How the NSA's Domestic Spying Program Works

The NSA's domestic spying program, known in official government documents as the "President's Surveillance Program," ("The Program") was implemented by President George W. Bush shortly after the attacks on September 11, 2001. The US Government still considers the Program officially classified, but a tremendous amount of information has been exposed by various whistleblowers, admitted to by government officials during Congressional hearings and with public statements, and reported on in investigations by major newspaper across the country.

Our NSA Domestic Spying Timeline has a full list of important dates, events, and reports, but we also want to explain—to the extent we understand it—the full scope of the Program and how the government has implemented it.

In the weeks after 9/11, President Bush authorized the National Security Agency (NSA) to conduct a range of surveillance activities inside the United States, which had been barred by law and agency policy for decades. When the NSA's spying program was first exposed by the *New York Times* in 2005, President Bush admitted to a small aspect of the program—what the administration labeled the "Terrorist Surveillance Program"—in which the NSA monitored, without warrants, the communications of between 500-1000 people inside the US with suspected connections to Al Qaeda.

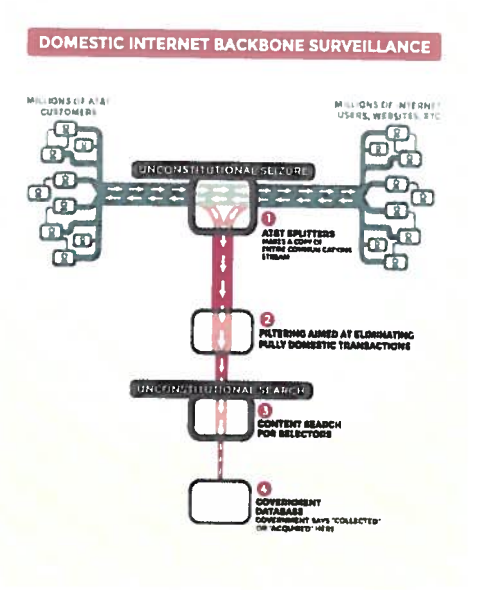
But other aspects of the Program were aimed not just at targeted individuals, but perhaps millions of innocent Americans never suspected of a crime.

Details of Every American's Call History

First, the government convinced the major telecommunications companies in the US, including AT&T, MCI, and Sprint, to hand over the "call-detail records" of their customers. According to an investigation by *USA Today*, this included

"customers' names, street addresses, and other personal information." In addition, the government received "detailed records of calls they made—across town or across the country—to family members, co-workers, business contacts and others."

A person familiar with the matter told *USA Today* that the agency's goal was "to create a database of every call ever made" within the nation's borders. All of this was done without a warrant or any judicial oversight.



Real Time Access to Phone and Internet Traffic

Second, the same telecommunications companies also allowed the NSA to install sophisticated communications surveillance equipment in secret rooms at key telecommunications facilities around the country. This equipment gave the NSA unfettered access to large streams of domestic and international communications in real time—what amounted to at least 1.7 billion emails a day, according to the Washington Post. The NSA could then data mine and analyze this traffic for suspicious key words, patterns and connections. Again, all of this was done without a warrant in violation of federal law and the Constitution.

The Technology That Made It Possible

But how did the government accomplish this task and how do we know? In addition to investigative reports by the *New York Times* and others, AT&T technician turned whistleblower Mark Klein provided EFF with eyewitness

testimony and documents describing one such secret room located at AT&T's Folsom Street facility in San Francisco, California.

It works like this: when you send an email or otherwise use the internet, the data travels from your computer, through telecommunication companies' wires and fiber optics networks, to your intended recipient. To intercept these communications, the government installed devices known as "fiber-optic splitters" in many of the main telecommunication junction points in the United States (like the AT&T facility in San Francisco). These splitters make exact copies of the data passing through them: then, one stream is directed to the government, while the other stream is directed to the intended recipients.

The Klein documents reveal the specific equipment installed at the AT&T facility and the processing power of the equipment within the secret rooms. One type of machine installed is a Narus Semantic Traffic Analyzer, a powerful tool for deep packet inspection. Narus has continually refined their capabilities and—as of the mid-2000s—each Narus machine was capable of analyzing 10 gigabits of IP packets, and 2.5 gigabits of web traffic or email, per second. It is likely even more powerful today. The Narus machine can then reconstruct the information transmitted through the network and forward the communications to a central location for storage and analysis.

In a declaration in our lawsuit, thirty-year NSA veteran William Binney estimates that "NSA installed no few than ten and possibly in excess of twenty intercept centers within the United States." Binney also estimates NSA has collected "between 15 and 20 trillion" transactions over the past 11 years.

In April 2012, long-time national security author James Bamford reported NSA is spending $2 billion to construct a data center in a remote part of Utah to house the information it has been collecting for the past decade. "Flowing through its servers and routers and stored in near-bottomless databases," Bamford wrote, "will be all forms of communication, including the complete contents of private emails, cell phone calls, and Google searches, as well as all sorts of personal data trails—parking receipts, travel itineraries, bookstore purchases, and other digital 'pocket litter.'"

The Utah data center will be fully operational in September 2013.