AT&T colludes with the NSA to carry out massive illegal surveillance

Meenakshi Jagadeesan
29 June 2018

In an investigative report released on Monday, The Intercept has further exposed the long-term and highly organized collusion between the communications behemoth AT&T and the National Security Agency (NSA). The story reveals the use of eight AT&T facilities in major cities across the US (New York, Chicago, Atlanta, San Francisco, Los Angeles, Seattle, Washington D.C., and Dallas) by the NSA to serve as "critical parts of one of the world's most powerful electronic eavesdropping systems, hidden in plain sight."

In large part due to the efforts of brave whistleblowers like Edward Snowden, the public has been made aware of the massive and illegal surveillance on all forms of electronic communications carried out by the NSA. In addition, there has been sufficient evidence of the "special relationship" between AT&T and the NSA. However, the new revelations are striking in that they not only provide us a much better look at the physical infrastructure of the spying, but also make clear that the sheer scale of the collusion and the surveillance is far greater than has been assumed.

The eight sites identified by The Intercept are different from the hundreds of other sites that are owned by AT&T across the US, in that they primarily carry and process large amounts of data not just from the company's own customers, but also from other internet providers. Not all internet operators have the infrastructure to send data in an efficient or cost-effective manner. So, when internet traffic in a particular area gets overwhelming for a particular internet provider, they tend to use the bandwidth that is sold or exchanged by another operator with capacity to spare.

Given its position as one of the largest US telecommunications companies, AT&T's vast network is often used by other operators around the world to transport their customers' data. Included in the list of companies that use AT&T's infrastructure are Sprint, Cogent Communications, and Level 3, as well as foreign companies such as Sweden's Telia, India's Tata Communications, Italy's Telecom Italia, and Germany's Deutsche Telekom. The initial transfer of data between the companies takes place in third party sites (such as those operated by California's Equinix), but then much or all of it is routed through the eight major sites. These sites are known as "peering" or "backbone" facilities. And it is these facilities that are being put to the service of the NSA's surveillance program.

Mark Klein, a technician who worked for AT&T over 22 years, told The Intercept that having access to the "peering sites" provides the NSA far greater access than just the usual data "because the peering links, by the nature of the connections, are liable to carry everybody's traffic at one point or another during the day, or the week, or the year."

NSA spokesman Christopher Augustine gave the expected official response that the agency could "neither confirm nor deny" the story, while insisting that it "conducts its foreign signals intelligence mission under the legal authorities established by Congress and is bound by both policy and law to protect U.S. persons' privacy and civil liberties."

However, the NSA's extra-legal activities are by now well-known enough for that assurance to sound quite hollow. In addition, the willingness of the ruling class to use all tools at its disposal to curtail mass opposition, means that even the existing "legal authorities" are at best vague and elastic enough to justify mass surveillance and violations of the Bill of Rights.

The NSA had laid the framework for its largest surveillance program, codenamed “FAIRVIEW,” in 1985, before technological developments allowed for this amount of data to be transported and processed. In fact, AT&T (incidentally, the only company to participate in FAIRVIEW) developed the eight “peering” sites, known as “Service Node Routing Complexes,” only in the late 1990s, following the internet boom. However, within a decade these sites were being fully used by the NSA, still within the purview of FAIRVIEW.

The kind and amount of data that control of the peering sites allows the NSA is truly mind-boggling. A majority of the data transmitted from around the world through the vast, under ocean, fiber-optic network is routed at one point or another through the US. This is in part due to the location of the country between the major continents, but also due to the pre-eminence of American telecommunications companies. It is this “home-field advantage” that the NSA has very systematically exploited, with the full support of AT&T.

Under a classified initiative called “SAGUARO,” AT&T worked with the NSA to create a framework on how to eavesdrop in the most effective manner in the peering sites, ranking “communications flowing through its networks on the basis of intelligence value, prioritizing data depending on which country it was derived from.” AT&T’s helpfulness seems to have gone even beyond just facilitating the use of its own servers. According to the information acquired by The Intercept, the company has worked hand-in-glove with the NSA to set up a centralized processing facility, believed to be somewhere in New Jersey, where the material collected from the peering sites are processed once again, before being sent to the NSA headquarters in Maryland.

The NSA has for decades claimed the legal right to eavesdrop on “communications which originate and terminate in foreign countries, but traverse U.S. territory,” under the Reagan-era Executive Order 12333. After 9/11, the agency creatively interpreted this right to surveil communications taking place between American citizens, leading to the eventual exposure of the “warrantless wiretapping” scandal.

While critics rightly pointed out that this constituted a violation of citizenship rights, in 2008 Congress provided a legal patina to the actions of the NSA by enacting Section 702 of the Foreign Intelligence and Surveillance Act (FISA). Under this, the NSA is allowed to continue warrantless wiretapping, so long as “it is incidental ... for instance, if it was monitoring people in Pakistan, and they were talking with Americans in the U.S. by phone, email, or through an internet chat service.” The absurdity of supposing this addition in any way protects Fourth Amendment rights was made apparent even in the FISA court’s own findings in 2011 that the NSA “had acquired some 13 million ‘internet transactions’ during one six-month period, and had unlawfully gathered ‘tens of thousands of wholly domestic communications’ each year.”

The court’s ruling meant that the NSA had two options: to shut down its surveillance operations or to put into place measures that would prevent it from reviewing its unlawfully collected information. The NSA claimed that it chose the latter, and had put into place “cautionary banners” that would ensure the protection of constitutional rights. However, there is no indication that these “banners” in fact function as their supporters claim.

In fact, in April 2017, the NSA admitted what it called “inadvertent compliance incidents” and stated that it would no longer be using surveillance programs authorized under Section 702. As with its earlier assurances about respect for constitutional rights, this statement should be taken with a healthy dose of skepticism. The exposure of the continued activities of the NSA in collusion with AT&T shows that the very same tactics, albeit not under the same legal framework, remain in place, and the construction of an Orwellian state apparatus continues unabated.