The New York Times

November 25, 2013

N.S.A. May Have Hit Internet Companies at a Weak Spot

By NICOLE PERLROTH and JOHN MARKOFF

SAN FRANCISCO — The recent revelation that the National Security Agency was able to eavesdrop on the communications of Google and Yahoo users without breaking into either company's data centers sounded like something pulled from a Robert Ludlum spy thriller.

How on earth, the companies asked, did the N.S.A. get their data without their knowing about it?

The most likely answer is a modern spin on a century-old eavesdropping tradition.

People knowledgeable about Google and Yahoo's infrastructure say they believe that government spies bypassed the big Internet companies and hit them at a weak spot — the fiber-optic cables that connect data centers around the world and are owned by companies like Verizon Communications, the BT Group, the Vodafone Group and Level 3 Communications. In particular, fingers have been pointed at Level 3, the world's largest so-called Internet backbone provider, whose cables are used by Google and Yahoo.

The Internet companies' data centers are locked down with full-time security and state-of-the-art surveillance, including heat sensors and iris scanners. But between the data centers — on Level 3's fiber-optic cables that connected those massive computer farms — information was unencrypted and an easier target for government intercept efforts, according to three people with knowledge of Google's and Yahoo's systems who spoke on the condition of anonymity.

It is impossible to say for certain how the N.S.A. managed to get Google and Yahoo's data without the companies' knowledge. But both companies, in response to concerns over those vulnerabilities, recently said they were now encrypting data that runs on the cables between their data centers. Microsoft is considering a similar move.

"Everyone was so focused on the N.S.A. secretly getting access to the front door that there was an assumption they weren't going behind the companies' backs and tapping data through the back door, too," said Kevin Werbach, an associate professor at the Wharton School.

Data transmission lines have a long history of being tapped.

As far back as the days of the telegraph, spy agencies have located their operations in proximity to communications companies. Indeed, before the advent of the Internet, the N.S.A. and its predecessors for decades operated listening posts next to the long-distance lines of phone companies to monitor all international voice traffic.

Beginning in the 1960s, a spy operation code-named Echelon targeted the Soviet Union and its allies'

voice, fax and data traffic via satellite, microwave and fiber-optic cables.

In the 1990s, the emergence of the Internet both complicated the task of the intelligence agencies and presented powerful new spying opportunities based on the ability to process vast amounts of computer data.

In 2002, John M. Poindexter, former national security adviser under President Ronald Reagan, proposed the Total Information Awareness plan, an effort to scan the world's electronic information — including phone calls, emails and financial and travel records. That effort was scrapped in 2003 after a public outcry over potential privacy violations.

The technologies Mr. Poindexter proposed are similar to what became reality years later in N.S.A. surveillance programs like Prism and Bullrun.

The Internet effectively mingled domestic and international communications, erasing the bright line that had been erected to protect against domestic surveillance. Although the Internet is designed to be a highly decentralized system, in practice a small group of backbone providers carry almost all of the network's data.

The consequences of the centralization and its value for surveillance was revealed in 2006 by Mark Klein, an AT&T technician who described an N.S.A. listening post inside a room at an AT&T switching facility.

The agency was capturing a copy of all the data passing over the telecommunications links and then filtering it in AT&T facilities that housed systems that were able to filter data packets at high speed.

Documents taken by Edward J. Snowden and reported by The Washington Post indicate that, seven years after Mr. Klein first described the N.S.A.'s surveillance technologies, they have been refined and modernized.

"From Echelon to Total Information Awareness to Prism, all these programs have gone under different names, but in essence do the same thing," said Chip Pitts, a law lecturer at Stanford University School of Law.

Based in the Denver suburbs, Level 3 is not a household name like Verizon or AT&T, but in terms of its ability to carry traffic, it is bigger than the other two carriers combined. Its networking equipment is found in 200 data centers in the United States, more than 100 centers in Europe and 14 in Latin America.

Level 3 did not directly respond to an inquiry about whether it had given the N.S.A., or the agency's foreign intelligence partners, access to Google and Yahoo's data. In a statement, Level 3 said: "It is our policy and our practice to comply with laws in every country where we operate, and to provide government agencies access to customer data only when we are compelled to do so by the laws in the country where the data is located."

Also, in a financial filing, Level 3 noted that, "We are party to an agreement with the U.S. Departments of Homeland Security, Justice and Defense addressing the U.S. government's national security and law

enforcement concerns. This agreement imposes significant requirements on us related to information storage and management; traffic management; physical, logical and network security arrangements; personnel screening and training; and other matters."

Security experts say that regardless of whether Level 3's participation is voluntary or not, recent N.S.A. disclosures make clear that even when Internet giants like Google and Yahoo do not hand over data, the N.S.A. and its intelligence partners can simply gather their data downstream.

That much was true last summer when United States authorities first began tracking Mr. Snowden's movements after he left Hawaii for Hong Kong with thousands of classified documents. In May, authorities contacted Ladar Levison, who ran Lavabit, Mr. Snowden's email provider, to install a tap on Mr. Snowden's email account. When Mr. Levison did not move quickly enough to facilitate the tap on Lavabit's network, the Federal Bureau of Investigation did so without him.

Mr. Levison said it was unclear how that tap was installed, whether through Level 3, which sold bandwidth to Lavabit, or at the Dallas facility where his servers and networking equipment are stored. When Mr. Levison asked the facility's manager about the tap, he was told the manager could not speak with him. A spokesman for TierPoint, which owns the Dallas facility, did not return a call seeking a comment.

Mr. Pitts said that while working as the chief legal officer at Nokia in the 1990s, he successfully fended off an effort by intelligence agencies to get backdoor access into Nokia's computer networking equipment.

Nearly 20 years later, Verizon has said that it and other carriers are forced to comply with government requests in every country in which they operate, and are limited in what they can say about their arrangements.

"At the end of the day, if the Justice Department shows up at your door, you have to comply," Lowell C. McAdam, Verizon's chief executive, said in an interview in September. "We have gag orders on what we can say and can't defend ourselves, but we were told they do this with every carrier."