The 10 Biggest Revelations From Edward Snowden's Leaks

By Lorenzo Franceschi-Bicchierai on June 5, 2014

Former intelligence contractor Edward Snowden poses for a photo during an interview in an undisclosed location in December 2013 in Moscow, Russia. Credit: Barton Gellman/Getty Images

One year ago, the Guardian published its first bombshell story based on leaked top-secret documents showing that the National Security Agency was spying on American citizens.

At the time, journalist Glenn Greenwald and the Guardian never mentioned that they had a treasure trove of other NSA documents, nor that they came from one person. Then

three days later, the source surprisingly unmasked himself: His name was Edward Snowden.

SEE ALSO: Meet the Man Hired to Make Sure the Snowden Docs Aren't Hacked →

Journalist Glenn Greenwald and the Guardian won a Pulitzer Prize for reporting based on Snowden's information.
Credit: John Minchillo

When asked if more revelations were in the pipeline, Greenwald always used to respond that yes, many more were coming -- and he wasn't kidding. Over the next year, explosive stories began to trickle out of those documents. Here are the top 10 revelations of the year.

1. Secret court orders allow NSA to sweep up Americans' phone records

The very first story revealed that Verizon had been providing the NSA with virtually all of its customers' phone records. It soon was revealed that it wasn't just Verizon, but virtually every other telephone company in America.

This revelation is still one of the most controversial ones. Privacy advocates have challenged the legality of the program in court, and one Judge deemed the program unconstitutional and "almost Orwellian," while another one ruled it legal.

The uproar caused by this first story has led President Barack Obama to endorse a reform to the program, and the House of Representatives to pass the first law that tries to change it.

2. PRISM

The existence of PRISM was the second NSA bombshell, coming less than 24 hours after the first one. Initially, reports described PRISM as the NSA's program to directly access the servers of U.S tech giants like Google, Facebook, Microsoft and Apple, among others.

Its reality was slightly different.

PRISM, we soon learned, was less less evil than first thought. In reality, the NSA doesn't have direct access to the servers, but can request user data from the companies, which are compelled by law to comply.

PRISM was perhaps as controversial as the first NSA scoop, prompting technology companies to first deny any knowledge of it, then later fight for the right to be more transparent about government data requests. The companies ended up partially winning that fight, getting the government to ease some restrictions and allow for more transparency.

3. Britain's version of the NSA taps fiber optic cables around the world

The British spy agency, the Government Communications Headquarters (GCHQ), taps fiber optic cables all over the world to intercept data flowing through the global Internet, we learned. The GCHQ works closely with the NSA, sharing data and intelligence in a program that's codenamed Tempora.

Tempora is one of the key NSA/GCHQ programs, allowing the spy agencies to collect vasts troves of data, but for some reason, it has sometimes been overlooked. After a couple of months from the Tempora revelation, a German newspaper revealed the names of the companies that collaborate with the GCHQ in the Tempora program: Verizon Business, British Telecommunications, Vodafone Cable, Global Crossing, Level 3, Viatel and Interoute.

4. NSA spies on foreign countries and world leaders

U.S. President Barack Obama, right, and German Chancellor Angela Merkel are seated together at a G7 dinner in Brussels, on June 4. Their relationship has been tense since reports revealed that the NSA tapped Merkel's phone.

Credit: Charles Dharapak

Over the months, countless stories based on Snowden documents have revealed that the NSA has spied on numerous world leaders and foreign governments.

The German newsweekly Der Spiegel revealed that the NSA targets at least 122 world leaders.

Other stories over the past years have named specific targets like German Chancellor Angela Merkel, Brazil's President Dilma Roussef, and Mexico's former President Felipe Calderon, the French Foreign Ministry, as well as leaders at the 2010 G8 and G20 summits in Toronto.

5. XKeyscore, the program that sees everything

XKeyscore is a tool the NSA uses to search "nearly everything a user does on the Internet" through data it intercepts across the world. In leaked documents, the NSA describes it as the "widest-reaching" system to search through Internet data.

6. NSA efforts to crack encryption and undermine Internet security

Encryption makes data flowing through the Internet unreadable to hackers and spies, making the NSA's surveillance programs less useful. What's the point of tapping fiber optic cables if the data flowing through them is unreadable? That's why the NSA has a developed a series of techniques and tricks to circumvent widely used web encryption technologies.

The NSA, however, isn't able to compromise the encryption algorithms underlying these technologies. Instead, it circumvents or undermines them, forcing companies to install backdoors, hacking into servers and computers, or promoting the use weaker algorithms.

In any case, technologists were alarmed.

"Even as the NSA demands more powers to invade our privacy in the name of cybersecurity, it is making the Internet less secure and exposing us to criminal hacking, foreign espionage, and unlawful surveillance. The NSA's efforts to secretly defeat encryption are recklessly shortsighted and will further erode not only the United States' reputation as a global champion of civil liberties and privacy but the economic competitiveness of its largest companies," Christopher Soghoian, principal technologist at the American Civil Liberties Union (ACLU) said at the time.

7. NSA elite hacking team techniques revealed

The NSA has at its disposal an elite hacker team codenamed "Tailored Access Operations" (TAO) that hacks into computers worldwide, infects them with malware and does the dirty job when other surveillance tactics fail.

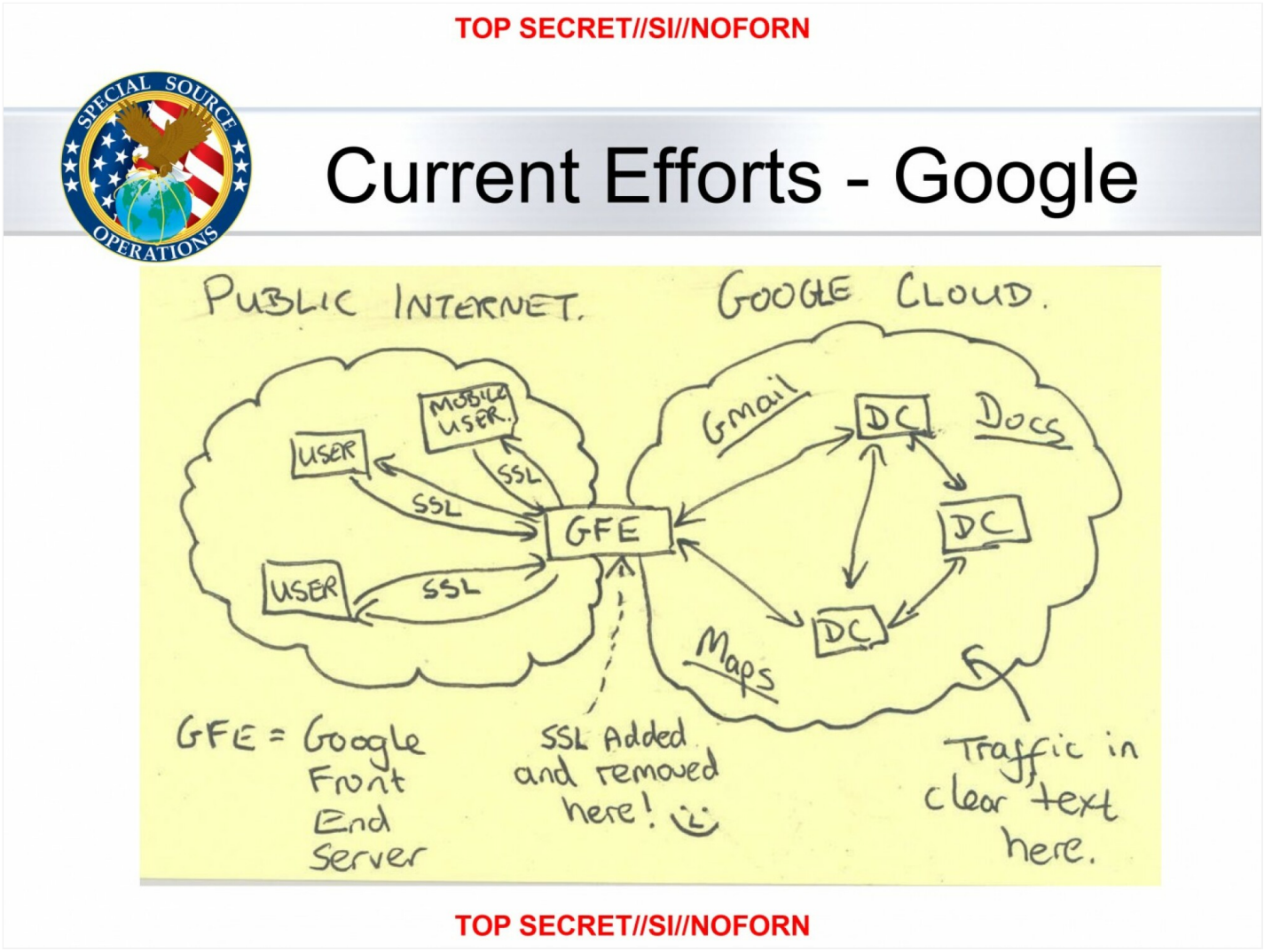
Der Spiegel, which detailed TAO's secrets, labelled it as "a squad of plumbers that can be called in when normal access to a target is blocked." But they can probably be best described as the NSA's black bag operations team.

TAO comes in for specific, targeted operations when the NSA can't find intelligence or needs more detailed information on a target through its bulk surveillance programs. Before Snowden, most of their operations and techniques were shrouded in secrecy, and their secrets make for one of the most fascinating revelations.

8. NSA cracks Google and Yahoo data center links

When bulk collection or PRISM fails, the NSA had other tricks up its sleeve: It could infiltrate links connecting Yahoo and Google data centers, behind the companies' backs.

This revelation was made famous mostly by a Power Point slide that included a celebratory smiley face.



Credit:

This story truly enraged the tech companies, which reacted with much more fury than before. Google and Yahoo announced plans to strengthen and encrypt those links to avoid this kind of surveillance, and a Google security employee even said on his Google+ account what many others must have thought privately: "Fuck these guys."

9. NSA collects text messages

It's not just about Internet data though. The NSA, following its unofficial motto of "collecting it all," intercepts 200 million text messages every day worldwide through a program called Dishfire.

In leaked documents, the agency described the collected messages as a "goldmine to exploit" for all kinds of personal data.

Here is what the NSA automatically extract from text messages *every day*: http://t.co/WyJnSX4Qui pic.twitter.com/DucMOOrdkK— James Ball (@jamesrbuk) January 16, 2014

Other documents also revealed that the NSA can "easily" crack cellphone encryption, allowing the agency to more easily decode and access the content of intercepted calls and text messages.

10. NSA intercepts all phone calls in two countries

The NSA intercepts and stores all phone calls made in the Bahamas and Afghanistan through a program called MYSTIC, which has its own snazzy logo.

Credit:

The Bahamas was revealed by The Intercept, Greenwald's new website, while the second was revealed by WikiLeaks, which protested The Intercept's decision to withhold the second country's name.

The NSA also collects all phone calls' metadata in Mexico, Kenya and the Philippines.

Bonus: Edward Snowden's first in-person interview with an American news outlet

(H/T to the site Free Snowden, which has an extensive and detailed list of all the NSA revelations.)

Email Address **Subscribe**

By signing up to the Mashable newsletter you agree to receive electronic communications from Mashable that may sometimes include advertisements or sponsored content.

TECH

SCIENCE

LIFE

SOCIAL GOOD

ENTERTAINMENT

BEST PRODUCTS

DEALS

About Mashable

Contact Us

We're Hiring

Newsletters

Sitemap