

slight paranoia

Security and privacy analysis by Christopher Soghoian

TUESDAY, DECEMBER 01, 2009

➔ 8 Million Reasons for Real Surveillance Oversight

Disclaimer: The information presented here has been gathered and analyzed in my capacity as a [graduate student](#) at Indiana University. This data was gathered and analyzed on my own time, without using federal government resources. This data, and the analysis I draw from it will be a major component of my PhD dissertation, and as such, I am releasing it in order to receive constructive criticism on my theories from other experts in the field. The opinions I express in my analysis are my own, and do not reflect the views of the Federal Trade Commission, any individual Commissioner, or any other individual or organization with which I am affiliated.

UPDATE 12/3/2009 @ 12:20PM: I received a phone call from an executive at TeleStrategies, the firm who organized the ISS World conference. He claimed that my recordings violated copyright law, and asked that I remove the mp3 recordings of the two panel sessions, as well as the YouTube/Vimeo/Ikbis versions I had embedded onto this blog. While I believe that my recording and posting of the audio was lawful, as a good faith gesture, I have taken down the mp3s and the .zip file from my web hosting account, and removed the files from Vimeo/YouTube/Ikbis.

Executive Summary

Sprint Nextel provided law enforcement agencies with its customers' (GPS) location information over 8 million times between September 2008 and October 2009. This massive disclosure of sensitive customer information was made possible due to the roll-out by Sprint of a new, special web portal for law enforcement officers.

The evidence documenting this surveillance program comes in the form of an audio recording of Sprint's Manager of Electronic Surveillance, who described it during a panel discussion at a [wiretapping and interception industry conference](#), held in Washington DC in October of 2009.

It is unclear if Federal law enforcement agencies' extensive collection of geolocation data should have been disclosed to Congress pursuant to a [1999 law](#) that requires the publication of certain surveillance statistics – since the Department of Justice simply [ignores the law](#), and has not provided the legally mandated reports to Congress since 2004.

Introduction

"[Service providers] have, last time I looked, no line entry in any government directory; they are not an agent of any law enforcement agency; they do not work for or report to the FBI; and yet, you would never know that by the way law enforcement orders them around and expects blind obedience."
– Albert Gidari Jr., Keynote Address: [Companies Caught in the Middle](#), 41 U.S.F. L. Rev. 535, Spring 2007.

"The reason we keep [search engine data] for any length of time is one, we actually need it to make our algorithms better, but more importantly, there is a legitimate case of the government, or particularly the police function or so forth, wanting, with a Federal subpoena and so forth being able to get access to that information."
– Eric Schmidt, CEO of Google, [All Things Considered](#), NPR interview between 5:40 and 6:40, October 2, 2009.

Internet service providers and telecommunications companies play a

Note: The opinions expressed on this blog are my own. The author is not a lawyer, and nothing written here should be taken as legal advice.

Subscribe To This Blog (RSS)

 [Subscribe in a reader](#)

Links

➔ [My home page \(with research papers\)](#)

Blog Archive

- ▶ 2010 (5)
- ▼ 2009 (46)
 - ▼ December (1)
 - [8 Million Reasons for Real Surveillance Oversight](#)
 - ▶ August (4)
 - ▶ July (15)
 - ▶ June (5)
 - ▶ May (4)
 - ▶ April (7)
 - ▶ March (10)
- ▶ 2007 (49)
- ▶ 2006 (127)
- ▶ 2005 (103)

made U.S. v. Microsoft, No. 08-30385 archived on August 23, 2010

significant, yet little known role in law enforcement and intelligence gathering.

Government agents routinely obtain customer records from these firms, detailing the telephone numbers dialed, text messages, emails and instant messages sent, web pages browsed, the queries submitted to search engines, and of course, huge amounts of geolocation data, detailing exactly where an individual was located at a particular date and time.

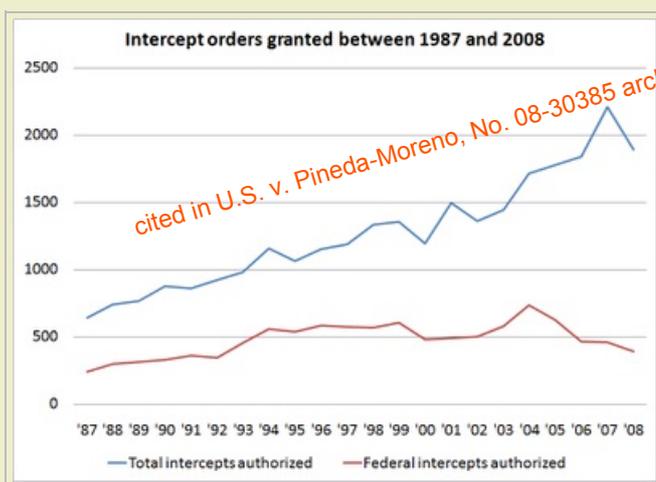
These Internet/telecommunications firms all have special departments, many open 24 hours per day, whose staff do nothing but respond to legal requests. Their entire purpose is to facilitate the disclosure of their customers' records to law enforcement and intelligence agencies – all following the letter of the law, of course.

'Juking' the stats

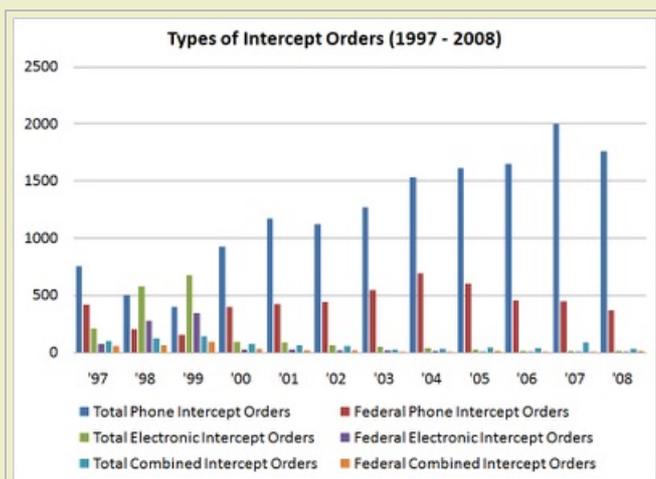
If you were to believe the public surveillance statistics, you might come away with the idea that government surveillance is exceedingly rare in the United States.

Every year, the US Courts produce the wiretap report which details every 'intercept' order requested by Federal, state and local law enforcement agencies during that year. Before the police, FBI, DEA or other law enforcement agents can tap a phone, intercept an Internet connection, or place a covert bug into a suspect's home, they must obtain one of these orders, which law professor and blogger Orin Kerr describes as a "super warrant," due to the number of steps the government must go through in order to obtain one.

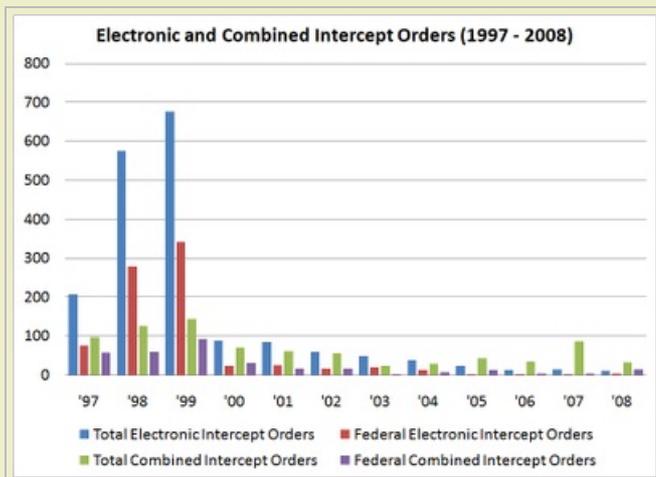
The official wiretap reports reveal that there are approximately 2000 intercept orders sought and approved by judges each year.



As you might expect, the vast majority of these intercept orders are for phone wiretaps. Thus, for example, of the 1891 intercept orders granted in 2008, all but 134 of them were issued for phone taps.



The number of electronic intercept orders, which are required to intercept Internet traffic and other computer assisted communications is surprisingly low. There were just 10 electronic intercept orders requested in 2008, and only 4 of those were from the Federal government – which was itself a massive increase over the **one single** order sought by the entire Department of Justice in both 2006 and 2007.



This graph, and the information contained within it, simply does not make sense. The number of electronic intercepts should, like the number of phone wiretaps, be going up over time, as more people purchase computers, and as criminals or other persons of government interest start to use computers to communicate and plan their business activities. Why were there almost 700 total (federal and state) electronic intercept orders obtained in 1998, but only 10 in 2008?

While I have no way of proving it, I suspect that there have never been a large amount of electronic intercept orders obtained in order to monitor computer communications. The electronic intercept orders, as reported by the US Courts, include those used to monitor computers, fax machines, and pagers. The wiretap report doesn't break down the numbers for these individual technologies – but I suspect that the nearly 700 electronic intercept orders granted in 1998 were largely for fax machines and pagers. Thus, as these technologies died out, it is only natural that the number of electronic intercept orders declined

That still leaves us with one large question though: How often are Internet communications being monitored, and what kind of orders are required in order to do so.

The stats don't cover all forms of law enforcement surveillance

As I described at the beginning of this article, the government routinely obtains customer records from ISPs detailing the telephone numbers dialed, text messages, emails and instant messages sent, web pages browsed, the queries submitted to search engines, and geolocation data, detailing exactly where an individual was located at a particular date and time.

However, while there are many ways the government can monitor an individual, very few of these methods require an intercept order.

In general, intercept orders are required to monitor the **contents** of real time communications. **Non-content** information, such as the To/From and Subject lines for email messages, URLs of pages viewed (which includes search terms), and telephone numbers dialed can all be obtained with a pen register/trap & trace order.

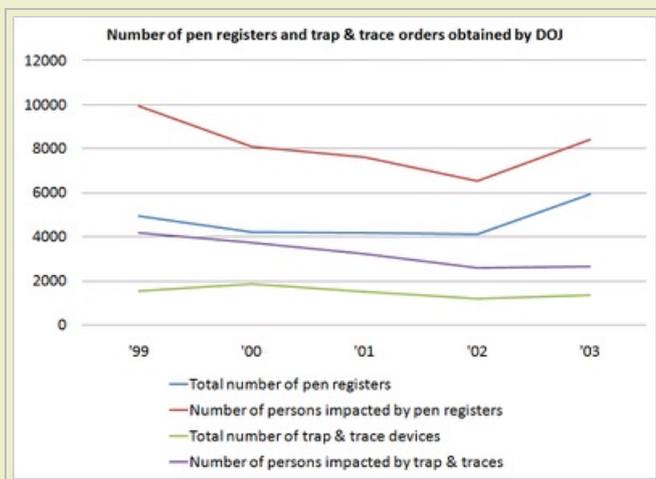
While wiretaps require a "superwarrant" which must be evaluated and approved by a judge following strict rules, government attorneys can obtain pen register orders by merely certifying that the information likely to be obtained is relevant to an ongoing criminal investigation – a far lower evidentiary threshold.

In addition to the fact that they are far easier to obtain, pen register

U.S. v. Pineda, No. 08-30585 archived on August 26, 2010

orders are also not included in the annual US courts wiretap report. Not to fear though -- a [1999 law requires](#) that the Attorney General compile annual statistics regarding DOJ's use of pen register orders, which he must submit to Congress.

Unfortunately, the Department of Justice [has ignored this law](#) since 2004 -- when five years worth of reports were provided to Congress in the form of a single document dump covering 1999-2003. Since that one submission, both Congress and the American people have been kept completely in the dark regarding the Federal government's extensive use of pen registers.



Since we don't have any pen register stats for the last five years, it is difficult to do a current comparison. However, for the five years worth of data that we do have, it is possible to make a few observations.

First, in 2003, Federal agents used 15 times more pen registers and trap & traces than intercepts. Perhaps this was because each of the 578 Federal intercept orders obtained in 2003 had to be thoroughly evaluated and then approved by a judge, while the 5922 pen registers or 2649 trap & trace devices each received a cursory review at best.

Second, the number of pen registers and trap & trace orders went **down** after 9/11, at a time when the FBI and other parts of DOJ were massively increasing their use of surveillance. 4210 pen registers were used in 2000, 4172 in 2001, and 4103 in 2002.

It is important to note that these numbers only reveal part of the picture, as these statistics only cover the use of pen registers/trap & traces by the Department of Justice. There are no public stats that document the use of these surveillance methods by state or local law enforcement. Likewise, these stats only cover the requests made for law enforcement purposes -- pen register surveillance performed by the intelligence community isn't reported, even in aggregate form.

Stored Communications

The reporting requirements for [intercepts](#) and [pen registers](#) only apply to the surveillance of live communications. However, communications or customer records that are **in storage by third parties**, such as email messages, photos or other files maintained [in the cloud](#) by services like Google, Microsoft, Yahoo Facebook and MySpace are routinely disclosed to law enforcement, and there is no legal requirement that statistics on these kinds of requests be compiled or published.

There is currently no way for academic researchers, those in Congress, or the general public to determine how often most email, online photo sharing or social network services deliver their customers' data to law enforcement agents.

While these firms deliver sensitive customer data to government agents on a daily basis, they go out of their way to avoid discussing it.

"As a matter of policy, [we do not comment](#) on the nature or substance of law enforcement requests to Google."

cited in U.S. v. Pisciotta, No. 08-30383, archived on August 26, 2010

"We do not comment on specific requests from the government. Microsoft is committed to protecting the privacy of our customers and complies with all applicable privacy laws."

"Given the sensitive nature of this area and the potential negative impact on the investigative capabilities of public safety agencies, Yahoo does not discuss the details of law enforcement compliance. Yahoo responds to law enforcement in compliance with all applicable laws."

Only Facebook and AOL have publicly disclosed the approximate number of requests they receive from the government – 10-20 requests per day and 1000 requests per month, respectively.

Follow the money

"When I can follow the money, I know how much of something is being consumed - how many wiretaps, how many pen registers, how many customer records. Couple that with reporting, and at least you have the opportunity to look at and know about what is going on.

– Albert Gidari Jr., Keynote Address: Companies Caught in the Middle, 41 U.S.F. L. Rev. 535, Spring 2007.

Telecommunications carriers and Internet firms do not just hand over sensitive customer information to law enforcement officers. No – these companies charge the government for it.

Cox Communications, the third largest cable provider in the United States, is the only company I've found that has made its surveillance price list public. Thus, we are able to learn that the company charges \$2,500 for the first 60 days of a pen register/trap and trace, followed by \$2,000 for each additional 60 days, while it charges \$3,500 for the first 30 days of a wiretap, followed by \$2,500 for each additional 30 days. Historical data is much cheaper – 30 days of a customer's call detail records can be obtained for a mere \$40.

Comcast does not make their price list public, but the company's law enforcement manual was leaked to the Internet a couple years ago. Based on that 2007 document, it appears that Comcast charges at least \$1000 for the first month of a wiretap, followed by \$750 for each month after that.

In the summer of 2009, I decided to try and follow the money trail in order to determine how often Internet firms were disclosing their customers' private information to the government. I theorized that if I could obtain the price lists of each ISP, detailing the price for each kind of service, and invoices paid by the various parts of the Federal government, then I might be able to reverse engineer some approximate statistics. In order to obtain these documents, I filed Freedom of Information Act requests with every part of the Department of Justice that I could think of.

The first agency within DOJ to respond was the U.S. Marshals Service (USMS), who informed me that they had price lists on file for Cox, Comcast, Yahoo! and Verizon. Since the price lists were provided to USMS voluntarily, the companies were given the opportunity to object to the disclosure of their documents. Neither Comcast nor Cox objected (perhaps because their price lists were already public), while both Verizon and Yahoo! objected to the disclosure.

I then filed a second request, asking for copies of the two firms' objection letters. Those letters proved to be more interesting than the price lists I originally sought.

[Click here](#) for the complete Verizon price list letter.

[Click here](#) for the complete Yahoo! price list letter.

First, Verizon revealed in its letter that it "receives tens of thousands of requests for customer records, or other customer information from law enforcement."

As background, each year Verizon receives tens of thousands of requests for customer records or other customer information from law enforcement. Verizon

cited in U.S. v. Pineda, No. 08-385 archived on August 26, 2010

Assuming a conservative estimate of 20,000 requests per year, Verizon alone receives more requests from law enforcement per year than can be explained by any published surveillance statistics. That doesn't mean the published stats are necessarily incorrect – merely that most types of surveillance are not reported.

In its letter, Verizon lists several reasons why it believes that its price list should remain confidential. Of these reasons – two stand out. First, the company argues, customers might "become unnecessarily afraid that their lines have been tapped, or call Verizon to ask if their lines are tapped (a question we cannot answer.)"

instances, court orders). Verizon makes a conscious effort to shield this pricing information from our competitors; we believe our competitors do the same. In addition, we do not want the general public to have access to these pricing schedules.

are reserved only for law enforcement emergencies. Other customers may, upon seeing the availability of certain services to law enforcement (such as wiretapping, for instance), become unnecessarily afraid that their lines have been tapped or call Verizon to ask if their lines are tapped (a question we cannot answer). Additionally, the pricing

The second interesting reason is that:

"Our pricing schedules reveal (for just two examples) that upon the lawful request of law enforcement we are able to [redacted by USMS]. In cooperation with law enforcement, we do not release that information to the general public out of concern that a criminal may become aware of our capabilities, see a change in his service, correctly assume that the change was made at the lawful request of law enforcement and alter his behavior to thwart a law enforcement investigation."

Moreover, the availability of the pricing schedules to the general public may interfere with law enforcement investigations. As a trustee of information that is lawfully used by law enforcement to enforce the law and protect the public, we take our duty to not unnecessarily release that information very seriously. Our pricing schedules reveal (for just two examples) that upon the lawful request of law enforcement we are able to [redacted] in cooperation with law enforcement, we do not release that information to the general public out of concern that a criminal may become aware of our capabilities, see a change to his service, correctly assume that the change was made at the lawful request of law enforcement and alter his behavior to thwart a law enforcement investigation.

I'm not sure what capabilities this section is referring to – but I'd love to find out more.

Yahoo!'s letter is far less exciting, and doesn't even hint at the number of requests that the company receives. There is one interesting tidbit in the letter though:

"It is reasonable to assume from [these comments](#) that the [pricing] information, if disclosed, would be used to "shame" Yahoo! and other companies – and to "shock" their customers. Therefore, release of Yahoo!'s information is reasonably likely to lead to impairment of its reputation for protection of user privacy and security, which is a competitive disadvantage for technology companies."

It is reasonable to assume from these comments that the information, if disclosed, would be used to "shame" Yahoo! and other companies -- and to "shock" their customers. Therefore, release of Yahoo!'s information is reasonably likely to lead to impairment of its reputation for protection of user privacy and security, which is a competitive disadvantage for technology companies.

Geolocation

"Federal officials are routinely asking courts to order cellphone companies to furnish real-time tracking data so they can pinpoint the whereabouts of drug traffickers, fugitives and other criminal suspects, according to judges and industry lawyers." Ellen Nakashima, [Cellphone Tracking Powers on Request](#), The Washington Post, November 23, 2007.

"Law enforcement routinely now requests carriers to continuously 'ping' wireless devices of suspects to locate them when a call is not being made ... so law enforcement can triangulate the precise location of a device and [seek] the location of all associates communicating with a target."

– Christopher Guttman-McCabe, vice president of regulatory

As mobile phones have become ubiquitous, the law enforcement community has learned to leverage the plentiful, often real-time location information that carriers can be compelled to provide. Location requests easily outnumber wiretaps, and as this article will reveal, likely outnumber all other forms of surveillance request too.

In terms of legal requirements, this information can often be gained through the use of a [hybrid order](#), combining a Stored Communications Act request and a Pen Register request. As noted before, the former law has no reporting requirement, and the law requiring reports for the Pen Register requests has been ignored by the Department of Justice since 2004.

In March of this year, telecommunications lawyer Al Gidari, who represents many of the major telcos and ISPs, [gave a talk](#) at the Berkman Center at Harvard University. During his speech, he revealed that each of the major wireless carriers receive approximately 100 requests per week for customers' location information.

100 requests per week * 4 wireless major carriers (Sprint, Verizon, AT&T, T-Mobile) * 52 weeks = 20k requests per year.

While Gidari's numbers were shocking when I first heard them, I now have proof that he significantly underestimated the number of requests by several orders of magnitude.

Hanging with the spooks

Several times each year, in cities around the globe, representatives from law enforcement and intelligence agencies, telecommunications carriers and the manufacturers of wiretapping equipment gather for a closed door conference: [ISS World](#): Intelligence Support Systems for Lawful Interception, Criminal Investigations and Intelligence Gathering

ISS World is no stranger to the privacy community. Back in 2000, FBI agents showed off a prototype of the [Carrier More interception system](#) to attendees at ISS World. Days later, stories appeared in both the Wall Street Journal and [The New York Times](#) after one attendee leaked information to the press.

ISS World had been on the list of events that I'd wanted to attend for a long time, even moreso after my research interests started to focus on government surveillance. Thus, in October of this year, just a month after moving to Washington DC, I found myself at the Washington DC Convention Center, attending ISS World.

Looking around at the name badges pinned to the suits milling around the refreshment area, it really was a who's who of the spies and those who enable their spying. Household name telecom companies and equipment vendors, US government agencies (both law enforcement and intel). Also present were representatives from foreign governments - Columbia, Mexico, Algeria, and Nigeria, who, like many of the US government employees, spent quite a bit of time at the vendor booths, picking up free pens and coffee mugs while they learned about the latest and greatest surveillance products currently on the market.

The main draw of the event for me was two panel discussions: A presentation on "Regulatory and CALEA Issues Facing Telecom Operators Deploying DPI Infrastructure", and a "Telecom Service Providers Roundtable Discussions"

Not knowing ahead of time what the speakers would say, and not wanting to be called a liar if I later cited an interesting quote in a research paper, I decided to make an audio recording of the two panels.

One wireless company, 50 million customers, 8 million law enforcement requests for customer GPS information in one year

Both panels are fascinating, and worth listening to in full. [Click here](#) for an mp3 of the complete the Deep Packet Inspection Panel.

File In U.S. v. Pineda-Moreno, No. 08-30385 archived on August 26, 2010

[Click here](#) for mp3 of entire telecom panel.

However, by far the most jaw-dropping parts of the telecom service providers roundtable were the following quotes:

"[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.
– [Paul Taylor](#), Electronic Surveillance Manager, Sprint Nextel.

"In the electronic surveillance group at Sprint, I have 3 supervisors. 30 ES techs, and 15 contractors. On the subpoena compliance side, which is anything historical, stored content, stored records, is about 35 employees, maybe 4-5 supervisors, and 30 contractors. There's like 110 all together."
– [Paul Taylor](#), Electronic Surveillance Manager, Sprint Nextel, describing the number of employees working full time to comply with requests for customer records.

"Cricket doesn't have as many subscribers so our numbers are going to be less. I think we have 4.5 - 5 million subscribers. We get approximately 200 requests per calendar day, and that includes requests for records, intercepts. We don't have the type of automation they do, and we can't do the location specificity that they can, because we don't have GPS."
– Janet A. Schwabe, Subpoena Compliance Manager, Cricket Communications

"Nextel's system, they statically assign IP addresses to all handsets ... We do have logs, we can go back to see the IP address that used MySpace. By the way - MySpace and Facebook, I don't know how many subpoenas those people get, or emergency requests but god bless, 95% of all IP requests for emergencies are because of MySpace or Facebook... On the Sprint 3G network, we have IP data back 24 months, and we have, depending on the device, we can actually tell you what URL they went to ... If [the handset uses] the [WAP] Media Access Gateway, we have the URL history for 24 months ... We don't store it because law enforcement asks us to store it, we store it because when we launched 3G in 2001 or so, we thought we were going to bill by the megabyte ... but ultimately, that's why we store the data ... It's because marketing wants to rifle through the data."
– [Paul Taylor](#), Electronic Surveillance Manager, Sprint Nextel.

"Two or three years ago, we probably had less than 10% of our requests including text messaging. Now, over half of all of our surveillance includes SMS messaging."
– [Paul Taylor](#), Electronic Surveillance Manager, Sprint Nextel.

Conclusion

As the information presented in this article has demonstrated, the publicly available law enforcement surveillance statistics are, at best misleading, and at worst, deceptive. It is simply impossible to have a reasonable debate amongst academics, public policy makers, and members of the public interest community when the very scale of these surveillance programs is secret.

As an example, consider the [following quote](#) from the November 4, 2009 markup hearing of the House Judiciary Committee, which is currently considering a bill to expand the government's PATRIOT Act surveillance powers. During the hearing, [Rep. Lamar Smith](#), the Ranking (Minority) Member said the following:

Unlike other tools which actually collect content, such as wiretaps, pen registers and trap-and-trace devices merely request outgoing and incoming phone numbers. Because the government cannot collect any content using pen registers, a minimization requirement makes no sense. What is there is there to minimize?

After reading this article, it should be clear to the reader that pen

Case v. Pineda, No. 08-50385 archived on August 26, 2010

registers and trap & trace devices are used for **far more** than just collecting phone numbers dialed. They are used to get email headers (including To, From and Subject lines), the URLs of web pages viewed by individuals, and in many situations, they are used (along with a Stored Communications Act request) to get geolocation information on mobile phone users.

The reason I'm quoting Rep. Smith isn't to poke fun at his expense, but to make a serious point. How can we have a serious public debate about law enforcement surveillance powers, when the senior most Republican on the committee responsible for the oversight of those powers doesn't understand how they are being used? Likewise, this paragraph should by no means be read as an attack on Rep. Smith. How can he be expected to understand the extensive modern use of pen registers, when the Department of Justice continues to break the law by failing to provide yearly statistics on the use of pen registers to Congress?

My point is this: The vast majority of the government's access to individuals' private data is not reported, either due to a failure on DOJ's part to supply the legally required statistics, or due to the fact that information regarding law enforcement requests for third party stored records (such as email, photos and other data located in the cloud) is not currently required to be collected or reported.

As for the millions of government requests for geo-location data, it is simply disgraceful that these are not currently being reported...but they should be.

at 7:00 AM

Labels: [4th amendment](#), [privacy](#), [surveillance](#)

90 comments:

 **cw said...**

This is awesome stuff, Chris. I am particularly happy to see you sharing your raw materials. This is something which (shamefully, in my opinion) researchers in the social sciences – especially those early in their careers – tend to hoard.

9:47 AM

 **Anonymous said...**

Great work!

11:18 AM

 **Christopher Parsons said...**

Impressive, as always. Many thanks for sharing out this information!

11:21 AM



 **Peter said...**

This is good research on privacy as a whole. The Eye opener here is that the 3rd data on the cloud seem to have no legal requirements on disclosure !

12:03 PM



 **Maurice said...**

OK. I should probably wade through all of this, but I have a quibble with the headline.

It's not clear to me from a quick perusal that Sprint gave up 8 million different customers' locations during that 13 month period. In fact, a little quick math gets me to roughly 900 hits per hour over that 13 month period, and if one makes (an obviously generous) assumption that they're tracking individuals over the course of that hour, say checking every minute, then we're talking about 15 individuals.

That's way too generous, but I offer it to make the point: The stats I want to know:

cited in U.S. v. Pineda, No. 08-10385 archived on August 26, 2010

1. How many distinct cell phones were tracked?
2. I'd like to see some descriptive stats on how long cell phones were tracked.

How many were mobsters that were tracked for the entire period? How many were one-shot deals, a cell at a specific time? How many of those were one-shot deals for the current position? What was the mean period a cell phone was tracked? It'd also be interesting to see which phones were tracked repeatedly, and get similar stats for that parameter.

None of this to say it's OK to give up the data without a warrant. But I want to skip the hype and know if we're talking about thousands of individuals or millions.

12:59 PM



earl wallace said...

Chris,

Thank you for releasing this information. I am not shocked nor surprised for I suspected it and more. If our founding fathers were here today i would love to see their reaction. I am aware of much farther reaching surveillance techniques such as Echelon which many people have no idea that it exists. Luckily for me my viewable data on electronic devices is inane and transparent. I have given up on the idea that I really have constitutional rights. I am at peace for this behavior has been fortold for thoud=sands of years and is now coming to pass.

earlwallace

1:08 PM

Dissent said...

Fascinating and troubling stuff, Chris. And your point about Congress is right on – despite what might be good intentions of some, in the absence of a fuller picture of the scope of what's really going, they are legislating in the dark.

Zip file now mirrored at

<http://www.pogowasright.org/files/soghoian-surveillance-dump.zip>

1:13 PM

Mashio X. said...

Saw your post from EFF's twitter.

Mirrored your zip file on my network.

http: <http://amerika.ath.cx:81/packages/soghoian-surveillance-dump.zip>

anonymous ftp: <ftp://amerika.ath.cx/soghoian-surveillance-dump.zip>

1:33 PM

Albert Gidari said...

Chris, inasmuch as I'm your opening quote, I thought I'd comment on your post to dispel any implication that service providers act without lawful authorization in response to law enforcement demands. Both my speech and article make it very clear that service providers push back hard when legal process or demands appear inadequate. Indeed, that was the point of the article – providers are in the middle and doing a pretty good job of it.

As far as your central thesis - that we need more transparency and reporting of the number of requests and customer records or information obtained - I couldn't agree with you more. The legal authorities need to be made clear so there is no mistake about who can get what with which form of process, and providers need to be reimbursed for the cost of compliance and immunized for good faith responses. When law enforcement has to pay for the service, indiscriminate requests disappear. For example, it is a common practice for some agencies to submit pen register

Discussed in U.S. v. Pineda-Moreno, No. 08-10385 archived on August 26, 2010

outputs day after day for subscriber information and toll records on everyone called by a target, and to use that pen register order with every carrier who owns one of the numbers on the output – a practice made possible by PATRIOT ACT amendment of the pen register statute to permit "roving" orders. These requests are a burden on providers, and over-collect. When you pay per record, you are more careful.

AI

2:00 PM

 **Anonymous said...**

A question to look into: How many of these calls resulted from people calling 911 from their cell phone? That number is bound to go up with the proliferation of cell phones and occurrences of people dropping their land lines in favor of cells.

2:29 PM



 **Gamoe said...**

Illuminating, on the lack of illumination.

Sure, we need to track and catch those who break our most sacred rules- murderers, rapists, etc. But among those sacred rules are also the right to privacy, the necessity of legal due process, the balancing of power and an ongoing dialog with a free people. The more these sacred rules are violated, the less free we become, and the less the difference between our "criminals" and our "defenders".

Than you for your work and your article, Chris.

3:02 PM

 **Anonymous said...**

Yahoos compliance guide is at

http://files.leagueathletics.com/Images/Club/2515/MEMBERS%20ONLY/BULLETIN%20BOARD%20Yahoo_Compilance_Guide_For_Law_Enforcement_11-08%5B1%5D.pdf

<http://tinyurl.com/ydyjgdt>

3:25 PM

 **Dan Collis-Puro said...**

Chris, you're a champ. This may make me leave sprint.

Oh, and mirrored at:

<http://www.collispuro.com/soghoian-surveillance-dump.zip>

3:30 PM

 **Anonymous said...**

Nice work Chris!!!! Don't you just love how the "Govt" attempts to make their "targets" (in their own words) look like the paranoid party in these matters?

3:32 PM

 **J. Clifford said...**

Thanks for your excellent work. We're going to be reading, and re-reading, your work for implications over at IregularTimes.com. That the House and Senate are working to reauthorize the Patriot Act and FISA Amendments Act, when there is abuse on this scale, is disturbing. We SHOULD expect our members of Congress to be on top of this information, or to vote against laws enabling this surveillance if they aren't given adequate information.

Keep up the important work!

*More info: No. 08-30385 archived on August 26, 2010
cited in U.S. v. Pineda-Moreno*

4:00 PM

 **Paul Ohm said...**

I've already posted this ad on my own group blog (freedom-to-tinker.com) but I thought I'd repeat it here. Chris and Al and other interesting people will be speaking this Friday in Boulder, Colorado, at a conference I am hosting on "[Reforming Internet Privacy Law.](#)" I recommend any of you who want to hear more about this and other cutting-edge Internet privacy issues to attend.

4:19 PM

 **keith.a.lane said...**

Interesting post, I would agree with comment #3 that it would be useful to see the number of distinct phones disclosed, and the average interval between disclosure. Personally my expectation of privacy is such that I would be concerned with any sort of constant 'ping' tracking my location over a period of time. However I might still consider this an acceptable consequence of using a mobile phone service (if we were made aware of when it is being used)

I would request a 'Sanity Check' on the AOL/Facebook numbers. Given the number of users of each service located in the US. A certain factor applies expressing the likelihood of an AOL user vs. a Facebook users information being requested.

I agree with your concern over the pricing lists, and compliancy information being restricted. I would expect that this information should be a matter of public record. If a legal pretext cannot be found, I would expect that enough bad PR would force the disclosure of this "secrets" anyway. I would be especially concerned if fulfilling these requests becomes a "profit center" for the carrier.

The quote about Yahoo's reputation being impaired if these were released is interesting, as in my understanding it is not generally considered slander/defamation to release a true fact.

Also interesting is the sprint quote about 95% of requests being due to myspace/facebook...what is he talking about, and why???

4:35 PM

 **Joris van Hoboken said...**

After reading through this great report I am left wondering whether this is a profitable operation for providers. My guess is that this is the case. Law enforcement access is treated as a market in these materials. And this market would be distorted because of transparency towards their actual customers???

In the Netherlands, there are standard public prices for compliance and some activities are not refunded at all. Although we have our own problems with transparency and staggering amounts of wiretaps (around 2000 active each day) and related requests (3 million requests for identifying information of communication provider customers each year on a population of 16 million) the pricing should not create perverse incentives for providers.

Maybe it would be interesting to add some data about law enforcement access to personal data markets outside of the communications field. I studied that field a bit a few years ago and the market seems quite attractive and very mature. It might be at least a little easier to get data there. On the general legal picture in that field, I found D.J. Solove's 'Access and aggregation: public records privacy and the constitution', in Minnesota Law Review (86) 2002, p. 1137-1218, very helpful.

4:47 PM

 **Anonymous said...**

I find it interesting that you did not make any mention of CALEA, signed into law by then president Clinton.

Site ID: 16, V. Pineda-Morales, No. 08-30383, archived on August 26, 2010

I suppose the reason it was excluded is that it wouldn't have helping your scare tactics.

4:52 PM

  **I said...**

Great article. Wondering if the information being made available to law enforcement is the same sort that is available to corporations who own the phones and plans they provide to employees for their use. This is a different sort of "big brother," but irks me enough that I keep my work cell phone in a drawer at my desk.

5:01 PM

  **Maurice said...**

Another random thought: Isn't it a *good* thing that the providers charge for the service?

If it takes a financial disincentive to get authorities to respect right, fine with me. Probably wouldn't guarantee a nosy detective wouldn't check up on an annoying neighbor, but maybe he'd think twice if he had to account for the expense.

5:22 PM

  **brian8655 said...**

http://www.google.com/url?sa=t&source=web&ct=res&cd=1&ved=0CAkQFjAA&url=http%3A%2F%2Fwww.michigan.gov%2Fdocuments%2Fmsp%2FSPAP-Contact-List-NextelSprint_176799_7.pdf&ei=hpoVS4SKLJXtIAfdusHCBQ&usq=AFQjCNGblJZmwdUWZFb_Ptsx7P4ZjZmxQ&sig2=FWft7O1UZFIJk4-Jew8uPQ

5:38 PM

 **Anonymous said...**

I fail to see how CALEA would do anything but add to the scare tactics. Do you even know what CALEA is?

5:39 PM

  **Paul said...**

Just don't be surprised if Chris mysteriously disappears.

5:55 PM



 **Jonathan Eyer-Werve said...**

@anon: upon looking up CALEA, I am not reassured – telcos are encouraged to turn over data quickly. How they do it is up to them. Not sure why you bring this act up here.

FCC says:

CALEA COMPLIANCE – SOME BASIC INFORMATION

Pursuant to CALEA, industry is basically responsible for setting CALEA standards and solutions. Unless a party files a special petition pursuant to CALEA § 107(b), the Commission does not get formally involved with the compliance standards development process. CALEA also does not provide for Commission review of manufacturer-developed solutions. Entities subject to CALEA are responsible for reviewing the Commission's regulations and analyzing how this regulation applies per their specific network architecture.

A telecommunications carrier may comply with CALEA in different ways. First, the carrier may develop its own compliance solution for its unique network. Second, the carrier may purchase a compliance solution from vendors, including the manufacturers of the equipment it is using to provide service. Third, the carrier may purchase a compliance solution from a trusted third party (TPP).

cited in *U.S. v. Pineda-Moreno*, No. 08-30385 archived on August 26, 2010

Regarding the use of trusted third parties, the Commission provided the following guidance on the use of TTPs in the CALEA Second Report and Order, at paragraph 26:

"The record indicates that TTPs are available to provide a variety of services for CALEA compliance to carriers, including processing requests for intercepts, conducting electronic surveillance, and delivering relevant information to LEAs. Given the effectively unanimous view of commenters that the use of TTPs should be permitted but not required, we conclude that TTPs may provide a reasonable means for carriers to comply with CALEA, especially broadband access and VoIP providers and smaller carriers. We emphasize, however, that if a carrier chooses to use a TTP, that carrier remains responsible for ensuring the timely delivery of CII and call content information to a LEA and for protecting subscriber privacy, as required by CALEA. Thus, a carrier must be satisfied that the TTP's processes allow the carrier to meet its obligations without compromising the integrity of the intercept. Carriers will not be relieved of their CALEA obligations by asserting that a TTP's processes prevented them from complying with CALEA. We note DOJ's concern about carriers attempting to use TTPs to shift costs to LEAs, but we make no decision here that would allow carriers who choose to use a TTP to shift the financial responsibility for CALEA compliance to the Attorney General under Section 109.... We will evaluate whether the availability of a TTP makes call-identifying information "reasonably" available to a carrier within the context of section 103 in acting on a section 109 petition that a carrier may file. As noted by several commenters, telecommunications carriers and manufacturers have legally-mandated privacy obligations, and we take no action herein to modify those obligations based on potential broadband access and VoIP provider use of TTPs. Finally, in accord with the consensus of comments, we will defer to standards organizations and industry associations and allow them to determine the degree to which the ability of a TTP external system to extract and isolate CII makes that information reasonably available for purposes of defining CALEA standards and safe harbors. See CALEA Second Report and Order at para. 26 (emphasis added).

To contact TTPs, carriers may conduct an Internet search using such key words as "CALEA compliance" and "CALEA compliance help," or any combination that will yield a display of TTPs.

<http://www.fcc.gov/calea/>

6:46 PM

 **Anonymous said...**

Please keep up the good work.

7:32 PM

 **jb89149 said...**

Good job bro. The spooks are not going to not like you. Watch your ass.

7:59 PM

 **Sean said...**

I wonder if one turns off the 'Locator' function of their cell phone, this system can still track someone. As I understand it, 911 tracking is enabled all the time, so I guess it would be possible.

Makes me want to dump my cell phone...

8:02 PM

 **Anonymous said...**

Wondering if there are any stats for OnStar or other in-car GPS / speaker combos accessed by law enforcement?

8:12 PM

Entered in U.S. v. Pineda-Moreno, No. 66-30385 archived on August 26, 2010

Anonymous said...

I have a problem with financial disincentives: where the money comes from. Law enforcement is paid for via taxes, so not only are we paying a higher bill to the phone company (TPC) on the front-end for the infrastructure, we're also funding federal, state, and local governments to pay for wiretaps, etc., on the back-end. Business is business for TPC, but the "law" is being used to strong-arm the consumer into paying for the privilege of being spied upon.

9:15 PM

Silent Assassin said...

Nice research and all. However, I believe you need to be responsible on what information is released. Not that I am in favor of uncontrolled police monitoring, but like your paper disclosed, the government has to go through a lot to gain access to this information. On the flip side, with the war on terrorism and law enforcement performing their jobs, informing the "bad guys" of these techniques defeats future endeavors. Now when a kidnapper has a child, he may think to not have his cellphone because he knows police may be able to get his gps location from a cell phone provider. Again, not trying to censor information, but certain information should not be available to everyone. We would ALL agree if terrorists, or Iran have the information to build a nuclear bond, what will they do with that information....

10:01 PM

Anonymous said...

Where and who are the gate keepers?!?!

10:30 PM

Matt said...

Chris,

As a follow-up to my earlier e-mail, I wanted to properly characterize the "8 million" figure that you prominently feature in your blog and email.

The "8 million" figure does not represent the number of customers whose location information was provided to law enforcement, nor does it represent the instances or cases in which law enforcement contacted Sprint seeking customer location information.

Instead, the figure represents the number of individual automated requests, or "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. The critical point is that a single case or investigation may generate thousands of individual requests to the network as the law enforcement or public safety agency attempts to track or locate an individual over the course of days or weeks.

As a result, the 8 million automated requests or pings were generated by thousands (NOT millions) of instances in which law enforcement or public safety agencies sought customer location information. Several thousand instances over the course of a year should not be shocking given that we have 47 million customers and requests from law enforcement and public safety agencies are due to a variety of circumstances: exigent or emergency situations, criminal investigations, or cases where a Sprint customer consents to sharing location information.

It's also important to note that we complied with applicable state and federal laws in all of the instances where we fulfilled a law enforcement or public safety request for location information.

Matt Sullivan
Sprint Nextel
Matthew.sullivan@sprint.com

Filed in U.S. v. Pineda, Moreno, No. 08-30385 archived on August 26, 2010

11:26 PM

 **Laura said...**

There's no such thing as privacy anymore.

12:46 AM

 **Greg said...**

Maurice wrote "Another random thought: Isn't it a good thing that the providers charge for the service?"

It's a mixed blessing. The only people in a position to question the lawfulness of these orders is the service provider. If the requests are a profit center then it would be reasonable to expect telcos to do everything they can to maximize them (regardless of the lawfulness if they also get immunity).

A better system might be to have statutory rates that get paid into a pool and then reimbursed to communications companies based purely on their subscriber count and not on requests processed. This is still market-distorting, but at least not distorting in a way which is harmful to the public.

3:12 AM

 **Ian said...**

My thanks to emergentchaos.com for drawing my attention to Chris's report, which I have yet to read fully. My comments below are responses to the comments section. I hope they may be of use.

Anonymous asked about the gatekeepers, who would appear to be the police management or/and, the public publication of audit reporting. What audit of computer use happens within US law enforcement and how/where is that reported?

FOI becomes a hit and miss audit method, reliant upon (ignoring those who are compromised and use FOI as a means of locating that compromise) the good will and timing of those who utilise it.

Law enforcement paying for the data may create a little more openness because of financial audit, but that does not in my opinion, provide an adequate answer. Overall the amounts may not be significant for each individual request so the underlying issues would/do remain the same.

People commenting generally seem more interested in the minutia that the over arching issue(s), which is understandable when allowing for individual documents which have yet to be written.

Peters comment on disclosure is one answer. However, Law enforcement agencies are not enamoured with the idea that the organisations they obtain data from should have to inform the person whom they intercept data about even if the notification is at a time when no compromise could be caused to the law enforcement efforts; (For example, at a time identified by law-enforcement during the initial connection and allowing for alteration to that period by law-enforcement to account for unexpectedly extended investigations.) Probably because they feel vulnerable relying upon another organisation to advise without compromising their efforts and the potential for litigation this opens up - they would have to be more open and trusting with each organisation concerned.

Gamoos comment on prioritising access to the more serious crimes in my experience will not stop any abuse, although it is a way of reducing the volume somewhat.

Anonymous comment about 911 calls sounds as if it is on a different track. 911 calls will be for subscriber or location information only. It is only at a later stage as things move into an investigation stage that other call information becomes of interest. If 911 calls are obtaining other information other than location or subscriber, they are already obtaining excessively. I

archived on August 26, 2010
No. ea-3038
U.S. v. Pineda-Moreno

do agree, and it is my experience, that law enforcement does use 911 reasons to obtain the initial access to communications provider's data and then utilise it more widely. i.e. They are not open about intended intelligence applications of the data.

Keith A. Lane raises an interesting point when he mentions the Facebook and AOL users which probably needs further research from within law enforcement to clarify the use of the data. If the data is being used as raw law enforcement intelligence then some of the requests may certainly be seen as fishing exercises. That is notwithstanding the issues of law enforcement using Myspace and Facebook as publicly available policing resources or using the data to trace a user/abuser of those sites.

Silent Assassins comments on the privacy aspects of research data are in my opinion very valid. Free availability of data within a research community is a different issue. The many comments about the vulnerability of the researcher(s) merely supports official secrecy in these types of area.

Matt Sullivan from Sprint himself was careful to point out that they complied with local laws, but that is a red tape response which pays no attention to the potential for abuse, something recognised by the question anonymous asked regarding audit.

Ian Welton

5:24 AM

Anonymous said...

To a degree, this is a matter of principled taste: Will you be satisfied with a procedural guarantee of no misuse of observable data or do you prefer a technical guarantee of non-observability in the first place? At its core, the issue is the collectivization of risk as in "what risks are you willing to take on to avoid other risks if the ones you take on are systemic?" A trivial example but germane to telecom is whether you are willing to accept recordability of your position in exchange for being able to call 911 without any coherent idea of where you are? I'm not and haven't carried a cell since the regulation came into force and explicitly because I will not accept the surveillance risk as a fair trade for the non-locatability risk. As John Gilmore eloquently put it: Never give a government a power you would not want a despot to have. Anything else is wishful thinking.

This is anonymous for much the same reason; I will not participate in the model of having an "identity" that is based on details shared with distant corporations no matter how pleasantly convenient nor conveniently pleasant their services may be. You get what you pay for and not just with money.

8:16 AM

Anonymous said...

Chris -

Nice work, but I recommend a more conservative approach in the future. It is not clear to me that this treatment of the topic will encourage future disclosure, given the initial ambiguity surrounding "8 million requests" being cleared up in the comments as really only thousands of unique instances.

Pete Lindstrom

9:38 AM

Anonymous said...

Mr. Sullivan, this is not about shaming your company. You say 8 million 'requests' doesn't mean 8 million phones are being monitored and I believe you. The problem is that there is no way to know how many phones are being monitored.

Now because there is no available information, if someone shouts a number like 8 million and makes it sound believable, then that is what it is. In the public's eye, the number is 8 million.

document ID: 985 archived on August 26, 2010

Even though in reality it may only be a few thousands.

The only solution is for the DOJ to obey the law and come forward with the real numbers. They're not doing anything wrong, so what do they have to hide?

9:40 AM

 **Anonymous said...**

Matt Sullivan (Sprint), that is good feedback. To me, the layman, the numbers Chris presents above are impressively high. While I don't know the frequency of GPS pings I think it would dramatically reduce the actual number of customers monitored. I would like to know the actual number of customers monitored, strictly out of curiosity; I don't *need* to know.

The more transparent the companies become with this information, the more comfortable their customers will be with keeping them as their mobile service provider.

In closing, I am positive Chris's information will get widely disseminated – it is **very** interesting.

10:00 AM



 **Logical Extremes said...**

Profit motive must be taken out of the equation. Reimbursement at incremental cost is the best trade-off use of tax dollars PROVIDED that there is full transparency (which of course there is none today).

Albert Gidari said: "providers need to be... immunized for good faith responses" - Absolutely not! Without liability, there is no incentive for providers to weed out requests not made with proper legal process.

10:06 AM

 **sunbird said...**

I wish we would have had these manuals last weekend. We did a workshop on surveillance and privacy here in Seattle and these would have been great examples.

We did tell everyone who attended about [Taco](#), which is a fantastic plugin.

Thanks for the great post, and also for writing Taco!

10:50 AM

 **Anonymous said...**

thank you chris, you are doing a service! 8million or 8 thousand, the point is that we have a government OF the people BY the people and FOR the people. I am posting this on the state of connecticut Bar Association listserve

2:07 PM

 **Adam said...**

Matt Sullivan,

Thanks for explaining the information in more detail. I'd like to understand more about those pings and how they relate to subjects.

1. How many subjects were there?
2. What were the mean and median # of pings?
3. Were the pings distributed in a "normal" (bell curve) distribution, or in a power law?

How frequent are the pings? Can that be controlled by the requestor?

I thank you for contributing to the public debate, and look forward to your additional clarifications.

Copyright © by Pinada Moreno, No. 08-30385 archived on August 26, 2010

2:22 PM

 **Ian said...**

Having now read the research document a few more hurried notes.

The demand from law enforcement for access to data has/is affecting retention periods.

This external action is having an affect on the market within those sectors, and is creating further demand. A strictly logical reaction of the market to an identified suppressed demand would be to service it.

To service a demand viable financial returns are required.

There is an acceptance within law enforcement that their actions prejudice the subjects of their focus.

The secrecy pressure applied to the organisations law enforcement agencies collect data from can be argued as protecting the data subject from prejudice.

Secret markets result in public unrest.

A natural instinct of individuals who are prejudiced is to learn the details of that prejudice.

Adaptation to prejudice is part of a normal learning cycle, not something suspicious.

Not to adapt to ones prejudices leads to restricted learning abilities.

All sectors generate a language of their own.

Those languages themselves are interesting.

The underlying driving philosophy, together with each individual's philosophy, is more important.

Thank you for making your brief report public.
It is useful.

Rather robotic, but quick.

Ian Welton

3:25 PM

 **Anonymous said...**

I think the country you are referring to is not Columbia but rather Colombia.

Great paper! Thanks for the information.

4:27 PM

 **Anonymous said...**

Sprint, Verizon, T-Mobile and AT&T will give out NOTHING without a court order signed by a judge. These orders are just as difficult (often more difficult) to get than a search warrant. They involve the same affidavit process. The only reason the providers give up that information is that they will be held in contempt if they do not.

4:33 PM

 **Anonymous said...**

Hi everybody! Question - can "they" get a personal data (like memos, tasks) stored on Blackberys, Palms and other devices?

6:29 PM

  **kbp said...**

Thanks,

Your sharing is greatly appreciated!

6:59 PM

  **Adam B said...**

I think it's time to create "Public Oversight" as envisioned by

cited in U.S. v. Pineda-Moreno, No. 08-30385 archived on August 26, 2010

Greg Bear in "Queen of Angels" and "Slant" where all surveillance data is guarded by an organization as tenacious as the ACLU is to civil liberties. To get access to the data you need to prove that you REALLY NEED it, not just suspect something.

7:54 PM

 **Jamie Laing** said...

Thanks for sharing this. I wonder if and when the popular media is going to pick this up?

It seems like your PhD dissertation is pretty well in the bag given the quality and depth of your work, so allow me to give you a premature congratulations!

You've helped your country and it's citizens by doing this work.

7:01 AM

 **1776blues** said...

Excellent job on exposing what our Government is up to. Now we need to get this info out to the masses who still believe we are a free nation with constitutional protections.

I have forwarded this info to my friends and family who will in turn forward it. We need to contact out state and federal reps and tell them we know what they are doing.

Note: I've read and heard that many of our federal agencies can act and implement laws without authorization from Congress.

They Own It All (Including you) is a book that is a must read.

<http://www.newpeopleorder.com/>

I am awaiting my copy but have heard the authors interviewed every Monday for the past 5 weeks on The National Intel Report on Republic Broadcasting Network and it was shocking. This is where I heard about the Federal agencies.

Here is what the book covers;

1. You are legally a debtor and chattel (property) owned by a hidden creditor.
2. There is a hidden lien on everything transacted for by or with a Federal Reserve Note.
3. Your entire alleged wealth is/has been liened, you don't own anything! You merely have possession by privilege. This privilege may be yanked at any time if you don't obey the real owner.
4. The Federal Reserve Note is a foreign product owned by a foreign corporation, and not by you or the U.S. government.
5. The States and the United States courts are bankruptcy courts representing the interests and property of the foreign creditor.
6. Without knowing it, you have been compelled into international commercial law, where you have none of your unalienable rights. Hence, you have been insulated from your birthright, the common Law from which your rights are immutable.
7. You are charged an income (excise) tax for transacting in the foreign commodity known as Federal Reserve Notes.
8. You have been divested of the rights to, value of, and profits from your labor, which has been stolen.
9. Lawful gold coin (pre 1933) money transactions are invisible to the states and national government(s).
10. The real cause of draconian governmental regulation and your

cited in *Book v. Pineda-Moreno*, No. 06-10385 archived on August 26, 2010

loss of rights is the toxic currency.

11. The United States lost its sovereignty in 1933. It is in receivership to the hidden creditor. The bankrupt government is a puppet to the real master, as declared by Banker Rothschild on the cover.

12. The real cause of the current economic calamity is the toxic currency.

13. The hidden creditor (international bankers) owns everything, including you.

14. You have been living within an illusion, believing that you are free, but in reality you are owned!

2:41 PM

 **Anonymous said...**

Geolocation may be a profit center. I don't know what Sprint charges, but going by their LEA pricelist, Nextel charges \$150 "per request". 8 million of those would be over a billion dollars.

3:03 PM

 **Anonymous said...**

I work at a police dept as a 911 calltaker and emergency dispatcher and I have called Sprint to obtain this information. They only give info if it is deemed a life threatening emergency or if the phone called 911. Sorry to bust you guys bubbles, but **EVERY COMPANY DOES THIS**, not just sprint. So it doesnt make a difference who you are with company wise, if you are wanted for a crime you committed or called 911, the police can and will locate you with gps coordinates from your cell phone company if deemed necessary.

6:43 PM

 **Anonymous said...**

Can you tell us what the nature of the copyright claim was? It was you who made the recording, so it was you who fixed the words into a tangible medium.

6:47 PM

 **Drumlib said...**

I would like to know how much of this police state stuff is the result of laws against consensual activities like the war on drugs. Outside of ruining a lot of good people's lives, such laws do little more than create black markets, organized crime and police states.

The important lesson from this is that the government needs to mind it's own business – at home and abroad.

10:20 PM

  **Dedicated Dad said...**

PLEASE don't bow down to their intimidation. If ANYONE archived this info, PLEASE send a message to my blog - I'll post it and they can see me in court.

This is CRITICAL, people - the LE Agencies are plainly and obviously accessing this GPS info in an illegal way.

You - as a whistleblower - have great Federal protection. PLEASE re-post the info!!

12:42 AM

  **Dedicated Dad said...**

QUOTE: ...We turned it on the web interface for law enforcement about one year ago last month, and we just passed 8 million requests.

used in *Shy v. Pineda-Moreno, No. 08-30385* archived on August 26, 2010

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... /QUOTE

They gave LE a web interface so they don't have to handle the requests, and since doing so they've had 8 million requests which they say they'd never be able to handle.

Ergo, NOBODY at sprint is doing ANY gatekeeping – based on this quote it seems plain that (some, at least) cops can access the data at will.

Explain how this is inaccurate if you can! The explanation offered on the blog update is weasel-wording at its finest. So, maybe it was only thousands of customers - still, WHO IS THE GATEKEEPER ENSURING WARRANTS ARE PROPER BEFORE RELEASING THE DATA TO LE AGENCIES??!!

Answer: Nobody.

As was said above: NEVER give any government any power you don't want a despot to have. In this case, Despots already DO have it...

God help us, and GOD SAVE OUR REPUBLIC!

12:59 AM

  **Stan said...**

Hmmm. This is graduate work? The research lacks contextual restrictions. For example. Sprint lists 8 million hits and you conclude oversight. How many of the requests from law enforcement were as a result of customers hitting 911 on their phone. This would constitute consensual GPS tracking. See the FCC and enhanced 911 services.

1:08 PM

 **Anonymous said...**

Hey Chris. Wanna story from someone whom they have surveilled for ten years or better, following them to grocery stores, Law Schools, family visits, the dentist? Ten years and no action other than to sneak behind, maligning them to their associates and community, furtively and maliciously. Dude has five journals, and videos and photographs of their stupid, visible activities. Post a contact point, I'll reach you.

5:32 PM

 **Anonymous said...**

Another interesting point, presumably professional "bad guys" (terrorists, spies, what have you) know to buy prepaid phones. You can get one of these with cash so that it isn't associated with you. So regardless of whether the phone is being tracked, they don't know who is using it.

This is relevant because I suspect the public justification for this violation of basic constitutional rights would be "we have to catch terrorists before they nuke a major city". They're really only going to locate amateurs with this.

10:46 PM

 **Anonymous said...**

Stan made a good observation about context. (Not that we should ignore the findings here altogether.) I would like to see a response from Chris. Academic debate is a two way street!

1:27 AM

cited in *Pinella Morero, No. 08-10385 archived on August 26, 2010*

 **Renee Sieber said...**

Locational privacy and geographic information systems are two of my specialties. So please allow me to correct a point that you and the telcoms have got wrong. What they are talking about is technically NOT GPS. It is cellphone triangulation. Likely the term GPS is being used because it is better understood by the telcom employees and their law enforcement users. However, the tracking does not rely on global positioning satellites to track individuals and does not require a GPS-enabled cell phone (the GPS-enabled device and the satellite are two of the three required components of the global positioning systems).

The distinction is important. Any phone will do. You don't need a smart phone or a phone with a GPS unit built in. The tracking will work in any location where cell phones can get a signal. That is, the tracking won't work in a remote area with no coverage. It works very well in urban areas where there's good coverage. Ironically, places where GPS work well—in remote areas—triangulation works poorly. Places where triangulation works well—in urban areas—GPS works poorly. There's lots of bounce off of buildings in an urban area that bias the signal. Plus you cannot get a GPS signal inside a building (note that you can get relative locations but that's not the same and not nearly as accurate).

In some sense, this is just an irritating minor difference: both technologies are used for geolocation and tracking. Conversely, the coverages/ accuracies are different and people might think that they're protected because they don't have a GPS-enabled phone when they are just as exposed as anyone with a cellphone.

11:50 AM

 **Galen said...**

First I would like to thank Mr. Soghoian for publishing this data. To turn the law enforcement advocates own words against them: "Why are you worried if you don't have anything to hide?"

Next I'd like to address two points raised in previous comments. The first is in quibbles with the "8 million" figure, with the argument that the actual number of people affected is much less. Mr. Soghoian never makes a claim as to how many people are affected, he simply published the data he had on number of requests. Telecoms are more than welcome to release additional details about this data if they feel that this article is somehow misleading.

Second, modern e-911 systems have no need for a phone in or web based portal to track GPS locations. Current technology allows the dispatch center to pull this information directly from the customer's phone. While a quick internet search didn't yield any hard numbers, anecdotally it appears that e-911 has reached all but the most rural areas. (I am an emergency services provider in a medium-sized metropolitan area that is bordered by rural counties.) Further detracting from this argument is the fact that this 8 million number is specifically attributed to a "web interface for law enforcement" with no mention of any incidental, non surveillance uses (like a 911 location request.) As such, I would very much doubt that legitimate 911 location traces make up any significant portion of these requests.

1:02 PM

 **Edward Hasbrouck said...**

Thanks for pursuing this.

Another unreported source of location info obtainable (and routinely obtained in unknown volume) by law enforcement is travel reservation records. These can be provided "voluntarily" either by travel services providers (airlines, etc.) or by the Computerized Reservation Systems (CRS's or GDS's) to which airlines, travel agencies, and other travel companies outsource hosting of both their reservations and CRM databases.

Cited in U.S. v. Pineda-Moreno, No. 08-36385 archived on August 26, 2010

The difference is that while telco records are subject to *some* legal protection, travel records in the USA are subject to none at all. They are considered entirely the property of travel companies, which can give or sell them "voluntarily" to anyone, including any government worldwide, without any customer knowledge or consent or reporting requirement.

How much do DHS and other agencies pay airlines and Sabre, Amadeus, and the Wordspan and Galileo divisions of Travelport each year for record retrieval?

http://hasbrouck.org/articles/Hasbrouck_et_al-FTC-6NOV2009.pdf

4:42 PM

Anonymous said...

Chris,

We should talk.

<http://www.modernhealthcare.com/article/20081013/REG/310139987>

Joe

9:37 PM

Anonymous said...

Good work but one clarification: When sprint nextel (or any telcom) fulfills subpoenas for historical data, those subpoenas are not solely from law enforcement, they also are from defense lawyers in criminal cases, parties in civil lawsuits, parties engaged in other legal actions. So the number of staff needed to fulfill subpoenas for the historical data is not entirely for law enforcement.

The real time data is an entirely different story - it would all be for law enforcement, as you said.

8:41 AM

Anonymous said...

Thanks Chris for your efforts. I enjoy reading them. I am never surprised by findings like this. Next time you receive a phone call by someone asserting to be a member of a group wanting your content suppressed, make sure you ask for it in writing on official letterhead of said organization. We as a citizenry have to push back and demand a RETURN to the privacy that our country was founded on. Government and Corporate collusion are eroding all rights a person has to privacy. To take the assumption a bit further, I could "borrow" your cell phone, commit a crime with it, and return it to you. Tag! You're guilty!

10:05 AM

Anonymous said...

You mention your interest in surveillance capabilities that are detectable by the person who is tapped. See this in the Sprint-spy document, section 7.

"In order to access stored voicemail, the subscriber's password must be reset/changed by Sprint. When the password is changed, the subscriber will not be able to access his/her voicemail and this procedure is not transparent to the subscriber."

11:15 AM

Anonymous said...

You should point out the actual sections of the code that mandate oversight.

You should also point out that certain states, such as California, allow people to obtain when data is disclosed.

cited in U.S. v. Pineda-Moreno, No. 09-100385 archived on August 26, 2010

As for your thesis, I do agree. 8 million gps request for a single carrier for a year is simply obscene to say the least.

1:50 PM

 **Anonymous said...**

Don't get bullied. No need to make "good faith" gestures to organizations that would not make them to you. Does anyone really believe that copyright law covers the sort of recording of a meeting in question? Lawyers bullshit and bluff all the time; if they really had DMCA rights, they would issue the demand to the corporation HOSTING the materials, not you.

Good luck!

8:39 PM

 **Ryan M. Ferris said...**

Great Post. I linked to it in my blog: <http://thinking-about-network-security.blogspot.com/>.

How many network security types like myself carry around devices on their person they don't have root access to? Answer: All of us...

10:17 PM

 **Anonymous said...**

You need to brush up on your knowledge of copyright law: the recordings were in no way covered by copyright.

8:47 PM

 **Anonymous said...**

Just a guess at the redacted section: "Our pricing schedules reveal (for just two examples) that upon the lawful request of law enforcement we are able to [prolong service on delinquent accounts or activate additional services on the user's device];"

9:40 PM

 **Anonymous said...**

I'm in the process of writing a book about surveillance. I'm particularly looking for anecdotal examples of surveillance operations that have gone bad and had some type of distasteful/disastrous result for the person. You might think of this as when cops/law enforcement or intelligence groups have abused the system. I'm specifically looking for actual examples. Please forward any info to research@integrity-investigations.com. If you would leave your contact information it would be greatly appreciated so that I can validate the details.

9:56 AM

 **MILENARIO said...**

A tragic, creepy world we'll inherit to our children if we let things go that way

10:09 AM

 **Antifascist said...**

Excellent research, Chris! Check out the piece I wrote on the information you gleaned from these goofs on my blog, Antifascist Calling <http://antifascist-calling.blogspot.com/2009/12/following-money-trail-telecoms-and-isps.html>

I highly recommend that privacy researchers, particularly those who have a handle on shady business practices, do more work on the groups behind ISS World. What I was able to discover was startling to say the least. I'm adding Slight Paranoia to my blog roll.

Keep up the great work!

cited in U.S. v. Pineda-Moreno, No. 09-0385 archived on August 26, 2010

7:41 PM

GPS Jammer said...

Never a better time to consider using a GPS jammer.

11:42 AM

Anonymous said...

why dont you use wikileaks!!

12:41 AM

Anonymous said...

Thought provoking, detailed - excellent stuff. Best of luck with the dissertation.

While with a slightly different focus, zerothedge dot com looks at some similarly "unreported" or undisclosed news on a daily basis, and could perhaps serve as inspiration/source of contacts useful to this particular line of investigation.

11:18 PM

Worked both Sides said...

Chris,

I find your entire post and 99% of the responses to it absolutely comical. First of all law enforcement doesn't have the time, desire, budget or manpower to surveil anywhere near the amount of targets you and most of your paranoid readers might suspect. So the targets they are surveiling they are surveiling for good reason and that is two fold; first it assists in bringing law breakers to justice; and second it does help to protect the public when valuable information is obtained that may prevent the death of innocent people at the hands of criminals. Geolocation pings are also used to find kidnap victims and even lost hikers and hunters - those stats weren't considered in your post by your paranoid readers.

As for the value you all seem to find in "knowing" how many people are targets of electronic surveillance/wiretaps there are - the only thing it might help you figure out is if everyone is being surveilled then you must be one of them - and that simply is not the case - see the statement above about time, money, resources etc.....

What I find really interesting is that your purpose in posting this was to glean information for your thesis. I have to say I don't really think you got what you bargained for. Mostly ata-boys with no real meat for you to include. You got a bunch of privacy advocates who would throw caution to the wind and over expose the majority of the population, who aren't as concerned about their privacy, to potentially dangerous consequences should wiretapping, pen trap, and geolocation tools be removed from law enforcements tool kit.

This sort of garbage has the same smack to it that news programs use to tell an enemy when and where we are going to strike - all in the name of FOI.

One other thing - pen/trap, Title III and FISA all need court approval. Yes there are different levels that need to be met for each to be issued but it is as it should be. If the same levels were needed for all then there would only be one type of order issued and that would be one for EVERYTHING and that is not the case today. Either criminal court orders or FIS Court orders can be for either P/T or P/T & Title III. Pen/Trap is call identifying information only - requiring a lesser standard and Title III is for content requiring a greater standard.

As for certain agencies not reporting pen/trap or wiretap numbers to the government well that maybe is an issue but albeit a very minor one. If you consider the number of people in this country and the numbers that have been reported you would have to times those numbers by one million to even make privacy rights

Quoted in U.S. v. Pineda-Moreno, No. 08-30365 archived on August 26, 2010

even an issue for the entire population of the US. To imply that because the numbers reported are low that there must be unauthorized pen/trap and wiretaps occurring is silly and screams of the "sky is falling" logic. From the carrier side I can say that nothing is turned up without proper legal process being served by a court. For records requests - valid legal process is also required.

5:25 PM

Anonymous said...

@ Worked Both Sides

Jealous much?

1:46 PM

Anonymous said...

I found the link to this post at cryptome.com. It seems, you're not the only one that got the "copyright infringement" warning message. (I call it a damage control tactic.)

As I recall, an exception clause exists in the copyright laws pertaining to material shared (published, broadcasted) for "educational purposes." I believe that this includes using such information for educational essays and thesis if you name the original source(s).

Did they provide you with absolute "proof" that the information which you shared was specifically given an official copyright protection? If so, they ought to be able to prove it by sending a copy of it to you. See how John Young at cryptome.org handled a similar situation with someone representing Yahoo.com:

<http://cryptome.org/0001/yahoo-cryptome.htm>

6:47 AM

annunci said...

I fully agree with you

3:34 AM

cited in U.S. v. Pineda-Moreno, No. 08-30385 archived on August 26, 2010

Anonymous said...

If you made the recording, you own the copyright on it. Material is not copyrightable until it is fixed in the form of media. The person who does that owns the copyright. Don't let them bully you, they can't claim copyright on words uttered at a meeting.

11:47 AM

Anonymous said...

and how many after-the-fact cell tower tracking requests were made in the same year, ANOTHER MILLION? The telephone companies can't keep up. up.

9:36 AM

Anonymous said...

i assume you are following the recent Federal Appeals case where the feds are pushing for the warrantless tracking of cellphones:

http://news.cnet.com/8301-13578_3-10451518-38.html?tag=rtcol;pop

a quote:

"the Obama administration has argued that warrantless tracking is permitted because Americans enjoy no "reasonable expectation of privacy" in their—or at least their cell phones'— whereabouts. U.S. Department of Justice lawyers say that "a customer's Fourth Amendment rights are not violated when the phone company reveals to the government its own records" that show where a mobile device placed and received calls.

4:56 AM

Anonymous said...

The FBI and the Justice Department push for warrantless tracking of cell phones in Federal Appeals Court:

http://news.cnet.com/8301-13578_3-10451518-38.html

I think this is pertinent to the posting and would like it if you posted it please.

1:44 AM

Anonymous said...

Question, are we as subscribers to the cell phone services permitted to request information on whether or not our cell phones have been "pinged" ?

10:26 AM

Anonymous said...

I worked for a compliance center for about 6 months and I would process on average 30 subpoenas a day. That's just one person, one company. These centers operate 24 hours a day so imagine what is going on.

1:44 PM

[Post a Comment](#)

[Newer Post](#)

[Home](#)

[Older Post](#)

Subscribe to: [Post Comments \(Atom\)](#)

cited in U.S. v. Pineda-Moreno, No. 08-30385 archived on August 26, 2010