The New York Times | http://nyti.ms/1WteOo8

U.S.

AT&T Helped U.S. Spy on Internet on a Vast Scale

By JULIA ANGWIN, CHARLIE SAVAGE, JEFF LARSON, HENRIK MOLTKE, LAURA POITRAS and JAMES RISEN AUG. 15, 2015

The National Security Agency's ability to spy on vast quantities of Internet traffic passing through the United States has relied on its extraordinary, decades-long partnership with a single company: the telecom giant AT&T.

While it has been long known that American telecommunications companies worked closely with the spy agency, newly disclosed N.S.A. documents show that the relationship with AT&T has been considered unique and especially productive. One document described it as "highly collaborative," while another lauded the company's "extreme willingness to help."

AT&T's cooperation has involved a broad range of classified activities, according to the documents, which date from 2003 to 2013. AT&T has given the N.S.A. access, through several methods covered under different legal rules, to billions of emails as they have flowed across its domestic networks. It provided technical assistance in carrying out a secret court order permitting the wiretapping of all Internet communications at the United Nations headquarters, a customer of AT&T.

The N.S.A.'s top-secret budget in 2013 for the AT&T partnership was

more than twice that of the next-largest such program, according to the documents. The company installed surveillance equipment in at least 17 of its Internet hubs on American soil, far more than its similarly sized competitor, Verizon. And its engineers were the first to try out new surveillance technologies invented by the eavesdropping agency.

One document reminds N.S.A. officials to be polite when visiting AT&T facilities, noting, “This is a partnership, not a contractual relationship.”

The documents, provided by the former agency contractor Edward J. Snowden, were jointly reviewed by The New York Times and ProPublica. The N.S.A., AT&T and Verizon declined to discuss the findings from the files. “We don’t comment on matters of national security,” an AT&T spokesman said.

It is not clear if the programs still operate in the same way today. Since the Snowden revelations set off a global debate over surveillance two years ago, some Silicon Valley technology companies have expressed anger at what they characterize as N.S.A. intrusions and have rolled out new encryption to thwart them. The telecommunications companies have been quieter, though Verizon unsuccessfully challenged a court order for bulk phone records in 2014.

At the same time, the government has been fighting in court to keep the identities of its telecom partners hidden. In a recent case, a group of AT&T customers claimed that the N.S.A.’s tapping of the Internet violated the Fourth Amendment protection against unreasonable searches. This year, a federal judge dismissed key portions of the lawsuit after the Obama administration argued that public discussion of its telecom surveillance efforts would reveal state secrets, damaging national security.

The N.S.A. documents do not identify AT&T or other companies by name. Instead, they refer to corporate partnerships run by the agency’s Special Source Operations division using code names. The division is responsible for more than 80 percent of the information the N.S.A. collects, one document

states.

Fairview is one of its oldest programs. It began in 1985, the year after antitrust regulators broke up the Ma Bell telephone monopoly and its long-distance division became AT&T Communications. An analysis of the Fairview documents by The Times and ProPublica reveals a constellation of evidence that points to AT&T as that program's partner. Several former intelligence officials confirmed that finding.

A Fairview fiber-optic cable, damaged in the 2011 earthquake in Japan, was repaired on the same date as a Japanese-American cable operated by AT&T. Fairview documents use technical jargon specific to AT&T. And in 2012, the Fairview program carried out the court order for surveillance on the Internet line, which AT&T provides, serving the United Nations headquarters. (N.S.A. spying on United Nations diplomats has previously been reported, but not the court order or AT&T's involvement. In October 2013, the United States told the United Nations that it would not monitor its communications.)

The documents also show that another program, code-named Stormbrew, has included Verizon and the former MCI, which Verizon purchased in 2006. One describes a Stormbrew cable landing that is identifiable as one that Verizon operates. Another names a contact person whose LinkedIn profile says he is a longtime Verizon employee with a top-secret clearance.

After the terrorist attacks of Sept. 11, 2001, AT&T and MCI were instrumental in the Bush administration's warrantless wiretapping programs, according to a draft report by the N.S.A.'s inspector general. The report, disclosed by Mr. Snowden and previously published by The Guardian, does not identify the companies by name but describes their market share in numbers that correspond to those two businesses, according to Federal Communications Commission reports.

AT&T began turning over emails and phone calls "within days" after the warrantless surveillance began in October 2001, the report indicated. By

contrast, the other company did not start until February 2002, the draft report said.

In September 2003, according to the previously undisclosed N.S.A. documents, AT&T was the first partner to turn on a new collection capability that the N.S.A. said amounted to a " 'live' presence on the global net." In one of its first months of operation, the Fairview program forwarded to the agency 400 billion Internet metadata records — which include who contacted whom and other details, but not what they said — and was "forwarding more than one million emails a day to the keyword selection system" at the agency's headquarters in Fort Meade, Md. Stormbrew was still gearing up to use the new technology, which appeared to process foreign-to-foreign traffic separate from the post-9/11 program.

In 2011, AT&T began handing over 1.1 billion domestic cellphone calling records a day to the N.S.A. after "a push to get this flow operational prior to the 10th anniversary of 9/11," according to an internal agency newsletter. This revelation is striking because after Mr. Snowden disclosed the program of collecting the records of Americans' phone calls, intelligence officials told reporters that, for technical reasons, it consisted mostly of landline phone records.

That year, one slide presentation shows, the N.S.A. spent $188.9 million on the Fairview program, twice the amount spent on Stormbrew, its second-largest corporate program.

After The Times disclosed the Bush administration's warrantless wiretapping program in December 2005, plaintiffs began trying to sue AT&T and the N.S.A. In a 2006 lawsuit, a retired AT&T technician named Mark Klein claimed that three years earlier, he had seen a secret room in a company building in San Francisco where the N.S.A. had installed equipment.

Mr. Klein claimed that AT&T was providing the N.S.A. with access to Internet traffic that AT&T transmits for other telecom companies. Such

cooperative arrangements, known in the industry as "peering," mean that communications from customers of other companies could end up on AT&T's network.

After Congress passed a 2008 law legalizing the Bush program and immunizing the telecom companies for their cooperation with it, that lawsuit was thrown out. But the newly disclosed documents show that AT&T has provided access to peering traffic from other companies' networks.

AT&T's "corporate relationships provide unique accesses to other telecoms and I.S.P.s," or Internet service providers, one 2013 N.S.A. document states.

Because of the way the Internet works, intercepting a targeted person's email requires copying pieces of many other people's emails, too, and sifting through those pieces. Plaintiffs have been trying without success to get courts to address whether copying and sifting pieces of all those emails violates the Fourth Amendment.

Many privacy advocates have suspected that AT&T was giving the N.S.A. a copy of all Internet data to sift for itself. But one 2012 presentation says the spy agency does not "typically" have "direct access" to telecoms' hubs. Instead, the telecoms have done the sifting and forwarded messages the government believes it may legally collect.

"Corporate sites are often controlled by the partner, who filters the communications before sending to N.S.A.," according to the presentation. This system sometimes leads to "delays" when the government sends new instructions, it added.

The companies' sorting of data has allowed the N.S.A. to bring different surveillance powers to bear. Targeting someone on American soil requires a court order under the Foreign Intelligence Surveillance Act. When a foreigner abroad is communicating with an American, that law permits the government

to target that foreigner without a warrant. When foreigners are messaging other foreigners, that law does not apply and the government can collect such emails in bulk without targeting anyone.

AT&T's provision of foreign-to-foreign traffic has been particularly important to the N.S.A. because large amounts of the world's Internet communications travel across American cables. AT&T provided access to the contents of transiting email traffic for years before Verizon began doing so in March 2013, the documents show. They say AT&T gave the N.S.A. access to "massive amounts of data," and by 2013 the program was processing 60 million foreign-to-foreign emails a day.

Because domestic wiretapping laws do not cover foreign-to-foreign emails, the companies have provided them voluntarily, not in response to court orders, intelligence officials said. But it is not clear whether that remains the case after the post-Snowden upheavals.

"We do not voluntarily provide information to any investigating authorities other than if a person's life is in danger and time is of the essence," Brad Burns, an AT&T spokesman, said. He declined to elaborate.

Correction: August 15, 2015

An earlier version of a picture caption with this article misstated the number of emails the National Security Agency has gotten access to with the cooperation of AT&T. As the article correctly noted, it is in the billions, not trillions.

Julia Angwin and Jeff Larson report for ProPublica.

A version of this article appears in print on August 16, 2015, on page A1 of the New York edition with the headline: AT&T Helped U.S. Spy on Internet On a Vast Scale .
