

Decoding the NSA files

Runa A. Sandvik (@runasand)

TOP SECRET//SI//ORCON//NOFORN



Runa A. Sandvik
Contributor

FOLLOW

*I cover all things
privacy, security and
technology.*

[full bio](#) →


TECH 5/27/2014 @ 2:25PM | 17,588 views

That One Time I Threw A CryptoParty With Edward Snowden

[+ Comment Now](#) [+ Follow Comments](#)

On June 9, 2013, the world learned the identity of an NSA whistleblower who had secretly met with journalists Laura Poitras, Glenn Greenwald and Ewen MacAskill in Hong Kong and given them thousands of documents about the spy agency's mass surveillance programs. The extent to which this young sysadmin would expose the previously secrecy-shrouded NSA was shocking to

See how St
help yo
life back in



1K? 500K? 1.7M?
Even the NSA
doesn't know.



June 5, 2013 – First Snowden disclosure published

The Guardian publishes the first of a series of disclosures exposing the NSA's mass surveillance programs.



The National Security Agency is currently collecting the telephone records of millions of US customers of Verizon, one of America's largest telecoms providers, under a top secret court order issued in April.

The order, a copy of which has been obtained by the Guardian, requires Verizon on an "ongoing, daily basis" to give the NSA information on all telephone calls in its systems, both within the US and between the US and other countries.

✓ June 6, 2013 – The NSA's PRISM program is revealed

The second NSA revelation is published in the Guardian and the Washington Post, revealing the existence...

PRISM/US-984XN
Overview

OR

SIGAD Used Most in NSA Report
Overview

 PRISM Collection Manager, S35333

April 2013


TOP SECRET//SI

TOP SECRET//SI//ORCON//NOFORN



Gmail

facebook



Hotmail

YAHOO!



skype

paltalk.com

YouTube

AOL mail



PRISM/US-984XN Overview

OR

*The SIGAD Used **Most** in NSA Reporting*
Overview



April 2013

Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20360901

TOP SECRET//SI//ORCON//NOFORN



facebook

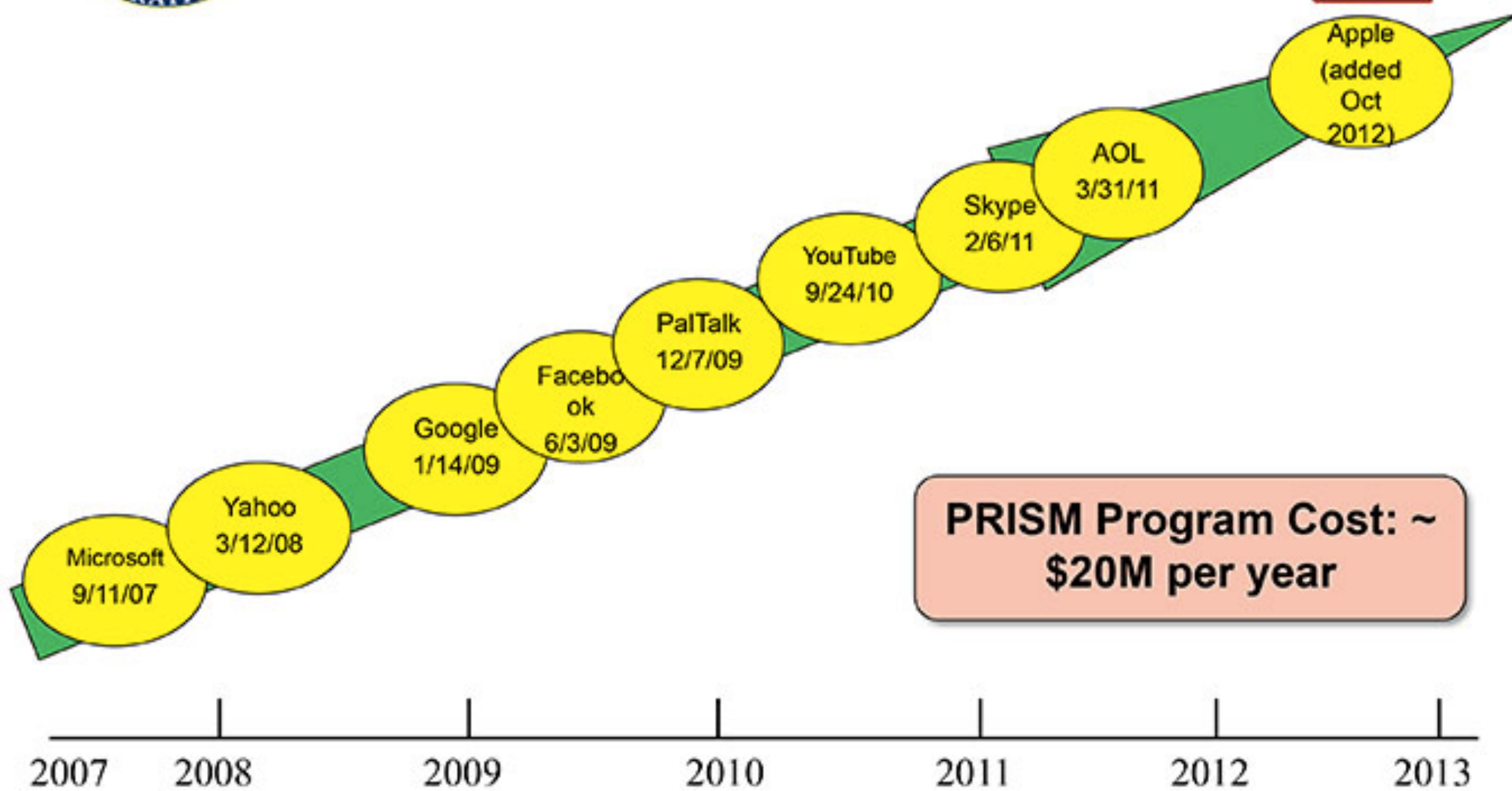


Hotmail

YAHOO!



(TS//SI//NF) Dates When PRISM Collection
Began For Each Provider



PRISM Program Cost: ~
\$20M per year

Series: [Glenn Greenwald on security and liberty](#)

Microsoft handed the NSA access to encrypted messages

- Secret files show scale of Silicon Valley co-operation on [Prism](#)
- Outlook.com encryption unlocked even before official launch
- Skype worked to enable Prism collection of video calls
- Company says it is legally compelled to comply

Glenn Greenwald, Ewen MacAskill, Laura Poitras, Spencer Ackerman and Dominic Rushe

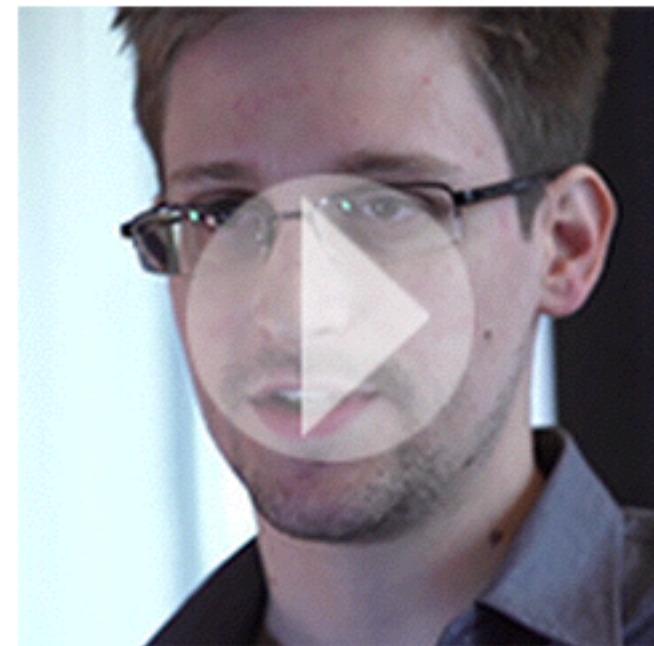
The Guardian, Thursday 11 July 2013

- Content dragnet: can intercept not only communications where a target is a party to a communication, but also communications “about a target.”



June 9, 2013 – Snowden is revealed as NSA whistleblower

The source of the leaks is revealed by the Guardian to be Edward Snowden, a 29-year-old employee of NSA...







August 8, 2013 – NSA searches Americans' international messages

The New York Times reveals that the NSA is "systematically searching" the contents of virtually every email...



Asked to comment, Judith A. Emmel, an N.S.A. spokeswoman, did not directly address surveillance of cross-border communications. But she said the agency's activities were lawful and intended to gather intelligence not about Americans but about "foreign powers and their agents, foreign organizations, foreign persons or international terrorists."

"In carrying out its signals intelligence mission, N.S.A. collects only what it is explicitly authorized to collect," she said. "Moreover, the agency's activities are deployed only in response to requirements for information to protect the country and its interests."

August 15, 2013 – NSA commits thousands of privacy violations for several years

The Washington Post publishes an internal NSA audit from 2012, which reveals that the agency violated the rules supposedly protecting Americans' privacy thousands of times since 2008. In one example, the NSA intercepted "a large number" of calls originating in Washington, D.C., because a programming error confused the D.C. area code, 202, with Egypt's international dialing code.



August 23, 2013 – NSA analysts spy on love interests

The Wall Street Journal [reveals](#) the existence of "LOVEINT," a term coined by NSA employees to describe the practice of spying on love interests. The NSA acknowledges the following month that at least 12 such incidents of improper eavesdropping were known by the agency to have occurred since 2003.



Sept. 5, 2013 – NSA undermines global encryption standards

The Guardian, New York Times, and
Propublica publish coordinated articles
revealing an NSA program called...



TOP SECRET STRAP1

Response to improving security

- For the past decade, NSA has lead an aggressive, multi-pronged effort to break widely used Internet encryption technologies
- Cryptanalytic capabilities are now coming on line
- Vast amounts of encrypted Internet data which have up till now been discarded are now exploitable
- Major new processing systems, SIGDEV efforts and tasking must be put in place to capitalize on this opportunity

PTD "We penetrate targets' defences."



This information is exempt from disclosure under the Freedom of Information Act 2000 and may be subject to exemption under other UK information legislation. Refer disclosure requests to GCHQ on 01242 221491 x30306 (non-sec) or email infoleg@gchq

© Crown Copyright. All rights reserved.



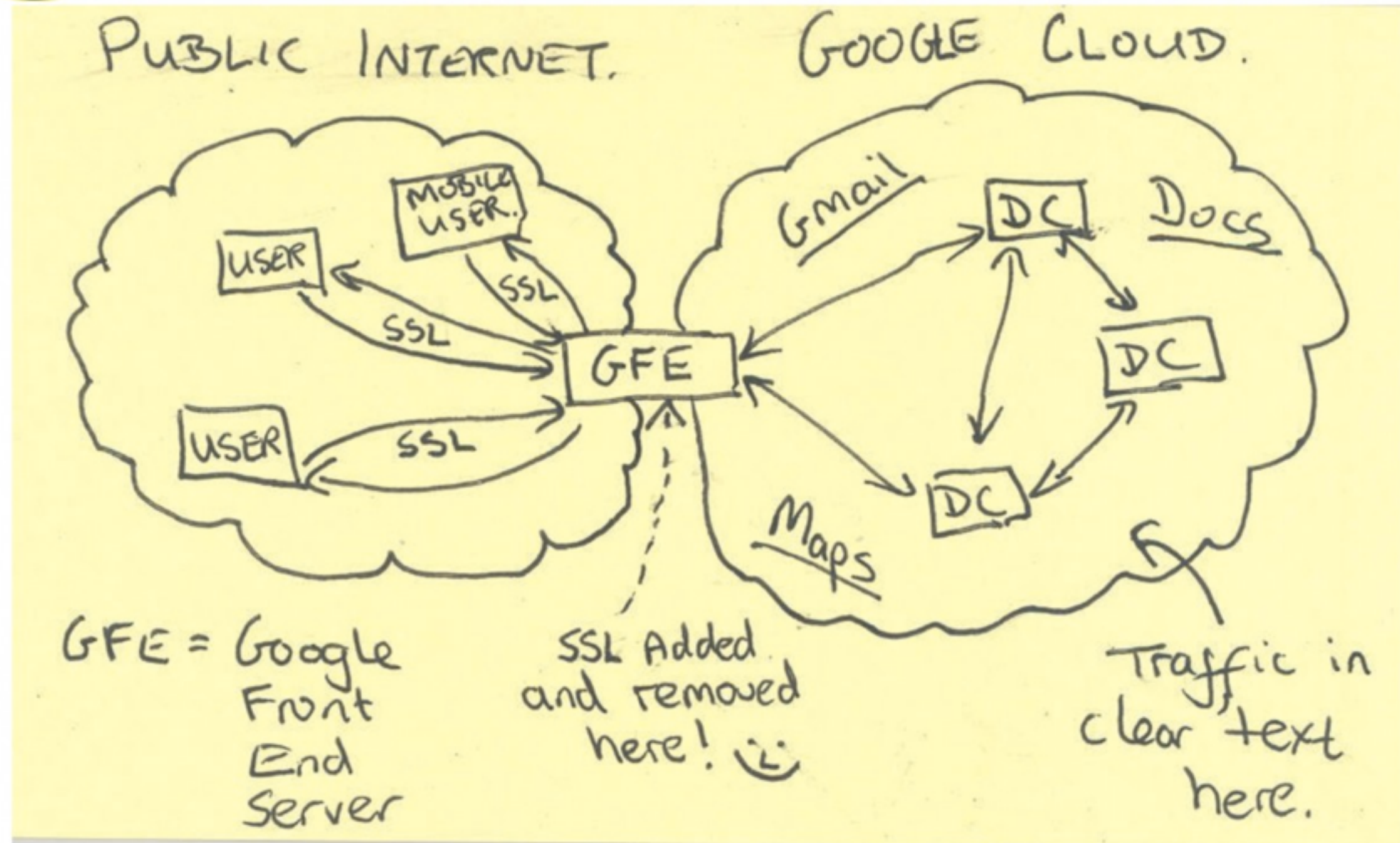
Oct. 30, 2013 – NSA hacks into data centers overseas

The Washington Post publishes a report
revealing that the NSA and GCHQ, its
British counterpart...





Current Efforts - Google



Inside the NSA's Secret Efforts to Hunt and Hack System Administrators

By Ryan Gallagher and Peter Maass

20 Mar 2014, 7:07 PM EDT

384

SECRET // SI // REL TO USA, FVEY

(U) I hunt sys admins

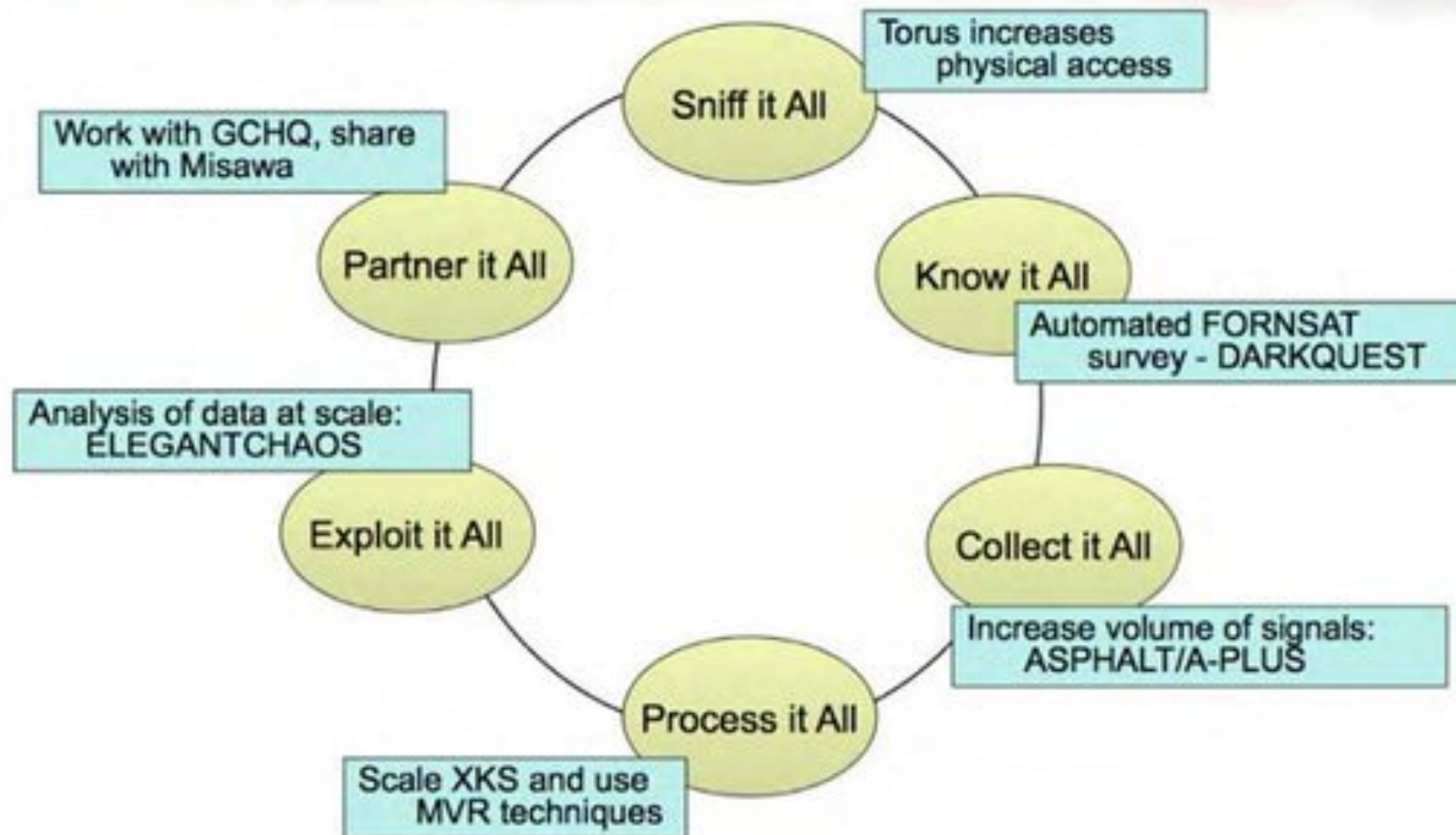
A secret document reveals how the NSA tracks down system administrators for surveillance. Illustration: Josh Begley.

**I STOLE YOUR FACEBOOK LOGIN,
CELLPHONE RECORDS & EMAIL
PASSWORD**

**BUT IT'S COOL, YOU HAVE
NOTHING TO HIDE, RIGHT?**

SECRET//REL TO USA, AUS, CAN, GBR, NZL//20320108

New Collection Posture



SECRET//REL TO USA, AUS, CAN, GBR, NZL//20320108



ALL IS LOST

“Encryption works.”

— Edward Snowden

- Encourage use of encryption tools, such as Tor
- Support encryption by default, even for static sites
- Ask questions, encourage use of FOIA requests
- Encourage transparency, set up SecureDrop

**“We’ve come a long way, but
there’s more to be done.”**

— Edward Snowden

Thank you!

Runa A. Sandvik (@runasand)

Resources

NSA Documents Database (ACLU):

<https://www.aclu.org/nsa-documents-search>

Timeline of NSA revelations (ACLU):

<https://www.aclu.org/they-knew-our-secrets-one-year-later-we-know-theirs>

65 things we know about NSA surveillance (EFF):

<https://www.eff.org/deeplinks/2014/06/65-65-things-we-know-about-nsa-surveillance-we-didnt-know-year-ago>