


Take Back the Net: Practical Countersurveillance

Teaching your mom, dad, cat, and dog how to protect their privacy online

Lisa Lorenzin
edited and presented by:
Maryam Abkar

Google





He sees you when
you're sleeping.
He knows when
you're awake.
He knows if you've
been bad or good.

**You need to change your
Facebook privacy settings.**

FP TECH DESK

TRENDING

[Taxes](#) | [Housing Market](#) | [BlackBerry](#) | [Loonie](#) | [Mortgages](#) | [Keystone XL Pipeline](#) | [GM](#)

Google to Gmail users: We scan all of your emails

NP

ALEXEI ORESKOVIC, **REUTERS** | April 17, 2014 | Last Updated: Apr 17 9:37 AM ET

[More from Reuters](#)



NSA uses Google cookies to pinpoint targets for hacking



By Ashkan Soltani, Andrea Peterson, and Barton Gellman

December 10, 2013

Our Approach

- Tracked target's converged communications and CNE accesses.
- Monitored passive internet traffic; created automated processes where possible (XKS ANCHORMAN, Workflows, Fingerprints).
- Provided TAO/GCHQ with WLLids/DSL accounts, Cookies, GooglePREFIDs to enable remote exploitation.
- Partnered with NGA and R4 to confirm locations and USRP equipment based on collected photographs.
- Drove CNE collection and partnered with TAO to increase USRP specific endpoint accesses.
- Provided knowledge to interagency partners for potential on the ground survey options and FBI-led intelligence guiding efforts.



A slide from an internal NSA presentation indicating that the agency uses at least one Google cookie as a way to identify targets for exploitation. (Washington Post)

Most Read [Business](#)



U S A

The Three Laws of Thermodynamics:

- 1. You can't win.*
- 2. You can't break even.*
- 3. You can't quit the game.*



“When we think about what is happening at the NSA for the past decade, the result has been an adversarial internet - a sort of global free fire zone for governments that is nothing that we ever asked for. It is not what we want. It is something that we need to protect against.”

- Edward Snowden



“The IETF should never again
approve a protocol that sends
plaintext over the Internet.”

- Ian Goldberg



A Guardian guide to your

metadata

Metadata is information generated as you use technology, and its use has been the subject of controversy since NSA's secret surveillance program was revealed. Examples include the date and time you called somebody or the location from which you last accessed your email. The data collected generally does not contain personal or content-specific details, but rather transactional information about the user, the device and activities taking place. In some cases you can limit the information that is collected – by turning off location services on your cell phone for instance – but many times you cannot. Below, explore some of the data collected through activities you do every day

Choose the services you use in a day



Email



Phone



Camera



Facebook



Twitter



Search



Web browser

Tweet

Share

Reset

'We Kill People Based on Metadata'

David Cole



Rick Bowmer/AP Photo

The National Security Agency's \$1.5 billion data storage facility in Bluffdale, Utah, June 2013

Supporters of the National Security Agency inevitably defend its sweeping collection of phone and Internet records on the ground that it is only collecting so-called “metadata”—who you call, when you call, how long you talk. Since this does not include the actual content of the communications, the threat to privacy is said to be negligible. That argument is profoundly misleading.

Of course knowing the content of a call can be crucial to establishing a particular threat. But metadata alone can provide an extremely detailed picture of a person’s most intimate associations and interests, and it’s actually much easier as a technological matter to search huge amounts of metadata than to listen to millions of phone calls. As NSA General Counsel Stewart Baker has said, “metadata absolutely tells you everything about somebody’s life. If you have enough metadata, you don’t really need content.” When I quoted Baker at a recent debate at Johns Hopkins University, my opponent, General Michael Hayden, former director of the NSA and the CIA, called Baker’s comment “absolutely correct,” and raised him one, asserting, “We kill people based on metadata.”

Meet Executive Order 12333: The Reagan rule that lets the NSA spy on Americans

by John Napier Tye • July 18, 2014 • 6 min read • [original](#)

John Napier Tye served as section chief for Internet freedom in the State Department's Bureau of Democracy, Human Rights and Labor from January 2011 to April 2014. He is now a legal director of [Avaaz](#), a global advocacy organization.

In March I received a call from the White House counsel's office regarding a speech I had prepared for my boss at the State Department. The [speech](#) was about the impact that the disclosure of National Security Agency surveillance practices would have on U.S. Internet freedom policies. The draft stated that "if U.S. citizens disagree with congressional and executive branch determinations about the proper scope of signals intelligence activities, they have the opportunity to change the policy through our democratic process."



HOME

ABOUT

OUR WORK

DEEPLINKS BLOG

PRESS ROOM

JUNE 11, 2013 | BY KURT OPSAHL AND TREVOR TIMM



The NSA's Word Games Explained: How the Government Deceived Congress in the Debate over Surveillance Powers

ANDREA MITCHELL: "Why do you need every telephone number? Why is it such a broad vacuum cleaner approach?"

JAMES CLAPPER: "Well, you have to start someplace."—NBC Meet the Press, this past Sunday

Concerned about the surveillance of millions of ordinary Americans, last year Senator **Ron Wyden** asked Director of National Intelligence **James Clapper, Jr.** a simple question: "Does the NSA collect any type of data at all on millions or hundreds of millions of Americans?"

Wyden had good reason to worry. As a member of the intelligence committee he had access to classified information and had been warning from the Senate floor that the **American people would be "shocked"** to find out how the government was interpreting the FISA Amendments Act and the PATRIOT Act in secret.

DNI Clapper's answer was simple: "No, sir ... not wittingly."



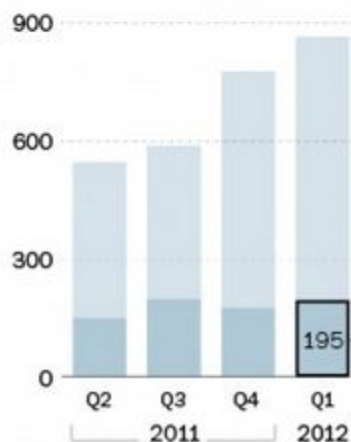
NSA broke privacy rules thousands of times per year, audit finds



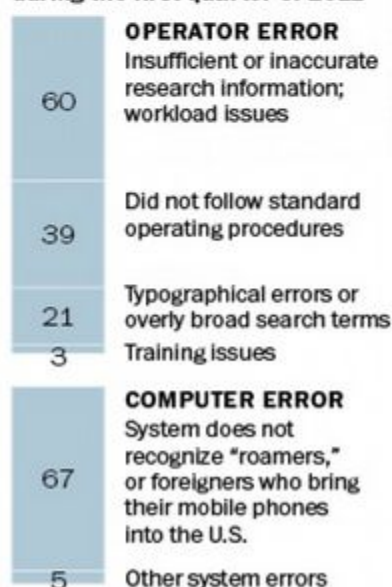
An internal NSA audit, dated May 2012, identifies **2,776 "Incidents,"** or violations of the rules or court orders for surveillance of Americans or foreign targets in the United States, from April 2011 through March 2012.

Quarterly violations, by authority

■ Presidential executive order violations
■ Foreign Intelligence Surveillance Act violations



Reasons for the FISA violations during the first quarter of 2012



Most Read [World](#)



#NSA KILLED MY INTERNET



NOW I HAVE TO BUILD A GNU ONE





ELECTRONIC FRONTIER FOUNDATION
DEFENDING YOUR RIGHTS IN THE DIGITAL WORLD

[HOME](#)[ABOUT](#)[OUR WORK](#)[DEEPLINKS BLOG](#)[PRESS ROOM](#)

HTTPS Everywhere

[HTTPS Everywhere](#)[FAQ](#)[Report Bugs / Hack On
The Code](#)[Creating HTTPS
Everywhere Rulesets](#)[How to Deploy HTTPS
Correctly](#)

HTTPS Everywhere is a Firefox, Chrome, and Opera extension that encrypts your communications with many major websites, making your browsing more secure. **Encrypt the web: Install HTTPS Everywhere today.**



Installed in Firefox
Version 3 Stable



Entering private browsing. As soon as you close this tab, all the information connected with it will be erased. [Learn more](#)



Private Browsing

Firefox won't remember any history for this window.





Duck Duck Go

The search engine that doesn't track you.

[See what's next!](#)



A PROJECT OF THE ELECTRONIC FRONTIER FOUNDATION



Privacy Badger



GHOSTERY

WORKS FOR OPENDNS

SysAdmin

OpenDNS

**I LOVE
DNS**
FASTER SAFER
MOST SECURE
BETTER

PINGS 8.8.8.8

Whisper & Wickr





Fork us on GitHub!

Need some privacy?

SILENCE ENCRYPTS YOUR TEXT MESSAGES OVER THE AIR AND ON YOUR PHONE.

 Send secure SMS



Anonymity Online

Protect your privacy. Defend yourself against network surveillance and traffic analysis.



[Download Tor](#) 

- Tor prevents people from learning your location or browsing habits.
- Tor is for web browsers, instant messaging clients, and more.
- Tor is free and open source for Windows, Mac, Linux/Unix, and Android

What is Tor?

Tor is free software and an open network that helps you defend against traffic analysis, a form of network surveillance that threatens personal freedom and privacy, confidential business activities and relationships, and state security.

[Learn more about Tor »](#)

Why Anonymity Matters

Tor protects you by bouncing your communications around a distributed network of relays run by volunteers all around the world: it prevents somebody watching your Internet connection from learning what sites you visit, and it prevents the sites you visit from learning your physical location.

[Get involved with Tor »](#)



Tails
the **amnesic** incognito **live** system

TECHNOLOGY LAB / INFORMATION TECHNOLOGY

How to run your own e-mail server with your own domain, part 1

Gmail? Apple? The cloud? Forget 'em all—in this series, we take your e-mail back.

by Lee Hutchinson - Feb 17, 2014 2:00 am UTC

INFORMATION TECHNOLOGY 318



GOOGLE HAS MOST OF MY EMAIL BECAUSE IT HAS ALL OF YOURS

🕒 MAY 11, 2014 👤 BENJAMIN MAKO HILL 💬 108 COMMENTS

For almost 15 years, I have run my own email server which I use for all of my non-work correspondence. I do so to keep [autonomy](#), control, and privacy over my email and so that no big company has copies of all of my personal email.

A few years ago, I was surprised to find out that my friend [Peter Eckersley](#) — a very privacy conscious person who is Technology Projects Director at the [EFF](#) — used Gmail. I asked him why he would willingly give Google copies of all his email. Peter pointed out that if all of your friends use Gmail, Google has your email anyway. Any time I email somebody who uses Gmail — and anytime they email me — Google has that email.

Since our conversation, I have often wondered just how much of my email Google really has. This weekend, I wrote a small program to go through all the email I have kept in my personal inbox since April 2004 (when Gmail was started) to find out.



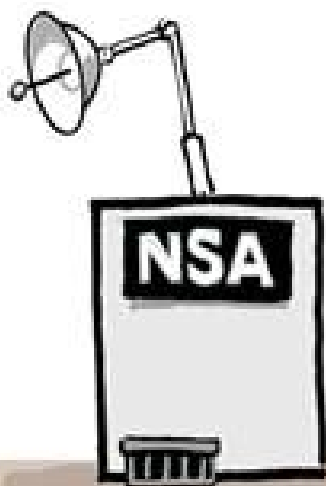
PARANOIA

Just a heightened state of awareness

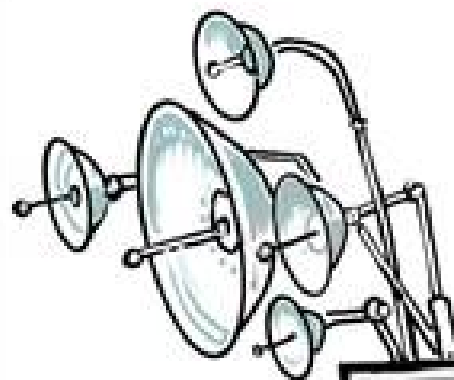


The Three Laws of Thermodynamics:

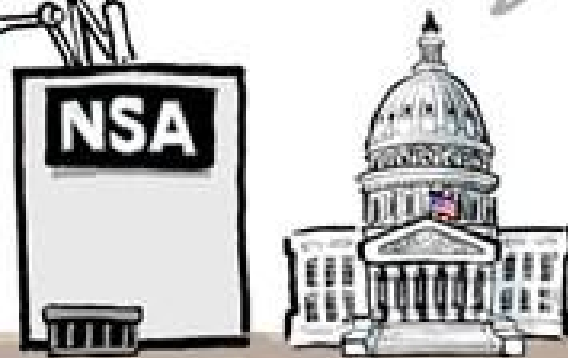
- 1. You can't prevent surveillance.*
- 2. You can make it harder.*
- 3. You can limit what they get.*



Fine.



okie
Dokie.



NO
ProBlemo.



**NOW
HOLD IT
RIGHT
THERE!**





Politics

Application

Presentation

Session

Transport

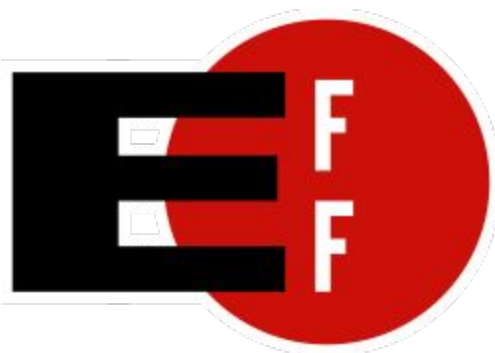
Network

Data Link

Physical



epic.org





Please attribute Lisa Lorenzin.

Take these slides and do something cool with them! Give a talk at your local school, or library, or hackerspace, or company. Add new tools that I haven't heard of yet (and then tell me about them, too! I'm @llorenzin on Twitter). Make a website, write a blog post, host a podcast... And use some of the tools here to protect your privacy and help make the Internet a more safe environment for free speech.

You can find these slides at:

original: https://www.trilug.org/~lisa/Practical_Countersurveillance-ITHotTopics2016-Lorenzin.pptx

edited:

<https://github.com/Freak-of-Nature/conference-slides>

FIN