

**From:** (b)(6)  
**To:** [James R Clapper](#)  
**Subject:** TITANPOINTE  
**Date:** Wednesday, November 16, 2016 8:56:17 PM  
**Attachments:** [image001.jpg](#)  
[image002.jpg](#)  
[image003.jpg](#)  
[image004.jpg](#)  
[image005.jpg](#)  
[image006.jpg](#)  
[image007.jpg](#)  
[image008.jpg](#)  
[image009.jpg](#)  
[image010.jpg](#)  
[image011.jpg](#)  
[image012.jpg](#)  
[image013.jpg](#)  
[image014.jpg](#)

---

It's amazing what one finds on the Drudge Report... And just why does America "need to know" this???

## [Titanpointe](#)

### [The NSA's Spy Hub in New York, Hidden in Plain Sight](#)



November 16 2016, 2:40 p.m. Still from "Project X"

They called it Project X. It was an unusually audacious, highly sensitive assignment: to build a massive skyscraper, capable of withstanding an atomic blast, in the middle of New York City. It would have no windows, 29 floors with three basement levels, and enough food to last 1,500 people two weeks in the event of a catastrophe.

But the building's primary purpose would not be to protect humans from toxic radiation amid nuclear war. Rather, the fortified skyscraper would safeguard powerful computers, cables, and switchboards. It would house one of the most important telecommunications hubs in the United States — the world's largest center for processing long-distance phone calls, operated by the New York Telephone Company, a subsidiary of AT&T.

The building was designed by the architectural firm John Carl Warnecke & Associates, whose grand vision was to create a communication nerve center like a "20th century fortress, with spears and arrows replaced by protons and neutrons laying quiet siege to an army of machines within."

Excerpt from "Project X," a short film by Henrik Moltke and Laura Poitras, screening at the [IFC Center](#) starting Nov. 18. This article is the product of a joint reporting project between The Intercept and Field of Vision.

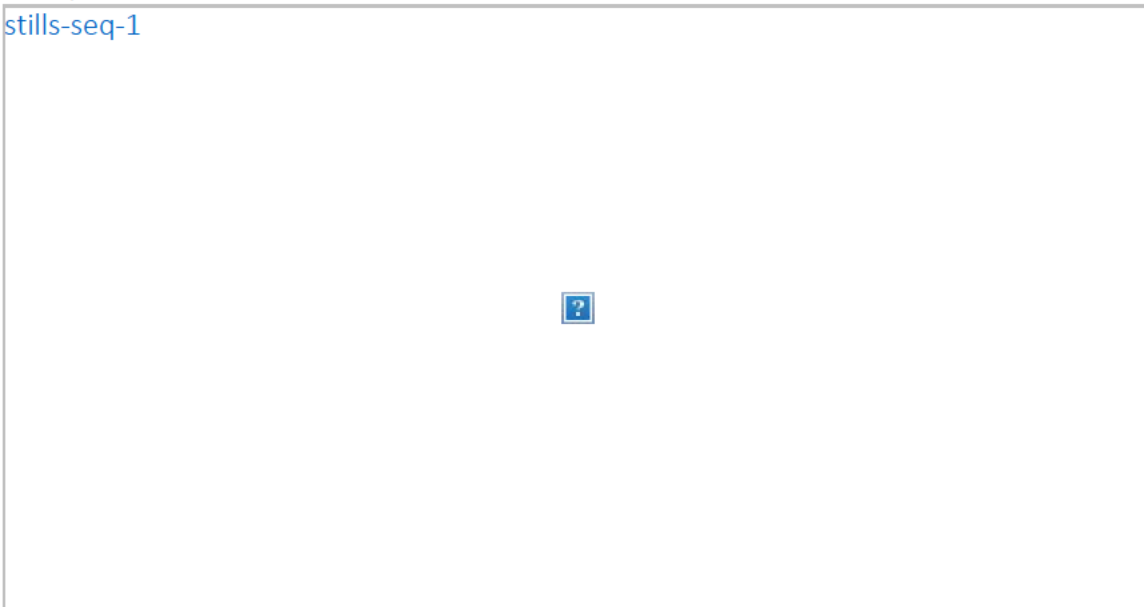
Construction began in 1969, and by 1974, the skyscraper was completed. Today, it can be found in the heart of lower Manhattan at 33 Thomas Street, a vast gray tower of concrete and

granite that soars 550 feet into the New York skyline. The brutalist structure, still used by AT&T and, according to the New York Department of Finance, owned by the company, is like no other in the vicinity. Unlike the many neighboring residential and office buildings, it is impossible to get a glimpse inside 33 Thomas Street. True to the designers' original plans, there are no windows and the building is not illuminated. At night it becomes a giant shadow, blending into the darkness, its large square vents emitting a distinct, dull hum that is frequently drowned out by the sound of passing traffic and wailing sirens.

For many New Yorkers, 33 Thomas Street — known as the “Long Lines Building” — has been a source of mystery for years. It has been labeled one of the city's weirdest and most iconic skyscrapers, but little information has ever been published about its purpose.

It is not uncommon to keep the public in the dark about a site containing vital telecommunications equipment. But 33 Thomas Street is different: An investigation by The Intercept indicates that the skyscraper is more than a mere nerve center for long-distance phone calls. It also appears to be one of the most important National Security Agency surveillance sites on U.S. soil — a covert monitoring hub that is used to tap into phone calls, faxes, and internet data.

[stills-seq-1](#)



Early model of the entrance of 33 Thomas Street as designed by John Carl Warnecke & Associates.

Still from “Project X”

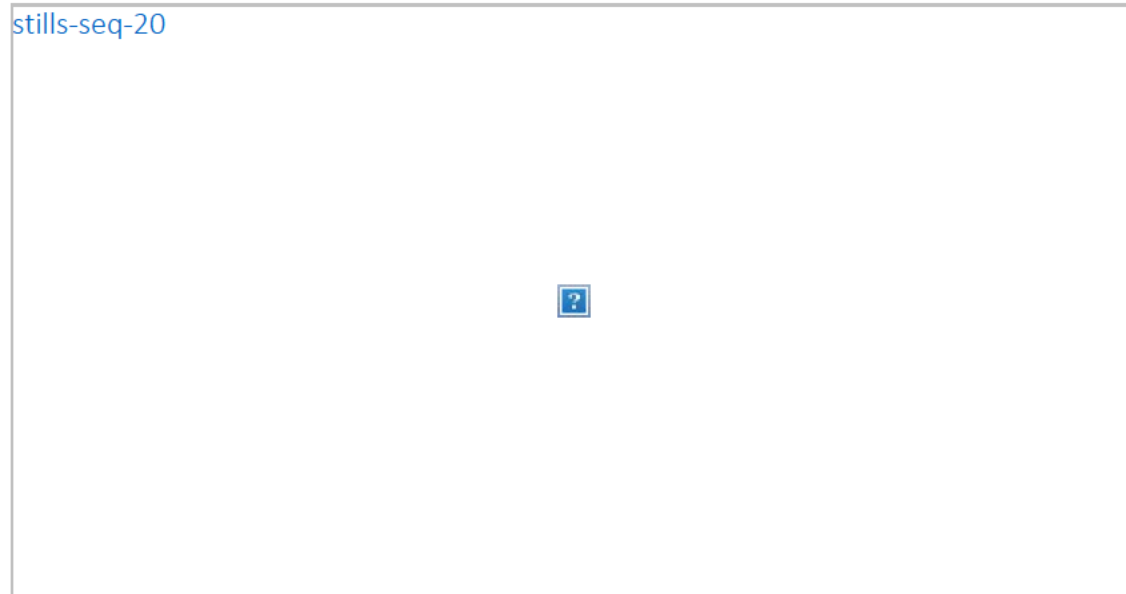
Documents obtained by The Intercept from the NSA whistleblower Edward Snowden do not explicitly name 33 Thomas Street as a surveillance facility. However — taken together with architectural plans, public records, and interviews with former AT&T employees conducted for this article — they provide compelling evidence that 33 Thomas Street has served as an NSA surveillance site, code-named TITANPOINTE.

Inside 33 Thomas Street there is a major international “gateway switch,” according to a former AT&T engineer, which routes phone calls between the United States and countries

across the world. A series of top-secret NSA memos suggest that the agency has tapped into these calls from a secure facility within the AT&T building. The Manhattan skyscraper appears to be a core location used for a controversial NSA surveillance program that has targeted the communications of the United Nations, the International Monetary Fund, the World Bank, and at least 38 countries, including close U.S. allies such as Germany, Japan, and France. It has long been known that AT&T has cooperated with the NSA on surveillance, but few details have emerged about the role of specific facilities in carrying out the top-secret programs. The Snowden documents provide new information about how NSA equipment has been integrated as part of AT&T's network in New York City, revealing in unprecedented detail the methods and technology the agency uses to vacuum up communications from the company's systems.

"This is yet more proof that our communications service providers have become, whether willingly or unwillingly, an arm of the surveillance state," said Elizabeth Goitein, co-director of the liberty and national security program at the Brennan Center for Justice. "The NSA is presumably operating under authorities that enable it to target foreigners, but the fact that it is so deeply embedded in our domestic communications infrastructure should tip people off that the effects of this kind of surveillance cannot be neatly limited to non-Americans."

The NSA declined to comment for this story.



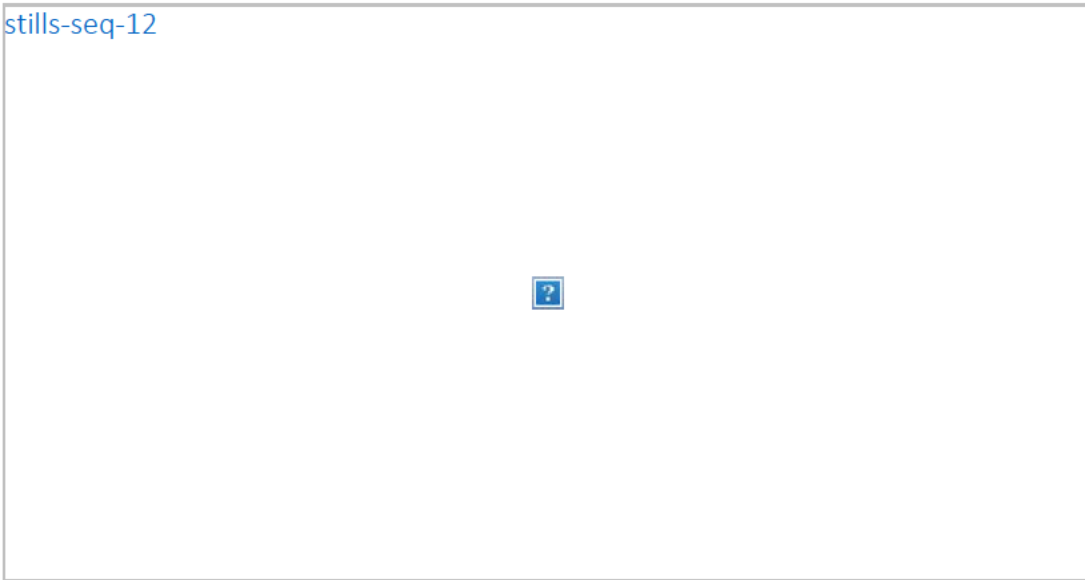
The FBI occupies the entire 23rd floor of 26 Federal Plaza, seen here behind 33 Thomas Street. Still from "Project X"

The code name TITANPOINTE features dozens of times in the NSA documents, often in classified reports about surveillance operations. The agency uses code names to conceal information it deems especially sensitive — for instance, the names of companies it cooperates with or specific locations where electronic spying is carried out. Such details are usually considered "exceptionally controlled information," a category beyond top secret and thus outside the scope of most of the documents that Snowden was able to obtain. Secret NSA travel guides, dated [April 2011](#) and [February 2013](#), however, reveal information about TITANPOINTE that helps establish its connection to 33 Thomas Street. The 2011 guide,

written to assist NSA employees visiting various facilities, discloses that TITANPOINTE is in New York City. The 2013 guide states that a “partner” called LITHIUM, which is NSA’s code name for AT&T, supervises visits to the site.

The 33 Thomas Street building is located almost next door to the FBI’s New York field office — about a block away — at Federal Plaza. The 2011 NSA travel guide instructs employees traveling to TITANTPOINTE to head to the FBI’s New York field office. It adds that trips to the site should be coordinated with AT&T (referenced as “LITHIUM”) and the FBI, including an FBI “site watch officer.”

[stills-seq-12](#)



Intercom at 33 Thomas Street.

Still from “Project X”

When traveling to TITANPOINTE, NSA employees are told to hire a “cover vehicle” through the FBI, especially if they are transporting equipment to the site. In order to keep their true identities secret while visiting, agency employees are instructed not to wear any clothing displaying NSA badges or insignia.

Upon arrival at TITANPOINTE, the 2011 travel guide says, agency employees should ring the buzzer, sign in, and wait for a person to come and meet them. The Intercept visited 33 Thomas Street and found a buzzer outside its entrance and a sign-in sheet on a desk in the building’s lobby, which is manned by a guard 24 hours a day. There are also parking bays in front of the skyscraper designated “AWM,” a [traffic code for federal agencies](#).

A [1994 New York Times article](#) reported that 33 Thomas Street was part of AT&T’s “giant Worldwide Intelligent Network, which is responsible for directing an average of 175 million phone calls a day.” Thomas Saunders, a former AT&T engineer, told The Intercept that inside the building there were at least three “4ESS switches” used to route calls across phone networks. “Of the first two, one handled domestic long-distance traffic and the other was an international gateway,” said Saunders, who retired from his role at the company in 2004. The NSA’s documents [describe](#) TITANPOINTE as containing “foreign gateway switches” and they state that it has a “RIMROCK access.” RIMROCK is an NSA code name for 4ESS switches. The NSA’s documents also reveal that one of TITANPOINTE’s functions is to conduct

surveillance as part of a program called SKIDROWE, which focuses on intercepting satellite communications. That is a particularly striking detail, because on the roof of 33 Thomas Street there are a number of satellite dishes. Federal Communications Commission records confirm that 33 Thomas Street is the only location in New York City where AT&T has an FCC license for satellite earth stations.

[026V9767-high-res-edit](#)



Design plan for the tower mechanical equipment floor at 33 Thomas Street.

The man behind the design of 33 Thomas Street, John Carl Warnecke, was one of the most prominent architects in the U.S. between the 1960s and 1980s.

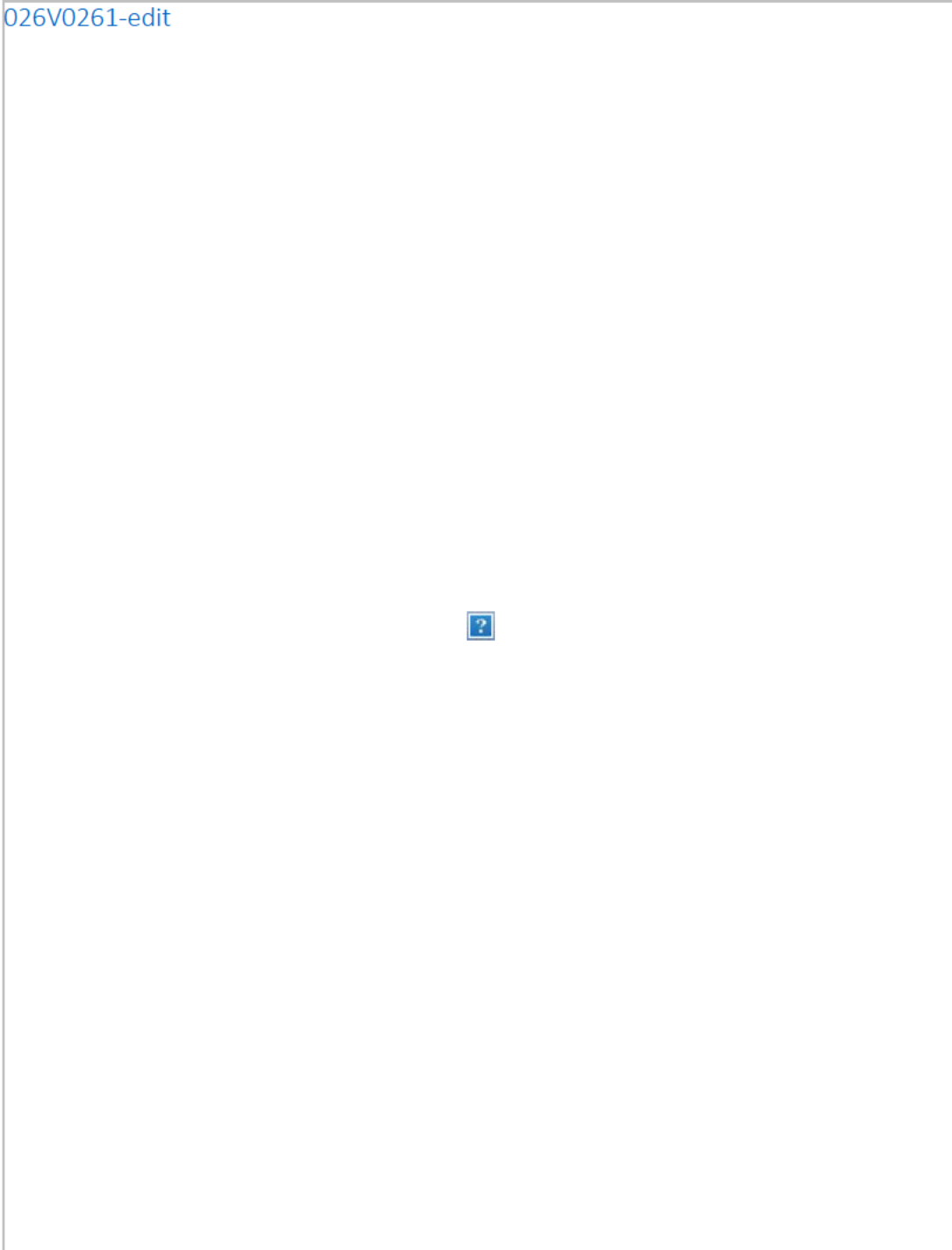
Warnecke's high-profile projects included producing designs for the U.S. Naval Academy in Maryland, the Hart Senate Office Building in Washington, D.C., and the Hawaii State Capitol. In 1962, President John F. Kennedy's administration commissioned Warnecke to preserve and restructure buildings at Lafayette Square, across from the White House. And following Kennedy's assassination, Warnecke was asked to design the president's eternal flame and gravesite at Arlington National Cemetery. He also helped construct a new embassy complex in Washington for the Soviet Union, in which the Soviets claimed they found eavesdropping equipment embedded in the walls.

But it was not only governments that trusted Warnecke — who died in 2010, aged 91 — with major construction projects. He cultivated a close relationship with telecommunications companies, too, possibly helped by family ties to the industry. Warnecke's father-in-law had been a director at Pacific Bell, a California-based AT&T subsidiary. In the 1960s, Warnecke was asked to design a telephone exchange building for Pacific Bell in Oakland. He would subsequently receive a series of other major commissions from AT&T: Aside from the 33 Thomas Street building, he also designed a telephone exchange in Williamsburg, Brooklyn, and an AT&T facility in Bedminster, New Jersey.

Some of Warnecke's original architectural drawings for 33 Thomas Street are labeled "Project

X." It was alternatively referred to as the Broadway Building. His plans describe the structure as "a skyscraper to be inhabited by machines" and say that it was "designed to house long lines telephone equipment and to protect it and its operating personnel in the event of atomic attack." (At the time the building was commissioned and built, amid the Cold War, there were genuine fears in the U.S. about the prospect of a Soviet nuclear assault.)

[026V0261-edit](#)



Sketch of the plaza at 33 Thomas Street.

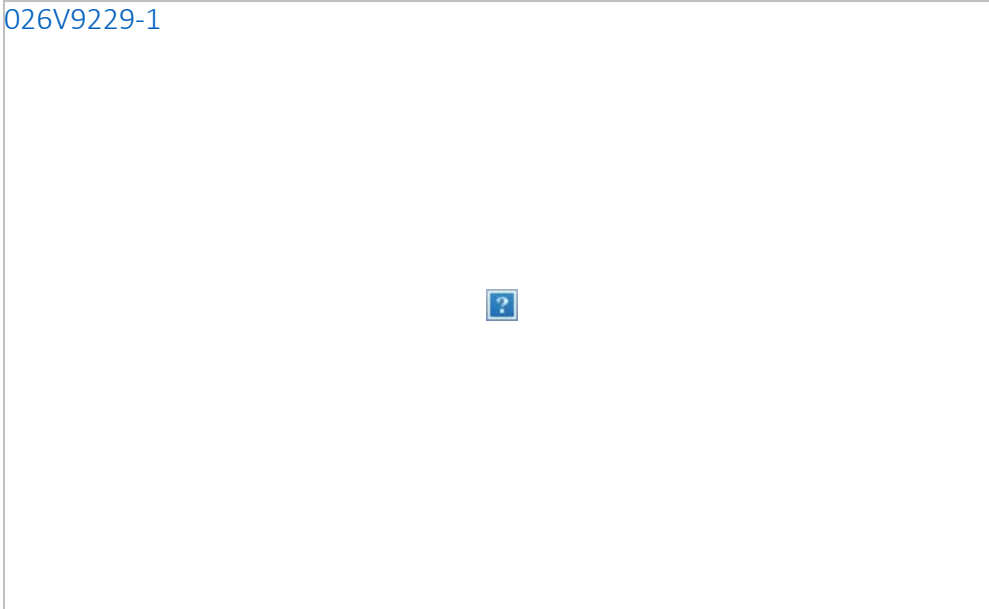
It is not clear how many people work at 33 Thomas Street today, but Warnecke's original plans stated that it would provide food, water, and recreation for 1,500 people. It would also store 250,000 gallons of fuel to power generators, which would enable it to become a "self-

contained city” for two weeks in the event of an emergency power failure. The blueprints for the building show that it was to include three subterranean levels, including a cable vault, where telecommunications cables likely entered and exited the building from under Manhattan’s bustling streets.

After it was built, the unusual style of 33 Thomas Street attracted a lot of attention. Its dark, somewhat dystopian appearance contrasted dramatically with other buildings in lower Manhattan. Yet it proved popular, particularly among architecture buffs.

In a 1982 [piece](#) in the New York Times, architecture critic Paul Goldberger praised 33 Thomas Street as “one of the neighborhood’s few pieces of good modern architecture,” adding that it “blends into its surroundings more gracefully than does any other skyscraper in this area.” “Other telephone company buildings from that era, designed solely for equipment, all look like horrible boxes,” Goldberger told The Intercept. “This one has an allure of its own to it. ... There’s something about that shape. You see it and you don’t see it at the same time.”

[026V9229-1](#)

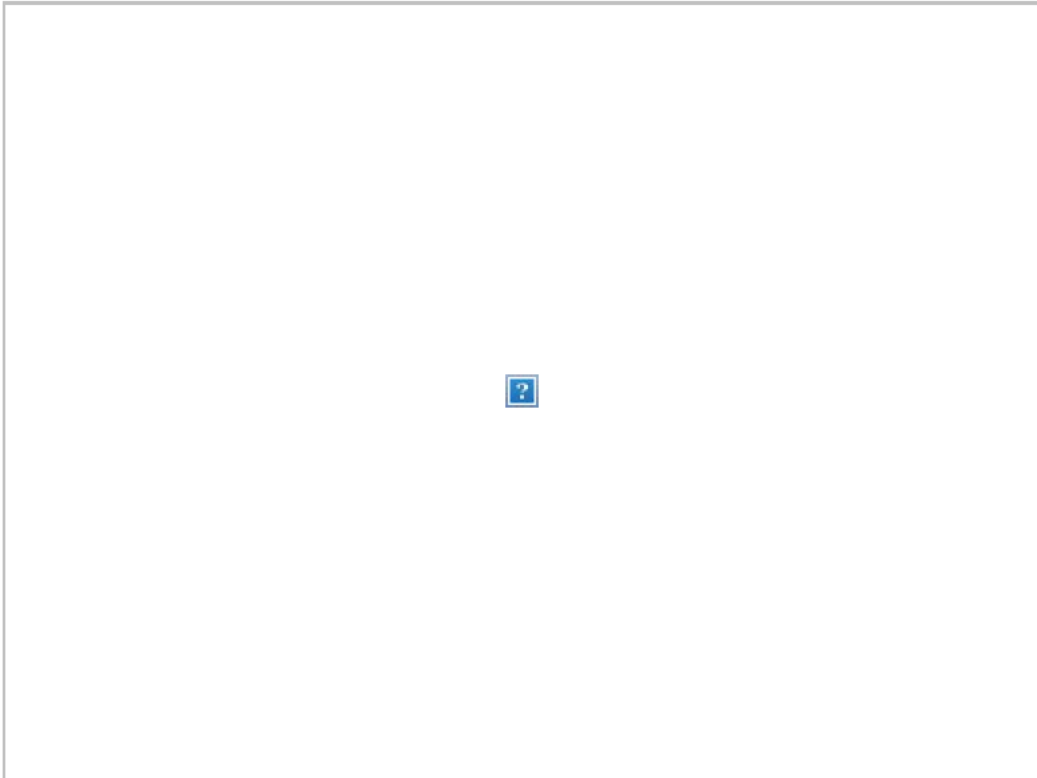


Satellite dishes on top of 33 Thomas Street. At TITANPOINTE, a program called SKIDROWE intercepts satellite communications.

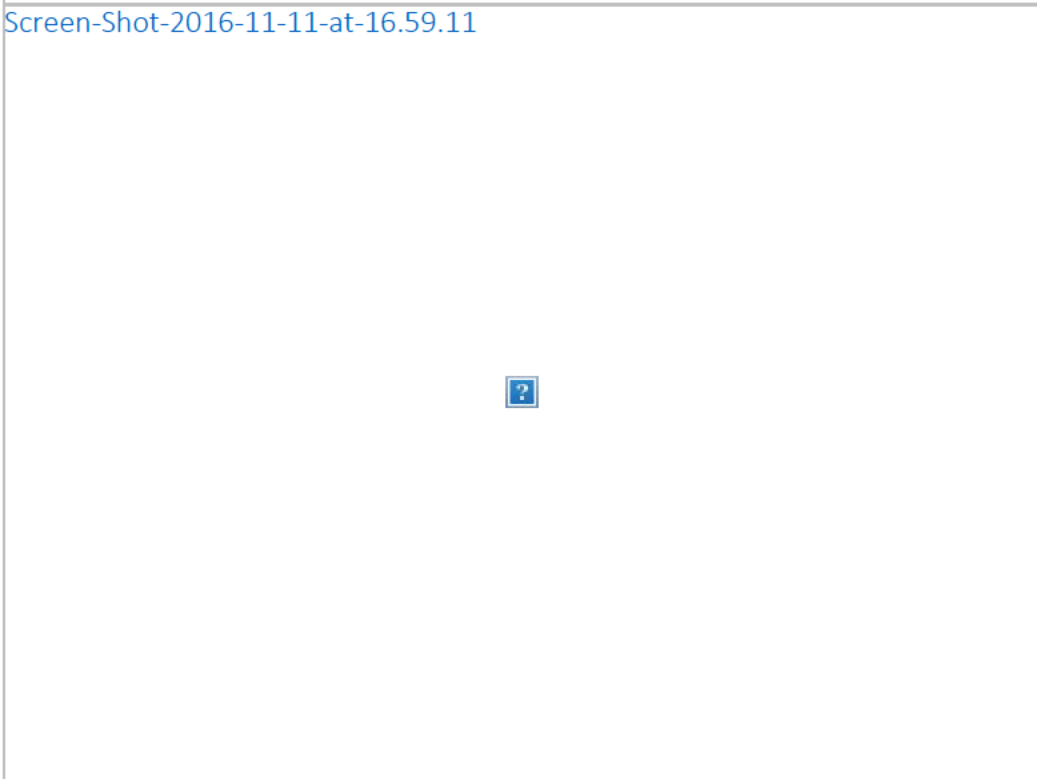
Photo: Henrik Moltke

In 1975, just a year after Warnecke’s 33 Thomas Street building was completed, the NSA became embroiled in one of the biggest scandals in the U.S. intelligence community’s history. Following revelations about domestic surveillance operations targeting anti-Vietnam War activists, a congressional select committee began investigating the alleged abuses. The inquiry, led by Democratic Sen. Frank Church, published its findings in April 1976. It concluded that U.S. intelligence agencies had “invaded individual privacy and violated the rights of lawful assembly and political expression.” Surveillance programs operated by the NSA through this period, it was later revealed, had targeted “domestic terrorist and foreign radical” suspects, including a host of eminent Americans, such as the civil rights leaders Martin Luther King and Whitney Young, the boxer Muhammad Ali, Washington Post columnist Art Buchwald, and New York Times journalist Tom Wicker.

The Church Committee recommended that new and tighter controls be placed on intelligence gathering. And in 1978, Congress approved the Foreign Intelligence Surveillance Act, requiring the executive branch to request warrants for spying operations from a newly formed court.



[Screen-Shot-2016-11-11-at-16.59.11](#)



Diagrams showing NSA-controlled equipment inside TITANPOINTE.

Document: NSA

Through this tumultuous time for American spies, the NSA established a new surveillance



program under the code name BLARNEY, which was first exposed in a Snowden-leaked slide published in 2013. According to a previously unpublished document provided to The Intercept by Snowden, BLARNEY was established in the early 1970s and, in mid-2013, remained one of the agency's most significant initiatives.

BLARNEY leverages "commercial partnerships" in order to "gain access and exploit foreign intelligence obtained from global networks," the [document states](#). It carries out "full take" surveillance — a term that refers to the bulk collection of both content and metadata — under six different categories: counterproliferation, counterterrorism, diplomatic, economic, military, and political.

As of July 2010, the NSA had [obtained at least 40 court orders](#) for spying under the BLARNEY program, allowing the agency to monitor communications related to multiple countries, companies, and international organizations. Among the approved targets were the International Monetary Fund, the World Bank, the Bank of Japan, the European Union, the United Nations, and at least 38 different countries, including U.S. allies such as Italy, Japan, Brazil, France, Germany, Greece, Mexico, and Cyprus.

The program was the NSA's leading source of data collection under the Foreign Intelligence Surveillance Act, an April 2013 document disclosed, and information gleaned from the communications it intercepted was a top contributor to the president's daily briefing. Notably, TITANPOINTE has played a central role in BLARNEY's operations. NSA documents dated between 2012 and 2013 list the TITANPOINTE surveillance facility among three of BLARNEY's "core sites" and describe it as "BLARNEY'S site in NYC." Equipment hosted at TITANPOINTE has been used to monitor international long-distance phone calls, faxes, voice calls routed over the internet (known as Voice-Over-IP), video conferencing, and other internet traffic.

In one case that may have involved 33 Thomas Street, NSA engineers with the BLARNEY program worked to eavesdrop on data from a connection serving the United Nations mission in New York. This spying resulted in "collection against the email address of the U.N. General leading the monitoring mission in Syria," an April 2012 memo said.

Mogens Lykketoft, former president of the U.N.'s general assembly, criticized the surveillance. "Such spying activities are totally unacceptable breaches of trust in international cooperation," he told The Intercept.

[skidrowe-keyscore](#)



Logo for the NSA's satellite communications exploitation program SKIDROWE.

NSA

At the TITANPOINTE site, the NSA equipment is stored inside a secure room, known as a "Sensitive Compartmented Information Facility." Top-secret [diagrams](#) dated April 2012 show that within the secure space there is "NSA controlled" equipment linked to the routers of its "access partner," referring to AT&T. Intercepted internet data was collected from the "backbone," then processed at TITANPOINTE, before being passed to NSA for storage. Phone calls that were intercepted were collected from TITANPOINTE's "foreign gateway switches" before being routed through the partner's "call processor." They were then forwarded to NSA's headquarters in Maryland through an interface shared with the partner.

Much of the surveillance carried out at TITANPOINTE seems to involve monitoring calls and other communications as they are being sent across AT&T's international phone and data cables. But the site has other capabilities at its disposal. The NSA's documents indicate that it is also equipped with powerful satellite antenna — likely the ones located on the roof of 33 Thomas Street — which monitor information transmitted through the air.

The [SKIDROWE](#) spying program focuses on covertly vacuuming up internet data — known as "digital network intelligence" — as it is passing between foreign satellites. The harvested data is then made accessible through XKEYSCORE, a Google-like mass surveillance system that the NSA's employees use to search through huge quantities of information about people's emails, chats, Skype calls, passwords, and internet browsing histories.

Fletcher Cook, an AT&T spokesperson, told The Intercept that the company does not "allow any government agency to connect directly to or otherwise control our network to obtain our customers' information. Rather, we simply respond to government requests for information pursuant to court orders or other mandatory process and, in rare cases, on a legal and voluntary basis when a person's life is in danger and time is of the essence, like in a kidnapping situation."

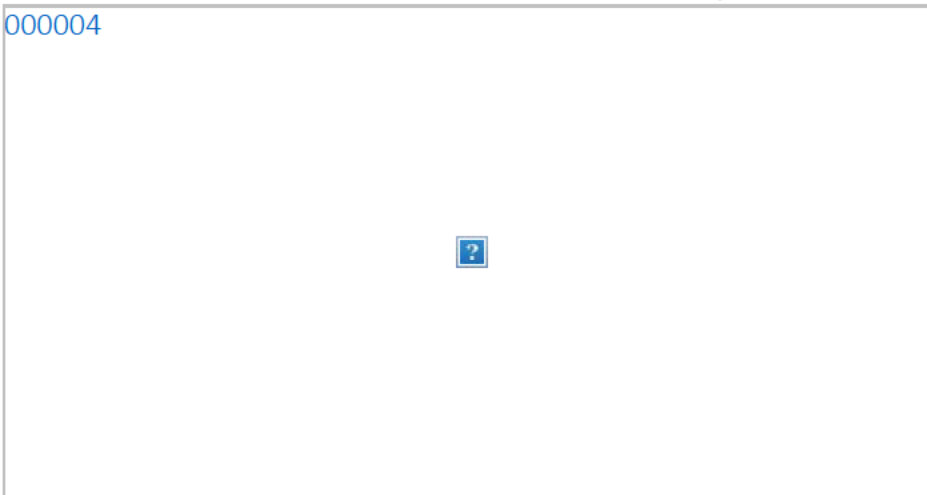
Cook added that NSA representatives "do not have access to any secure room or space within our owned portion of the 33 Thomas Street building." When pressed on whether *any* room within 33 Thomas Street contains equipment used for the purposes of NSA surveillance, an AT&T spokesperson pointed to a 1983 [deed](#) and [declaration](#) filed with New York City

indicating that Verizon's predecessor company maintained ownership of three floors and a basement floor in the building. The New York City Department of Finance said the predecessor company has an easement for the space and pays utility taxes, but insisted that AT&T owns the whole building. The AT&T spokesperson declined to comment further.

The NSA's documents do not state that it can "connect directly to" or "otherwise control" AT&T's networks, but they do make clear that the agency has placed its own equipment inside TITANPOINTE to tap into phone calls and internet data. It may be the case that the secure room where the equipment is installed is overseen by AT&T's own engineers or technicians who have a security clearance. One NSA document dated from March 2013 suggests such a relationship, noting that the "corporate sites" the agency collects data from "are often controlled by the partner, who filters the communications before sending to NSA."

As in 1983, AT&T may not be completely alone at 33 Thomas Street. Earlier this year, a technician working at the building — who did not want to be named because he was not authorized to speak to the media — told The Intercept that a handful of Verizon employees were still based inside. However, the NSA's documents do not suggest that Verizon is implicated in the surveillance at the TITANPOINTE facility, and instead only point to AT&T's involvement. Verizon declined to comment for this story.

000004



The entrance to 33 Thomas Street.

Still from "Project X"

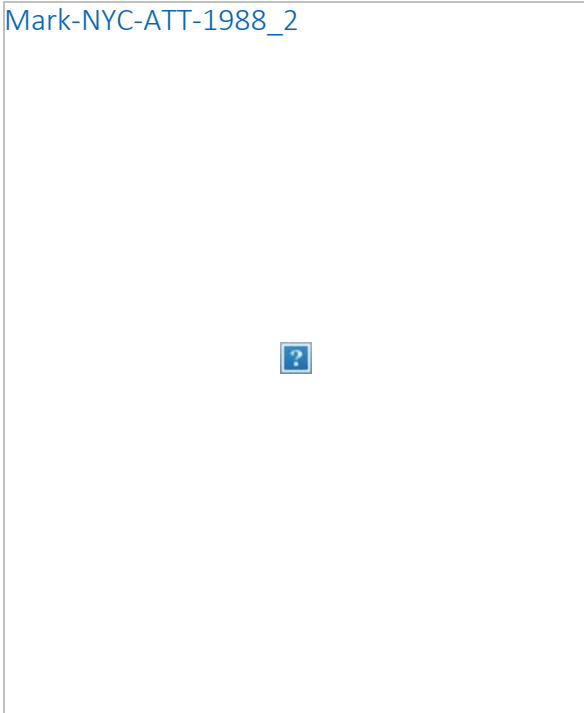
AT&T is far from the only company that has a relationship with the NSA. The agency has established what it calls "strategic partnerships" with more than 80 corporations. But some companies are more cooperative than others.

Historically, AT&T has always maintained close ties with the government. A good example of this came in June 1976, when a congressional subcommittee served AT&T with a subpoena demanding that it hand over information about its alleged role in unlawful FBI wiretapping of phone calls. President Gerald Ford personally intervened to block the subpoena, stating that AT&T "was and is an agent of the United States acting under contract with the Executive Branch." Ford said the company was in a "unique position" with respect to telephone and other communication lines in the U.S., and therefore it had been "necessary for the Executive Branch to rely on its services to assist in acquiring certain information necessary to the

national defense and foreign policy.” The details sought by the committee could not be shared, Ford asserted, because they could expose “extremely sensitive foreign intelligence and counterintelligence information.”

In more recent decades, as the New York Times and ProPublica [reported](#) last year, AT&T has allowed the NSA to access billions of emails, exhibiting what the agency called its “extreme willingness to help.” These revelations were foreshadowed in 2006 by allegations made by Mark Klein, a former AT&T technician. Klein stated that the company had maintained a “secure room” in one of its San Francisco offices, which was fitted with communications monitoring equipment apparently used by the NSA to tap into phone and internet traffic. Klein’s claims formed the basis of a lawsuit brought by the Electronic Frontier Foundation on behalf of AT&T customers ([Jewel v. NSA](#)), which remains ongoing today.

[Mark-NYC-ATT-1988\\_2](#)



Mark Klein at 33 Thomas Street in 1988. Klein worked as an AT&T employee at that location for 10 years.

Photo courtesy of Mark Klein

Coincidentally, between 1981 and 1990, Klein also worked for AT&T at 33 Thomas Street. “I wasn’t aware of any NSA presence when I was there, but I had a creepy feeling about the building, because I knew about AT&T’s close collaboration with the Pentagon, going way back,” he told The Intercept. When presented with the details linking 33 Thomas Street to NSA’s TITANPOINTE, Klein added: “I’m not surprised. It’s obviously a major installation. ... If you’re interested in doing surveillance, it’s a good place to do it.”

According to the Snowden documents, AT&T has installed surveillance equipment in at least 59 U.S. sites. And on any given day, NSA employees may be working at the company’s facilities. Classified memos dated from April 2013 describe one- to four-day deployments of NSA technical staff to TITANPOINTE and other buildings. Most AT&T personnel at these locations, however, are unlikely to have knowledge of the agency’s presence. NSA staff are

encouraged to wear clothes that make them “blend in to the environment.” Even the car hire company the agency uses for its trips to AT&T facilities is kept in the dark. “Some personnel are aware of the FBI link,” states the agency’s travel guidance, “but [they] have no knowledge of NSA’s involvement.”

*This article is the product of a joint reporting project between The Intercept and Field of Vision. “Project X,” a Field of Vision documentary directed by Henrik Moltke and Laura Poitras, will screen at IFC Center starting November 18.*

— — —

*Documents published with this story:*

- [BLARNEY site book](#)
- [FAIRVIEW site book](#)
- [FAIRVIEW dataflow charts April 2012](#)
- [Special Source Operations corporate overview](#)
- [BLARNEY report April 2013](#)
- [BLARNEY program overview](#)
- [SKIDROWE program](#)