

In worldwide surveillance age, US has big edge (Update)

July 2 2013, by Raphael Satter



This June 23, 2013 file photo shows a TV screen shows a news report of Edward Snowden, a former CIA employee who leaked top-secret documents about sweeping U.S. surveillance programs, at a shopping mall in Hong Kong. The saga of Edward Snowden and the NSA makes one thing clear: The United States' central role in developing the Internet and hosting its most powerful players has made it the global leader in the surveillance game . Other countries, from dictatorships to democracies, are also avid snoopers, tapping into the high-capacity fiber optic cables to intercept Internet traffic, scooping their citizens' data off domestic servers, and even launching cyberattacks to win access to foreign networks. (AP Photo/Vincent Yu, File)

The saga of Edward Snowden and the NSA makes one thing clear: The United States' central role in developing the Internet and hosting its most powerful players has made it the global leader in the surveillance game.

Other countries, from dictatorships to democracies, are also avid snoopers, tapping into the high-capacity fiber optic cables to intercept Internet traffic, scooping their citizens' data off domestic servers, and even launching cyberattacks to win access to foreign networks.

But experts in the field say that Silicon Valley has made America a surveillance superpower, allowing its spies access to massive mountains of data being collected by the world's leading communications, social media, and online storage companies. That's on top of the United States' fiber optic infrastructure—responsible for just under a third of the world's international Internet capacity, according to telecom research firm TeleGeography—which allows it to act as a global postmaster, complete with the ability to peek at a big chunk of the world's messages in transit.

"The sheer power of the U.S. infrastructure is that quite often data would be routed though the U.S. even if it didn't make geographical sense," Joss Wright, a researcher with the Oxford Internet Institute, said in a telephone interview. "The current status quo is a huge benefit to the U.S."

The status quo is particularly favorable to America because online spying drills into people's private everyday lives in a way that other, more traditional forms of espionage can't match. So countries like Italy, where a culture of rampant wiretapping means that authorities regularly eavesdrop on private conversations, can't match the level of detail drawn from Internet searches or email traffic analysis.

"It's as bad as reading your diary," Wright said. Then he corrected

himself: "It's FAR WORSE than reading your diary. Because you don't write everything in your diary."

Although the details of how the NSA's PRISM program draws its data from these firms remain shrouded in secrecy, documents leaked by spy agency systems analyst Edward Snowden to the Guardian and The Washington Post newspapers said its inside track with U.S. tech firms afforded "one of the most valuable, unique, and productive" avenues for intelligence-gathering. How much cooperation America's Internet giants are giving the government in this inside track relationship is a key unanswered question.

Whatever the case, the pool of information in American hands is vast. Redmond, Washington-based Microsoft Corp.'s popular Internet Explorer accounts for between a quarter and half of all browsers, according to various estimates. Mountain View, California-based Google Inc. carries two-thirds of the world's online search traffic, analysts say. Menlo Park, California-based Facebook Inc. has some 900 million users—a figure that accounts for a third of the world's estimated 2.7 billion Internet-goers.

Electronic eavesdropping is, of course, far from an exclusively American pursuit. Many other nations pry further and with less oversight.

China and Russia have long hosted intrusive surveillance regimes. Russia's "SORM," the Russian-language acronym for System for Operational-Investigative Activities, allows government officials to directly access nearly every Internet service provider in the country. Initially set up to allow the FSB, the successor organization to the KGB, unfettered access to Russia's Internet traffic, the scope of SORM has grown dramatically since Vladimir Putin took power in 2000 and now allows a wide range law enforcement agencies to monitor Russians'

messages.

In China, surveillance is "pervasive, extensive, but perhaps not as high-tech" as in the United States, said Andrew Lih, a professor of journalism at American University in Washington. He said major Internet players such as microblogging service Sina, chat service QQ, or Chinese search giant Baidu were required to have staff—perhaps as many as several hundred people—specially tasked with carrying out the state's bidding, from surveillance to censorship.

What sets America apart is that it sits at the center of gravity for much of world's social media, communications, and online storage.

Americans' "position in the network, the range of services that they offer globally, the size of their infrastructure, and the amount of bandwidth means that the U.S. is in a very privileged position to surveil internationally," said Wright. "That's particularly true when you're talking about cloud services such as Gmail"—which had 425 million active users as of last year.

Many are trying to beat America's tech dominance by demanding that U.S. companies open local branches—something the Turkish government recently asked of San Francisco-based Twitter Inc., for example—or by banning them altogether. Santa Clara, California-based WhatsApp, for example, may soon be prohibited in Saudi Arabia.

Governments are also racing to capture traffic as it bounces back and forth from California, importing bulk surveillance devices, loosening spy laws, and installing centralized monitoring centers to offer officials a one-stop shop for intercepted data.

—Middle Eastern governments have installed Western-made surveillance technology to monitor domestic communications in

bulk—sometimes with help the very same contractors which do work for the NSA.

—India's government has begun deploying a centralized system which would route the nation's Internet traffic through a single monitoring point—one of several countries working to give law enforcement a one-stop shop for intercepted data.

—Recently-passed Brazilian money laundering laws allow authorities to access Internet and communication data without a court order—a no-warrants-needed trend the report said was being repeated across the globe.

"Eventually, it won't just be Big Brother," said Richard J. Aldrich, the author of a book about Britain's GCHQ eavesdropping agency. "There will be hundreds of little brothers."

But the siblings have a lot of catching up to do if they want to match surveillance powers of the United States, and some have turned to cyberespionage to try to even the playing field. A high-profile attack on Gmail users in 2010, for example, was blamed on Chinese hackers, while suspicion for separate 2011 attack on various U.S. webmail services fell on Iran.

But even in the dark arts of cyberespionage, America seems to have mastered the field. The FBI has been targeting criminals with sophisticated surveillance software for years, while one U.S. general recently boasted of hacking his enemies in Afghanistan.

In his comments to the South China Morning Post, Snowden said Americans had broken into computer systems belonging to a prominent Chinese research university, a fiber optic cable company and Chinese telecoms providers.

"We hack everyone everywhere," Snowden said.

U.S. officials haven't exactly denied it.

"You're commuting to where the information is stored and extracting the information from the adversaries' network," ex-NSA chief Michael Hayden told Bloomberg Businessweek earlier this year. "We are the best at doing it. Period."

© 2013 The Associated Press. All rights reserved.

Citation: In worldwide surveillance age, US has big edge (Update) (2013, July 2) retrieved 19 April 2024 from <https://phys.org/news/2013-07-golden-age-surveillance-big-edge.html>

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.