

NSA's Spying On Metadata Violates Our Freedom of Association

By [Washington's Blog](#)

Global Research, September 28, 2013

[Washington's Blog](#)

Region: [USA](#)

Theme: [Intelligence](#), [Police State & Civil Rights](#)

Why You Should You Care If the Government Spies On Your Metadata

The government has sought to “reassure” us that it is only tracking “metadata” such as the time and place of the calls, and [not the actual content of the calls](#).

But technology experts say that “metadata” can be **more revealing** than the content of your actual phone calls.

For example, the ACLU [notes](#):

A Massachusetts Institute of Technology study a few years back [found](#) that reviewing people’s social networking contacts alone was sufficient to [determine their sexual orientation](#). Consider, metadata from [email communications](#) was sufficient to [identify the mistress](#) of then-CIA Director David Petraeus and then drive him out of office.

The “who,” “when” and “how frequently” of communications are often **more revealing** than what is said or written. **Calls between a reporter and a government whistleblower**, for example, may reveal a relationship that can be incriminating all on its own.

Repeated calls to **Alcoholics Anonymous, hotlines for gay teens, abortion clinics or a gambling bookie** may tell you all you need to know about a person’s problems. If a politician were revealed to have repeatedly called a **phone sex hotline** after 2:00 a.m., no one would need to know what was said on the call before drawing conclusions. In addition sophisticated data-mining technologies have compounded the privacy implications by allowing the government to analyze terabytes of metadata and reveal far more details about a person’s life than ever before.

The Electronic Frontier Foundation [points out](#):

What [government officials] are trying to say is that disclosure of metadata—the details about phone calls, without the actual voice—isn’t a big deal, not something for Americans to get upset about if the government knows. Let’s take a closer look at what they are saying:

- They know you rang a **phone sex service** at 2:24 am and spoke for 18 minutes. But they don’t know what you talked about.
- They know you called the **suicide prevention hotline** from the Golden Gate Bridge. But the topic of the call remains a secret.

- They know you spoke with an **HIV** testing service, then your doctor, then your health insurance company in the same hour. But they don't know what was discussed.
- They know you received a call from the local **NRA** office while it was having a campaign against gun legislation, and then called your senators and congressional representatives immediately after. But the content of those calls remains safe from government intrusion.
- They know you called a gynecologist, spoke for a half hour, and then called the local **Planned Parenthood's** number later that day. But nobody knows what you spoke about.

Sorry, your phone records—oops, “so-called metadata”—can reveal a lot more about the content of your calls than the government is implying. Metadata provides enough context to know some of the most intimate details of your lives. And the government has given no assurances that this data will never be correlated with other easily obtained data.

New York Magazine [explains](#):

“When you take all those records of who’s communicating with who, **you can build social networks and communities for everyone in the world,**” mathematician and NSA [whistle-blower](#) William Binney — “one of the best analysts in history,” who left the agency in 2001 amid privacy concerns — told Daily Intelligencer. “And when you marry it up with the content,” which he is convinced the NSA is collecting as well, “you have leverage against everybody in the country.”

“You are unique in the world,” Binney explained, based on the identifying attributes of the machines you use. “If I want to know who’s in the tea party, I can put together the metadata and see who’s communicating with who. I can construct the network of the tea party. If I want to pass that data to the IRS, then I can do that. That’s the danger here.”

At [The New Yorker](#), Jane Mayer quoted mathematician and engineer Susan Landau’s hypothetical: “For example, she said, in the world of business, **a pattern of phone calls from key executives can reveal impending corporate takeovers.** Personal phone calls can also reveal sensitive medical information: ‘You can see **a call to a gynecologist, and then a call to an oncologist, and then a call to close family members.**’” [Landau gives a more detailed explanation [here](#).]

“There’s a lot you can infer,” Binney continued. “**If you’re calling a physician and he’s a heart specialist, you can infer someone is having heart problems.** It’s all in the databases.” The data, he said, is “all compiled by code. The software does it all from the beginning — they have dossiers of everyone in the country. That’s done automatically. When you want to investigate or target somebody, a human becomes involved.”

“The public doesn’t understand,” Landau told Mayer. “It’s **much more intrusive than content.**”

The Guardian [reports](#):

The information collected on the AP [in the recent scandal regarding the government spying on reporters] was telephony metadata: precisely what the court order against Verizon shows is being collected by the NSA on millions of Americans every day.

Discussing the use of GPS data collected from mobile phones, an [appellate court noted](#) that even location information on its own could reveal a person’s secrets: “A person who knows all of another’s travels **can deduce whether he is a weekly churchgoer, a heavy drinker, a regular at the gym, an unfaithful husband, an outpatient receiving medical treatment, an associate of particular individuals or political groups,**” it read, “and not just one such fact about a person, but all such facts.”

ARS Technica [noted](#) last month:

The ACLU filed a [declaration](#) by Princeton Computer Science Prof. Edward Felten to support its quest for a preliminary injunction in that lawsuit. Felten, a former technical director of the Federal Trade Commission, has testified to Congress several times on technology issues, and he explained why “metadata” really is a big deal.

There are already programs that make it easy for law enforcement and intelligence agencies to analyze such data, like IBM’s Analyst’s Notebook. IBM offers [courses](#) on how to use Analyst’s Notebook to understand call data better.



Figure 1: Screenshot of IBM's Analyst Notebook.²²

Court Documents

Unlike the actual contents of calls and e-mails, the metadata about those calls often can't be hidden. And it can be incredibly revealing—sometimes **more so than the actual content**.

Knowing who you're calling reveals information that isn't supposed to be public. Inspectors general at nearly every federal agency, including the NSA, "have hotlines through which misconduct, waste, and fraud can be reported." Hotlines exist for people who suffer from addictions to alcohol, drugs, or gambling; for victims of rape and domestic violence; and for people considering suicide.

Text messages can measure donations to churches, to Planned Parenthood, or to a particular political candidate.

Felten points out what should be obvious to those arguing "it's just metadata"—the most important piece of information in these situations is the recipient of the call.

The metadata gets more powerful as you collect it in bulk. For instance, showing a call to a bookie means a surveillance target probably made a bet. But "analysis of metadata over time could reveal that the target has a gambling problem, particularly if the call records also reveal a number of calls made to payday loan services."

The data can even reveal the most intimate details about people's romantic lives. Felten writes:

Consider the following hypothetical example: A young woman calls her gynecologist; then immediately calls her mother; then a man who, during the past few months, she had repeatedly spoken to on the telephone after 11pm; followed by a call to a family

planning center that also offers abortions. A likely storyline emerges that would not be as evident by examining the record of a single telephone call.

With a five-year database of telephony data, these patterns can be evinced with “even the most basic analytic techniques,” he notes.

By collecting data from the ACLU in particular, the government could identify the “John Does” in the organization’s lawsuits that have John Doe plaintiffs. They could expose litigation strategy by revealing that the ACLU was calling registered sex offenders, or parents of students of color in a particular school district, or people linked to a protest movement.

Indeed, the government’s spying on our metadata violates our right to freedom of expression, [guaranteed by numerous laws and charters](#) including the U.S. Constitution, the European Convention on Human Rights, the Canadian Charter of Rights and Freedoms, and international law, including articles 20 and 23 of the Universal Declaration of Human Rights, and Conventions 87 and 98 of the International Labor Organization.

Remember, a U.S. federal judge found that the statute allowing indefinite detention of Americans without due process has a [“chilling effect” on free speech](#). Top reporters have said that they are [less likely to interview controversial people, for fear of being accused](#) of “supporting” terrorists.

Given the [insanely broad list of actions and beliefs](#) which may get one labeled as a “potential terrorist” by local, state or federal law enforcement, the free association of Americans is being chilled. For example, people may be less willing to call their niece calling to end the Fed, their Occupy-attending aunt, their Tea Party-promoting cousin, their anti-war teacher, or their anti-fracking uncle.

Foreign Policy reported this week that [metadata may not catch terrorists, but it’s great at busting journalists and their sources](#):

The National Security Agency says that the telephone [metadata](#) it collects on every American is essential for finding terrorists. And [that’s debatable](#). [Indeed, top counter-terrorism experts say that all of this spying [doesn’t keep us safe](#), and that it actually [hurts U.S. counter-terror efforts](#) (more [here](#) and [here](#)).] But this we know for sure: Metadata is very useful for tracking journalists and discovering their sources.

On Monday, a former FBI agent and bomb technician pleaded [guilty](#) to leaking classified information to the Associated Press about a successful CIA operation in Yemen. As it turns out, phone metadata was the key to finding him.

The real reason the government is going after leakers is because it can. Investigators today have greater access to phone records and e-mails than they did before Obama took office, allowing them to follow digital data trails straight to the source.

In a highly controversial move, investigators secretly obtained a subpoena for phone records of AP reporters and editors.

Once investigators looked at that phone metadata, they got their big break in the case.

It's no wonder that the Obama administration is going after leakers so often. Metadata is the closest thing to a smoking gun that they're likely to have, absent a wiretap or a copy of an email in which the source is clearly seen giving a reporter classified information.

If you're looking for a case study in the power of metadata, you've found it.

Top experts have said that mass surveillance sets up the technological framework [allowing for "turnkey tyranny"](#).

Spying on Americans' metadata destroys our constitutional right to freedom of association ... and virtually everything the Founding Fathers fought for.

Indeed, computer experts have used an analogy to explain how powerful metadata is: the English monarchy could have stopped the Founding Fathers in their tracks [if they only possessed "metadata" regarding which colonist talked to whom](#).

Postscript: The government is - [in fact](#)- [gathering content](#), and [not just metadata](#).

The original source of this article is [Washington's Blog](#)
Copyright © [Washington's Blog](#), [Washington's Blog](#), 2013

[Comment on Global Research Articles on our Facebook page](#)

[Become a Member of Global Research](#)

Articles by: [Washington's Blog](#)

Disclaimer: The contents of this article are of sole responsibility of the author(s). The Centre for Research on Globalization will not be responsible for any inaccurate or incorrect statement in this article. The Centre of Research on Globalization grants permission to cross-post Global Research articles on community internet sites as long the source and copyright are acknowledged together with a hyperlink to the original Global Research article. For publication of Global Research articles in print or other forms including commercial internet sites, contact: publications@globalresearch.ca

www.globalresearch.ca contains copyrighted material the use of which has not always been specifically authorized by the copyright owner. We are making such material available to our readers under the provisions of "fair use" in an effort to advance a better understanding of political, economic and social issues. The material on this site is distributed without profit to those who have expressed a prior interest in receiving it for research and educational purposes. If you wish to use copyrighted material for purposes other than "fair use" you must request permission from the copyright owner.

For media inquiries: publications@globalresearch.ca