone's location when it has a search warrant based on probable cause. EFF has also complained before that a dangerous level of secrecy surrounds law enforcement's communications surveillance practices like a dense fog, and that without stronger laws requiring detailed reporting about how the government is using its surveillance powers, the lack of accountability when it comes to the government's access to information through third-party phone and Internet service providers will necessarily breed abuse. But we never expected such huge numbers to be lurking in that fog.

Now that the fact is out that law enforcement is rooting through such vast amounts of location data, it raises profoundly important questions that law enforcement and the telcos must answer:

- How many innocent Americans have had their cell phone data handed over to law enforcement?
- How can the government justify obtaining so much information on so many people, and how can the telcos justify handing it over?
- How did the number get so large? Is the government doing massive dragnet sweeps to identify every single cell phone that was in a particular area at a particular time? Is the government getting location information for entire "communities of interest" by asking not only for their target's location, but also for the location of every person who talked to the target, and every person who talked to them?
- Does the number only include requests to track phones in real-time, or does it include requests for historical GPS data, and if so, why did the telcos have that incredibly sensitive data sitting around in the first place? Exactly when and how are they logging their users' GPS data, and how long are they keeping that data?
- What legal process was used to obtain this information? Search warrants? Other court orders? Mere subpoenas issued by prosecutors without any court involvement? How many times was this information handed over without any legal process at all, based on government claims of an urgent emergency situation?
- Looking beyond Sprint and GPS, how many Americans have had their private communications data handed over to law enforcement by their phone and Internet service providers?
- What exactly has the government done with all of that information? Is it all sitting in an FBI database somewhere?
- Do you really think that this Orwellian level of surveillance is consistent with a free society and American values? *Really*?

These questions urgently need to be asked — by journalists, and civil liberties groups like EFF, and by every cell phone user and citizen concerned about privacy. Most importantly, though, they must be asked by Congress, which has failed in its duty to provide oversight and accountability when it comes to law enforcement surveillance. Congress should hold hearings as soon as possible to demand answers from the government and the telcos under oath, and clear the fog so that the American people will finally have an accurate picture of just how far the government has reached into the private particulars of their digital lives.

Even without hearings, though, the need for Congress to update the law is clear. At the very least, Congress absolutely must stem the government's abuse of its power by:

- Requiring detailed reporting about law enforcement's access to communications data using the Electronic Communications Privacy Act (ECPA), just as it already requires for law enforcement wiretapping under the Wiretap Act, and make sure that the government actually fulfills its

obligations rather than ignore the law for years on end.

- Requiring that the government "minimize" the communications data it collects under ECPA rather than keep it all forever, just like it is supposed to do with wiretaps.
- Prohibiting the government from using in a criminal trial any electronic communications content or data that it obtains in violation of ECPA, just as the government is prohibited by the Wiretap Act from using illegally acquired telephone intercepts.
- Clarifying that ECPA can only be used to get specific data about particular individuals and cannot be used for broad sweeps, whether to identify everyone in a particular geographic area or to identify every person that visits a particular web site.

It's time for Congress to pull the curtain back on the vast, shadowy world of law enforcement surveillance and shine a light on these abuses. In the meantime, we give our thanks to those like Chris Soghoian who are doing important work to uncover the truth about government spying in America.

UPDATE: Sprint has responded to Soghoian's report:

> *The comments made by a Sprint corporate security officer during a recent conference have been taken out of context by this blogger. Specifically, the "8 million" figure, which the blogger highlights in his email and blog post, has been grossly misrepresented. The figure does not represent the number of customers whose location information was provided to law enforcement, as this blogger suggests.*
>
> *Instead, 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. 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.*
>
> *Instances where law enforcement agencies seek customer location information include exigent or emergency circumstances such as Amber Alert events, criminal investigations, or cases where a Sprint customer consents to sharing location information.*
>
> *Sprint takes our customers' privacy extremely seriously and all law enforcement and public safety requests for customer location information are processed in accordance with applicable state and federal laws.*

This response provides some important answers, while raising even more questions. First off, Sprint has confirmed that it received 8 million requests, while denying a charge that no one has made: that 8 million individual customers' data was handed over. Sprint's denial also begs the question: how many individual customers *have* been affected?

As for Sprint's claim that in some instances a single case or investigation may generate thousands of location "pings", that is certainly possible, but that doesn't make the 8 million number any less of a concern, or moot any of the important questions raised by Soghoian in his report or by EFF in its post regarding the lack of effective oversight and transparency in this area.

Even assuming that Sprint's statement about "pings" is true, 8 million — or, in other words, 8,000 thousands — is still an astronomical number and more than enough to raise serious concerns that Congress should investigate and address. Moreover, the statement raises additional questions: exactly what legal process is being used to authorize the multiple-ping surveillance over time that Sprint is cooperating in? Is Sprint demanding search warrants in those cases? How secure is this automated interface that law

enforcement is using to "ping" for GPS data? How does Sprint insure that only law enforcement has access to that data, and only when they have appropriate legal process? How many times has Sprint disclosed information in "exigent or emergency circumstances" without any legal process at all? And most worrisome and intriguing: what customers does Sprint think have "consent[ed] to the sharing [of] location data" with the government? Does Sprint think it is free to hand over the information of anyone who has turned on their GPS functionality and shared information with Sprint for location-based services? Or even the data of anyone who has agreed to their terms of service? What *exactly* are they talking about?

These questions are only the beginning, and Sprint's statement doesn't come close to answering all of them. Of course, we appreciate that Sprint has begun a public dialogue about this issue. But this should be only the beginning of that discussion, not the end. Ultimately, the need for Congress to investigate the true scope of law enforcement's communications surveillance practices remains. Congress can and should dig deeper to get the hard facts for the American people, rather than forcing us to rely solely on Sprint's public relations office for information on these critical privacy issues.

Related Issues: Cell Tracking, Locational Privacy

[Permalink: http://www.eff.org/deeplinks/2009/12/surveillance-shocker-sprint-received-8-million-law]

Want to learn how you can defend free speech, stand up for privacy, fight for government transparency, support consumer rights, and protect your right to innovation in the digital world? Visit **http://eff.org/fight** to find ways to help.