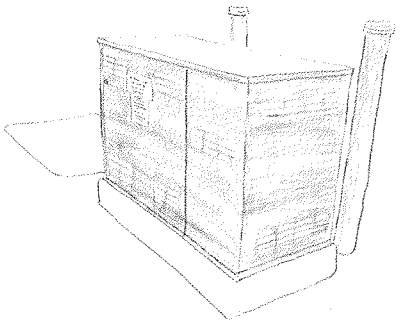
GROUND LEVEL

If staring at things on the ground isn't your thing (or you've realized the hazard of only looking down while crossing streets in New York), there are plenty of surface-level indicators of network infrastructure. They're usually not as colorful as street markings, but they're just as ubiquitous, if not more so, since they tend to be more permanent than spray paint. Many of them are wireless devices, sending signals through the air and relaying signals back to a cable network.

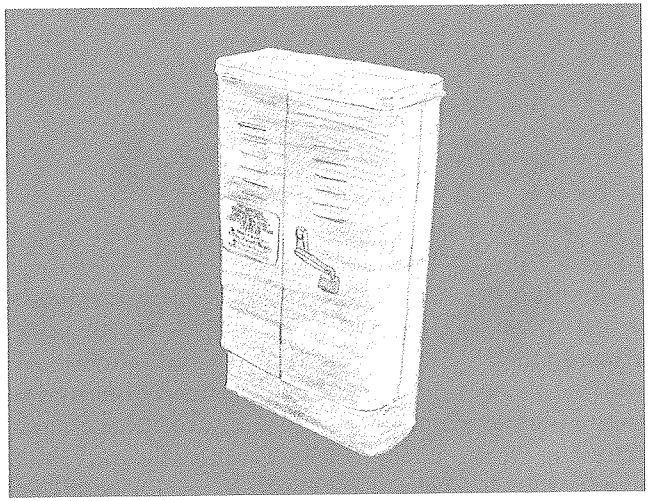
While we'll start with some examples of ground-level pieces of network infrastructure, this section also covers what might be called networked infrastructure—objects that receive or transmit data across a network but aren't connected to or accessible via the public Internet. These objects are mainly

used for city services. Finally, this section includes a very brief list of landmark buildings for New York City's network infrastructure. Because of security concerns, you probably won't be able to access the cool infrastructure parts of the buildings, but in at least a few of them the lobbies alone are worth checking out. These are also good starting points for beginner infrastructure-sightseers to train themselves to search for infrastructure on the street. Since these buildings hold major concentrations of fiber, their perimeters tend to have a lot of orange spray-paint markings and relevant manhole covers.

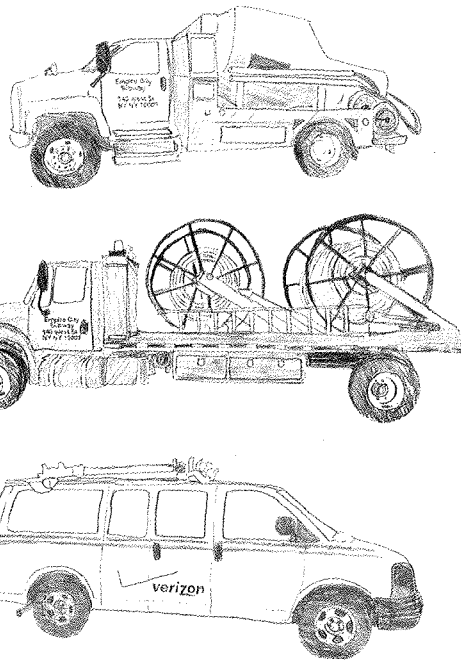
JUNCTION BOXES



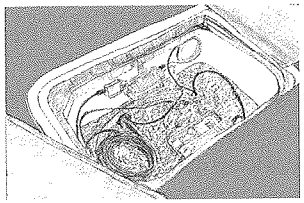
For objects that are so bulky and obtrusive, it's surprising how easy it is to miss these gray and green boxes on the street. More common in outer boroughs than in Manhattan, these boxes are basically the ground-level switching stations for home cable connections. Within these boxes are thousands of wires and cables for telephone, television, and the Internet, all coming from nearby buildings. In the junction box, those cables get connected to terminals that are themselves spliced into the underground cable network.

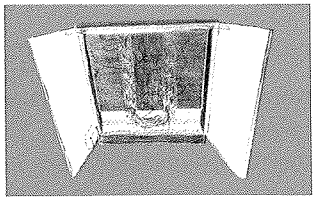


PEOPLE WORKING IN OPEN TELECOMMUNICATIONS MANHOLES



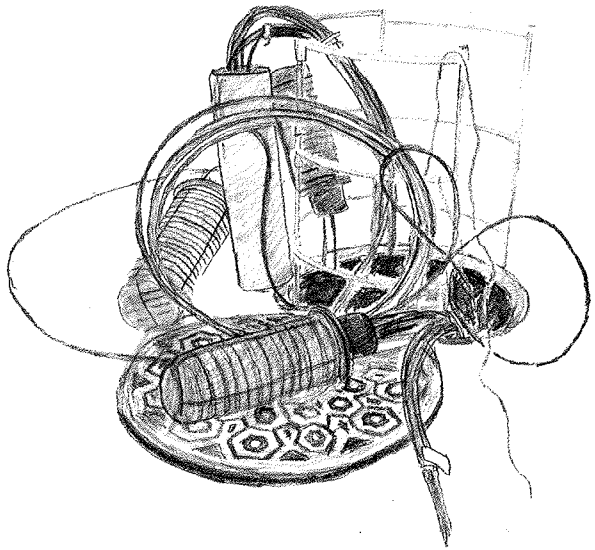
Most of the time, construction or street excavation work is something that people in most cities try to walk around rather than stop to look at. Good indicators of whether the work happening at a particular site is telecommunications-related are the types of vehicles surrounding the site and the kinds of equipment and cables visible. It's also helpful to look for certain company





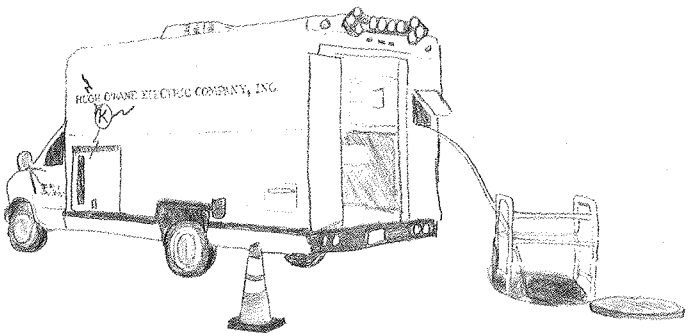
names. (Verizon, Empire City Subway, and Hugh O'Kane Company are among the companies most commonly seen working in Manhattan ducts.)

Sometimes it's possible to take a peek inside an open manhole or handhole to see what's going on under the street. In open manholes, you'll often see large cylinders into which a whole bunch of cables feed in and maybe only one cable feeds out. These cylinders are fiber splice enclosures, where different fiber optic cables get spliced into another cable. In handholes like the one illustrated here, you'll sometimes see devices that connect and convert signal from coaxial cable into optical cable and feed older coaxial from buildings into a fiber network.



Hugh O'Kane Electric Company

Founded in 1946 as a general electric and maintenance contractor, Hugh O'Kane Electric Company is now one of the top independent fiber installation contractors in New York City. It pulls and splices cable for most of the major networks in the city. In 2002, the O'Kane family created Lexent Inc., which owned and operated dark fiber services company Lexent Metro Connect until 2010, when the company was sold to Lightower. The O'Kane family has apparently continued to work in the fiber leasing world, and many former Lexent employees work for network services startup ZenFi, which shares an office address with Hugh O'Kane Electric Company.

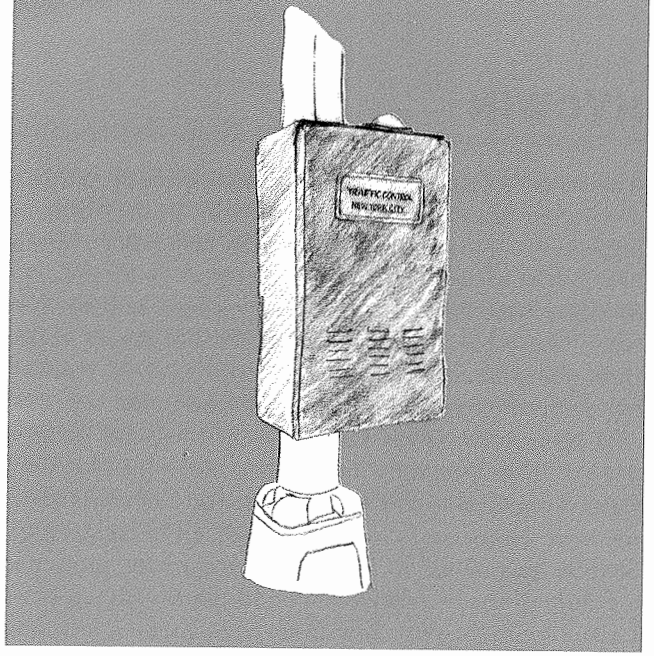


NYCWIN

The New York City Wireless Network (NYCWiN) is a citywide broadband wireless network project initially proposed in 2004 for emergency first responders. While NYCWiN itself isn't necessarily easy to "see" since it's mostly a bunch of cell towers comprising a wireless network, the actual impact of NYCWiN is pretty visible through certain devices connected to its network, including the next two devices described in this guide.

Construction of the network began in 2006 under a $500 million contract with defense contractor Northrop Grumman ($20 million of which came from a Department of Homeland Security grant), and the network became operational in 2009. Some regard the project as a failure given its relatively limited use by city agencies (according to the *New York Daily News* in 2012, less than 15 percent of the network capacity is used on a daily basis) and its exorbitant cost (around $40 million annually just to maintain).

In 2015, the city announced a Request for Expression of Interest and Information (REOI) seeking potential vendors to take over NYCWiN operations. Essentially the vendor would buy the network from the city and then resell municipal services on the network (public Wi-Fi, city agency services, etc.) back to the city. As of this writing, it's unclear what, if any, vendor would take over NYCWiN from the city.

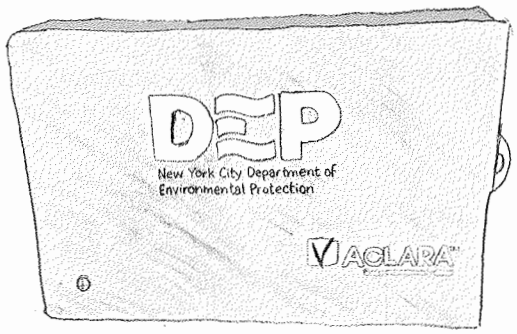


TRAFFIC SIGNAL CONTROLLERS

When first introduced in the 1950s, traffic signals operated electromechanically, using simple timers that changed traffic lights at fixed intervals. Over time, these systems became computerized and networked. Given the size and complexity of New York City's traffic network, it makes sense it would develop an equally massive and complex system of sensors and networked objects to control it.

The dark green signal control boxes attached to traffic signal posts throughout New York are just one piece of a massive system of networked objects. The system, designed by the Nashville–based transit services company TransCore, combines data collected by real-time traffic cameras, RFID (radio frequency identification) scanners, and other field sensors to create traffic signal times that adapt to the immediate conditions of traffic. Each signal control box contains wireless routing equipment and traffic controllers that connect back to a fiber hub. The little green dome on top of the signal control is actually a powerful wireless router used for communicating with the other sensors in the traffic network and the city's Traffic Management Center in Long Island City. Initially piloted in 2011 and slowly rolled out to New York City's over 12,500 traffic signals, this system couldn't have really come to fruition without NYCWiN, which provides the communications backbone that enables all these pieces of the traffic system to talk to one another.

AUTOMATED WATER METERS

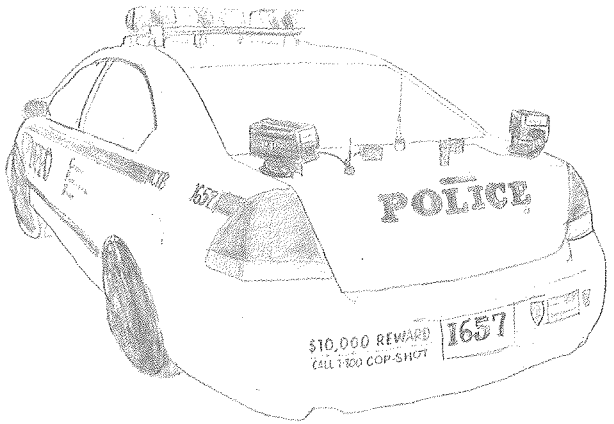


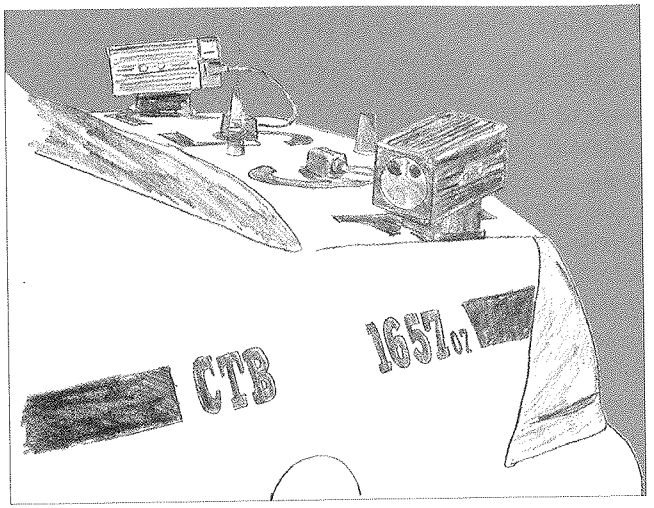
Aside from the Department of Transportation, the other major user of NYCWiN is the Department of Environmental Protection (DEP), who implemented a network of automated water meters in 2008. The meters are connected to low-power radio transmitters that send meter readings to NYCWiN antennae on city rooftops, which in turn send those readings to the DEP's servers. The readings are used to verify billing for water use and to detect potential leaks.

MOBILE LICENSE PLATE READERS

There are more than 34,000 police officers in New York City and more than 8,000 police vehicles. While police cars were networked to each other long before the Internet thanks to radio communications, in the last few years the NYPD has pursued increasingly impressive networked tools to help cops do their jobs.

Starting around 2006, NYPD began equipping some NYPD cars with Automated License Plate Readers (APLRs), devices that photograph and store records of license plates of vehicles on the street. The APLRs on NYPD vehicles are manufactured by ELSAG North America, a subsidiary of Italian company Finmeccanica. Its Mobile Plate Hunter-900 can capture up to 1,800 license plate reads per minute. The camera takes a picture of a passing vehicle's plate and then processes that image into raw letters and numbers that feed into a central database maintained by the NYPD. These plate





records, which include the location, date, and time that the plate was captured, are kept in NYPD databases for five years.

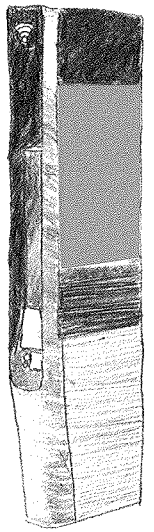
While law enforcement tends to point to the usefulness of ALPRs in tracking down stolen vehicles, the NYPD's first foray into the technology began as part of what was then called the Lower Manhattan Security Initiative, a post-9/11 project that initially focused on security for the Financial District and later expanded to include Midtown and then the rest of the city. In other cities throughout the United States, state and municipal police departments have also acquired ALPRs in the service of counterterrorism or security, as federal agencies like the Department of Homeland Security, the Drug Enforcement Agency, and Customs and Border Protection offer grants to help police departments purchase this type of technology. The majority of vehicles I've seen with ALPRs are marked as CTB—Counterterrorism Bureau.

ALPRs aren't only vehicle-mounted; the devices are also placed at street intersections and bridge and tunnel

entrances, sometimes used in conjunction with speed cameras. As of 2013, the NYPD had fewer than 400 ALPR devices, some of which were vehicle-mounted and some of which were not. And that same year, the NYPD collected more than 16 million records of license plate data.

In 2015, the NYPD signed a $442,500 contract with license plate reader company Vigilant Solutions for a subscription to their ALPR database, which boasts 2.2 billion records of nationwide license plate data. Since its founding in 2005, Vigilant built up its database by selling ALPRs to vehicle recovery and repossession companies, which would passively collect license plate data as company tow trucks drove throughout a city and then send that data back to Vigilant. The company has a pretty strict terms of service policy that prevents police departments from discussing the program or its services with the media, so there's little public information about what the NYPD is doing with these records aside from the initial announcement of the contract.

LINKNYC: FUTURE NETWORKS OF NEW YORK



In 2012, Mayor Michael Bloomberg announced the Reinvent Payphones Design Challenge, a competition seeking proposals for new initiatives to replace the city's thousands of unused and sometimes unusable public payphones with new technology that could be more accessible and functional for today's city residents. After a lengthy review process, the city announced in 2014 the selection of a proposal called LinkNYC, a network of free wireless hotspots throughout the city. The company behind LinkNYC, CityBridge, was actually a consortium of four companies (Titan, Control Group, Qualcomm, and Comark) that specialized in various facets of the project. The "links" are supposed to offer free Wi-Fi, a touchscreen tablet with maps and other useful local information, domestic phone calls, and charging stations for mobile devices. They also offer advertising space, which is how LinkNYC intends to cover the cost of the service.

While using advertising to support municipal services isn't a radically new idea in New York (just look at the subway system!), LinkNYC's reliance on advertising revenue has raised concerns that the initiative may only further increase the city's existing digital divides rather than decrease them. After the project's initial announcement, the *New York Daily News* reported that the connection speeds offered on LinkNYC kiosks without advertising—primarily kiosks in lower-income

neighborhoods—would be much slower than the speeds available on the kiosks with advertising. While the city has argued that this tiered system is temporary and still better than nothing, it is unclear whether advertising revenue will be enough to cover the costs required to bring high-speed fiber cables into neighborhoods that currently don't have them.

Similar to the negotiations that led Empire City Subway to become a subsidiary of Verizon, LinkNYC's consortium has also been reshaped by that familiar alchemy of mergers and acquisitions. In between the initial announcement of LinkNYC and the installation of its first test nodes in the East Village in winter 2015, Google (now Alphabet) subsidiary Sidewalk Labs acquired and merged two of the major companies working on LinkNYC: Titan (the franchise holder for most of the city's existing pay phones) and Control Group (the company largely responsible for the functionality of the kiosks, best known for its work on the MTA subway system's information touch screens). This is one way of saying that the mega-corporation behind Google now has a small but significant share of and role in New York City's pilot program to provide ad-supported public Wi-Fi.

LinkNYC is a promising endeavor from the city to bridge local digital divides, though it's far from the first one. In the Brooklyn neighborhood of Red Hook, local nonprofit Red Hook Initiative has been operating a local wireless mesh network, Red Hook Wi-Fi, since 2011, and in 2013 the Bloomberg administration rolled out a free Wi-Fi network in Harlem designed to cover ninety-five square blocks. LinkNYC's chief distinctions are its installation of a custom hardware unit (the actual "link" kiosk), which appropriates the existing network infrastructure of the telephone grid, and its particular brand of ad-supported public-private partnership.

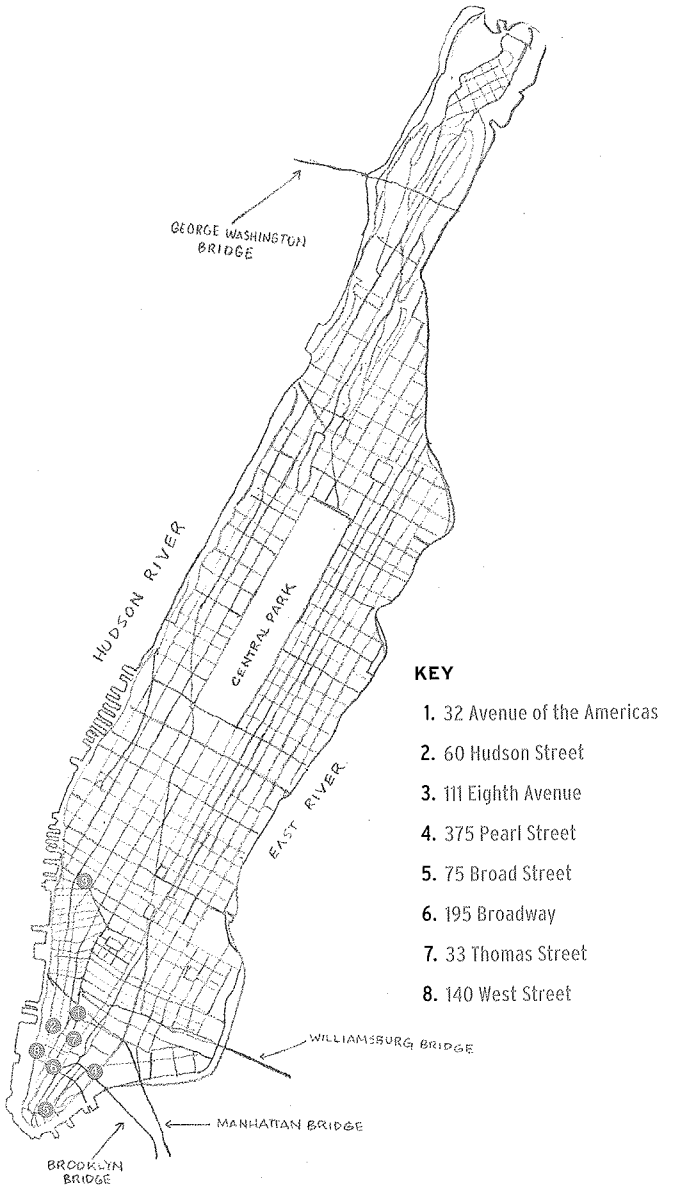
As of this writing, 134 links have been installed

throughout the city. While the program has mostly been lauded for its ambition and technical achievements, the New York Civil Liberties Union has raised concerns about possible risks faced by LinkNYC users based on the terms of CityBridge's privacy policy. The policy states that CityBridge collects a tremendous amount of user data (including information about a user's device and their on-line activity) that may be used for a variety of purposes, from technical administrative applications to "[providing users] with information about goods or services that may interest [them]"—an indication that the ad-supported service will seek far greater granularity in its targeting than a mere street-level banner advertisement. The NYCLU has also raised concerns about CityBridge sharing user data with law enforcement. While all of these concerns are extremely valid, the fact that LinkNYC is a private company makes it difficult to hold them accountable—they have no public service prerogative to protect or delete user data, and every business incentive to collect and keep it. To paraphrase George Orwell, if you want a vision of the future of public Wi-Fi, imagine a corporation doing exactly the kind of vaguely slimy things corporations do by design—forever.

CARRIER HOTELS AND DATA CENTERS: ARCHITECTURE FOR THE INTERNET

Sometimes people who want to learn about seeing Internet infrastructure ask me to tell them "where the Internet lives." At first glance, this seems like a bit of a misnomer—the Internet isn't a static object, it's defined by the constant movement of information. It doesn't "live" anywhere; it's already everywhere at once—it "lives" in the library down the street, in office buildings, in undersea cables. But there are a few specific types of buildings that hold crucial pieces of Internet infrastructure—less homes for the Internet than waystations that data traffics through. While we'll look a bit at data centers in this section, the buildings we'll primarily focus on are often called "carrier hotels" because it's sort of where different ISPs and network companies "check in" with one another.

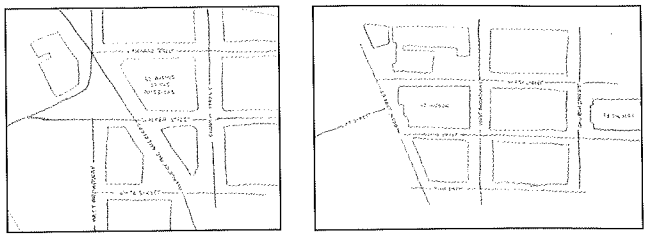
Imagine someone sitting at home trying to watch something on Netflix. They click on a movie they want to watch and that click sends a request to Netflix's servers saying, "Hey, bring me the movie *Terminator 2: Judgment Day*!" The person watching Netflix is connected to the Internet via Company A, and Netflix is connected to the Internet via Company B. At some point, the request for *T2* has to move from the Company A network to the Company B network, and carrier hotels are where it happens. Racks and racks of switching equipment and cables run through these buildings, which are also sometimes called "Internet exchanges" or "meet-me rooms" since it's where networks meet one another.



In general, these aren't spaces that are open to the public for tours—in one of them, you're not even allowed to take photos of the lobby. This limited access is typical of major network infrastructure nodes. To some extent this has to do with (valid) security concerns, but from my own experiences attempting to get into these spaces, I suspect the managers of these spaces just don't want to deal with infrastructure tourists. (Unfortunately society does not yet view Internet infrastructure with the same reverence or civic zeal as it does other tourist-worthy infrastructure like the Hoover Dam.) But getting inside the server room, while an exciting experience, isn't necessarily required to appreciate these buildings or their role in the network.

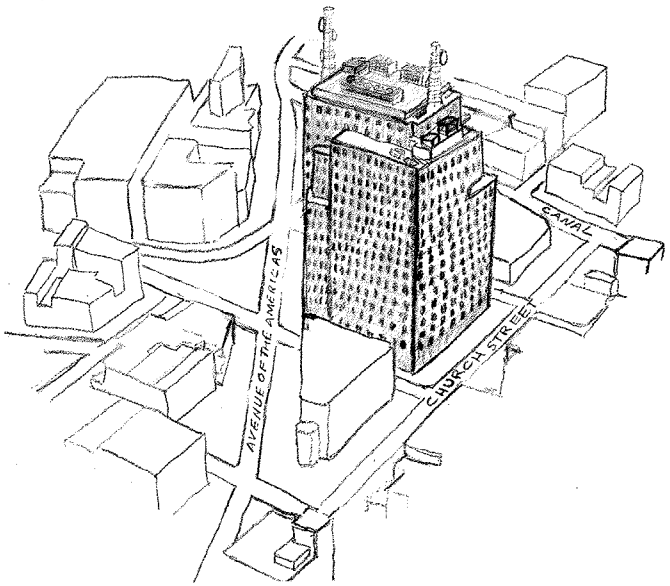
In most of the United States, new infrastructure has a tendency to inherit the landscapes of past infrastructure—Internet cables follow telephone lines, which follow telegraph lines, which follow railroads. New York City's Internet infrastructure is no exception. Although there are other data centers and sites of network exchange throughout New York (I particularly regret not having space for the Staten Island Teleport), this section focuses on buildings around Downtown and Lower Manhattan because of the major role these areas have played, and continue to play, in the history of New York's telecommunications infrastructure.

60 HUDSON STREET AND 32 AVENUE OF THE AMERICAS



New York's Internet history is deeply intertwined with the history of the telegraph and the telephone, and the two buildings that best represent that history are 60 Hudson Street and 32 Avenue of the Americas, which are both located just below Canal Street in Downtown Manhattan.

The stories behind both of these buildings in some ways begin over at 195 Broadway, the original New York



headquarters of the American Telephone and Telegraph Company and Western Union (a space used for offices by AT&T until 1978). In 1914, switching equipment for both companies was moved to 24 Walker Street, but eventually Western Union outgrew this space and in 1928 commissioned the architecture firm Voorhees, Gmelin & Walker to design what would become 60 Hudson Street. In turn, AT&T hired the same firm to create a new building in the same footprint as its Walker Street building and completed 32 Avenue of the Americas in 1932.

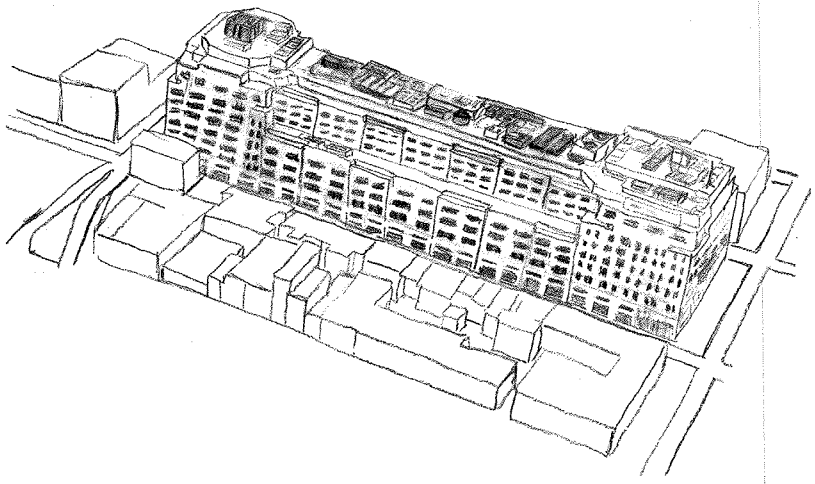
Since so much of AT&T's and Western Union's operations overlapped with each other, the creation of the two separate buildings, less than ten blocks apart, also meant the creation of a dense underground cable duct infrastructure. Beneath Church Street, rows and rows of conduit filled with copper wires connected 60 Hudson Street to 32 Avenue of the Americas. As a result, 60 Hudson Street became a major telephone exchange site during the deregulation of the U.S. telephone industry in the 1970s, when nascent competitor telephone companies like MCI and Sprint rapidly moved their equipment into the building in order to take advantage of this duct infrastructure, which made it extremely easy to connect their networks to AT&T's network. 60 Hudson Street's evolution into carrier hotel followed naturally from this period—today, it is home to hundreds of Internet companies' equipment and has the largest concentration of connections to transatlantic cables on the East Coast. 32 Avenue of the Americas's conversion to carrier hotel began with its acquisition by real estate company Rudin Management in 1999.

Not only are both buildings hubs of communication, but they are also magnificent examples of the Deco period in which they were created. Their lobbies harken back to a time when telecommunications had an air of grandeur and idealism (and the wall mosaics at 32 Avenue of the Americas building are an absolute must-see for this).

111 EIGHTH AVENUE

Built in 1932 when Manhattan's ports were far more active in shipping and trade, 111 Eighth Avenue was initially the Port Authority Commerce Building, a warehouse and center for the transport and storage of packaged freight goods, and later became home to some Port Authority offices. In 1998, Taconic Investment Partners turned it into a carrier hotel. In 2010, Google purchased the building for nearly $2 billion. While Google uses a majority of the building for its own office space, the carrier hotel and a number of ISPs, startups, and ground-level retail stores remain. 111 Eighth Avenue is interesting in itself, but it's also a compelling site because of its Chelsea neighbors. Sometimes I think of it as a metaphor for the Internet itself—a weird palimpsest of law enforcement, network infrastructure, spectacle, and commodities.

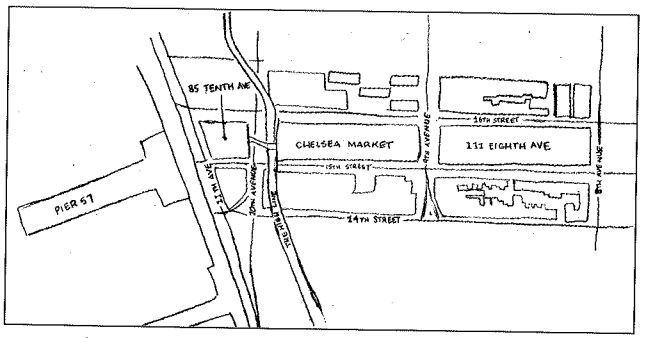
No building near 111 Eighth Avenue better reflects this idea than Chelsea Market. Formerly part of the National Biscuit Company's factory, the block-long building is now an upscale mall and food court. Restricted-access



elevators lead to the offices of several cable channels, real estate companies, and other tenants. Google leases three floors of the building too.

Chelsea Market is also home to the NYPD Intelligence Division, which was formed after 9/11 and became notorious for its massively overreaching operations for spying on Muslims. The earliest reference to the existence of the Intelligence Division in Chelsea Market that I found was a redacted NYPD document detailing plans for the 2004 Republican National Convention. The executive summary notes that an "Intelligence Fusion Center" was located in Chelsea Market and served as the "main intelligence gathering and dissemination center" during the Convention. A 2012 document made by Chelsea Market's developer, Jamestown Properties, lists the NYPD as an office tenant occupying 48,000 square feet (for comparison, Google occupies 108,000 square feet in the same building).

Past the Chelsea Market and above the High Line, an enclosed footbridge connects the market to 85 Tenth Avenue, another former National Biscuit Company building turned into a mix of luxury retail, technical infrastructure, and law enforcement. The building is home to a Level 3 colocation center, ground-level expensive restaurants, 360,000 more square feet of Google offices, Möet



Hennessy's New York offices, and the FBI's Joint Terrorism Task Force.

The JTTF began as a partnership between the NYPD and the FBI in 1980 while investigating the Puerto Rican paramilitary organization Fuerzas Armadas de Liberación Nacional (FALN). Essentially, it's a program designed to make it easier for city police departments and the FBI to work together on investigations rather than having the two agencies work separately on the same case. Today, it has offices in 103 cities; 71 of those offices were created after 9/11.

According to a General Services Administration document from 2014, the JTTF has been at 85 Tenth Avenue since 2005 and intended at that time to renew its lease through 2020 or until it could move to another "government-owned location." It's unclear whether they chose the location for its proximity to Internet cables (Level 3 acquired its colocation space in 1999) or for its raw post-industrial interior, which can accommodate its unusual architectural needs. In *Enemies Within*, a comprehensive volume on the NYPD Intelligence Division, the authors Matt Apuzzo and Adam Goldman describe a "cavernous" secure compartmentalized information facility (SCIF, a fancy acronym for "surveillance-proof government building") on the tenth floor, and a 2015 House of Representatives document approving the lease renewal noted that the task force rented 168,000 square feet at an annual cost of around $13 million. The footbridge above the High Line that connects the building to Chelsea Market is supposedly a direct link between the Intelligence Division and the JTTF, although it remains locked—communication across agencies is apparently Not Their Thing.

One less obviously relevant but still interesting landmark in this accidental luxury-as-cloaking-device tour is located across the West Side Highway from 85 Tenth Avenue: Pier 57, which is currently under development

by Youngwoo & Associates to be a luxury retail site rebranded as the SuperPier. The building, a former MTA bus repair center, is more familiar to some as "Guantanamo on the Hudson" due to its use as an arrest holding site for an estimated 1,200 protesters during the 2004 Republican National Convention.

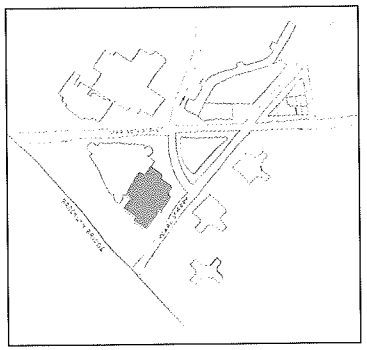
In a press statement following several settlements to RNC cases in 2014, the National Lawyers Guild described conditions in Pier 57 circa 2004:

> . . . cyclone fencing was used to create cages in a warehouse-like area still covered with grease and brake fluid. Signs still hung from the walls warning workers to wear hazmat suits. There was no heat, no place to lie down, and a handful of port-a-potties. Protesters were held in these disgraceful conditions for up to 48 hours before being transported to court facilities—long enough to exhaust them and keep them off the streets until after George Bush was re-nominated. Many left with skin rashes and respiratory problems, and some developed more serious medical conditions.

No word as of yet on whether SuperPier tenants Opening Ceremony or Google will incorporate the Guantanamo-on-the-Hudson aesthetic into their interior design.

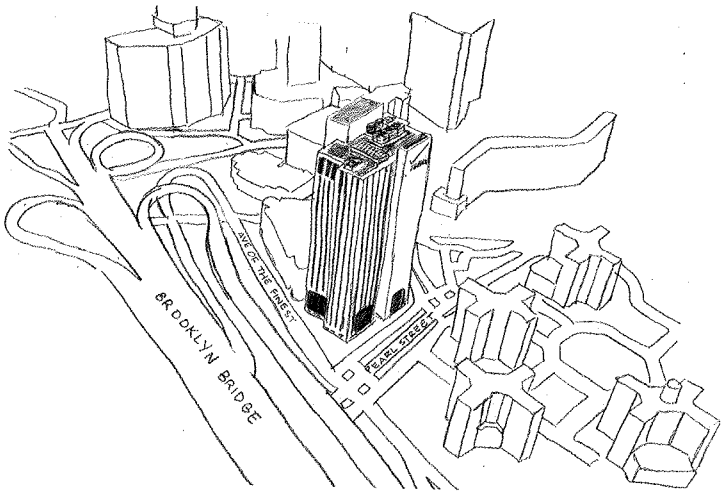
That an industrial bakery like National Biscuit Company and a Port Authority warehouse would be transformed into a data center and an Internet exchange is perhaps not a surprise, given infrastructure's tendency to inherit the spaces of preceding technologies (the same could be said for Google's steadily increasing footprint in the area). The presence of high-end retail in former industrial spaces is also a familiar narrative; spaces for other people's leisure love to evoke nostalgia for other people's labor. Law enforcement's placement within this landscape is probably more pragmatic than poetic (raw industrial spaces reworked for retail can be as easily reworked for government-specified security standards), but there is something weirdly dislocating about walking through the retail corridors along Fifteenth Street, aware of the layers of state and infrastructural control a few floors aboveground and layers of fiber-optic networks several meters underground—systems and histories mostly glimpsed by following orange spray-paint markings from Eighth Avenue to the end of Fifteenth Street.

375 PEARL STREET



Relatively younger and decidedly less Deco than other major connection points in Manhattan, 375 Pearl Street was built in 1975 as a switching station for the New York Telephone Company. Taconic Investment Partners (the same company that turned 111 Eighth Avenue into a carrier hotel) purchased the building in 2007 with grandiose plans to transform its much-derided windowless exterior and add new office space and condominiums. The economic collapse of 2008 pretty much killed that plan, and 375 Pearl Street ended up being sold at a massive loss to Sabey Data Center Properties in 2011. Sabey rechristened the building Intergate Manhattan, describing it in publicity materials as "the world's tallest data center."

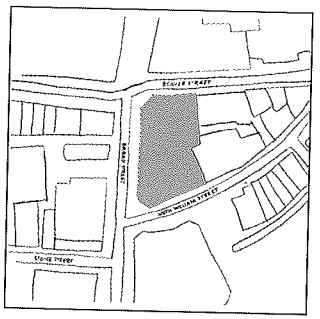
As with 111 Eighth Avenue, 375 Pearl Street is consid-



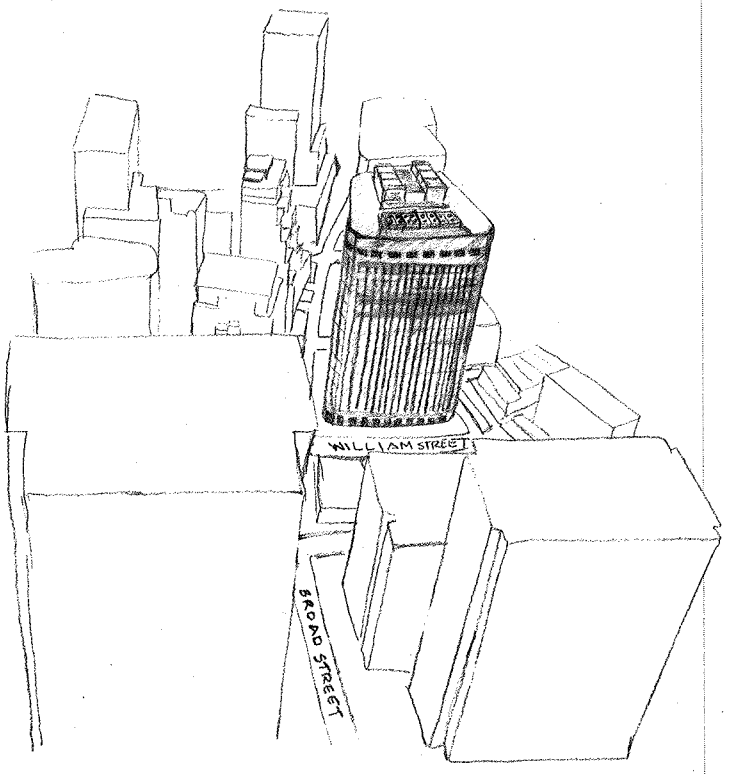
ered remarkable in part due to what's around it, or more specifically what surrounds it. Its next-door neighbor is 1 Police Plaza, the NYPD's headquarters, so the building has police checkpoints on almost every side.

75 BROAD STREET

There are a few small indicators that this building in the heart of Manhattan's Financial District was once the heart of a major telecommunications company. Built in



1929, 75 Broad Street was originally the headquarters of the International Telephone and Telegraph Company (ITT), a telecommunications conglomerate founded in 1920 through the acquisition of various Caribbean and European communications companies. ITT established its U.S. presence by acquiring industrialist John William Mackay's various telecommunications ventures: the Commercial Cable Company, the Commercial Pacific Cable Company, Postal Telegraph, and the Federal Telegraph Company. The building entrance at the corner of Broad and William Streets features a mosaic depicting an angel foregrounded by maps of the Eastern and Western Hemispheres, apparently connecting the two sides of the world with the wonder of communications technology (depicted here as lightning bolts). ITT's colorful history may be too voluminous of a detour within this guide (highlights include: collaboration with the Nazi party and



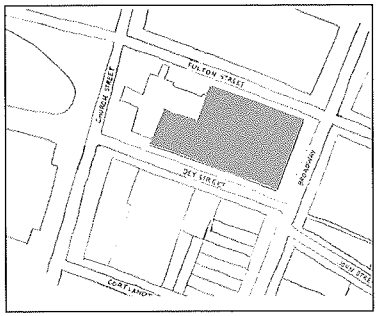
Nazi-sympathetic governments, working with the CIA to covertly finance the 1973 coup of Chilean president Salvador Allende, being bombed by the leftist radical organization the Weather Underground for involvement in the Chilean coup, and being the subject of the Fela Kuti song "International Thief Thief"—seriously, this company was really evil). In any case, it had left 75 Broad Street by 1961 and sold off its telecommunications assets to what would become Alcatel-Lucent in 1986. It wasn't until 1999 that Newmark and Company repurposed several floors of the building into a data center.

75 Broad Street's central Lower Manhattan location, while great for its proximity to Manhattan carrier hotels, proved terrible in 2012 when Hurricane Sandy hit the New York City area. Although the data centers had backup generators, the building's data center operations were on the eighteenth floor, which meant that operations managers had to carry fuel up eighteen flights of stairs while the power was out throughout the Financial District.

OTHER NEW YORK TELECOMMUNICATIONS LANDMARKS

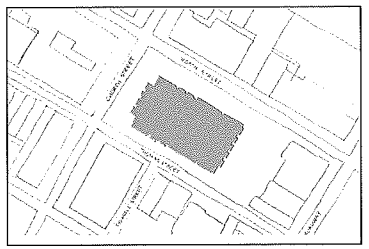
While some of these buildings have little or no remaining telecommunications equipment, they are notable landmarks of New York's network history, worth checking out if you have the chance to do so.

195 Broadway



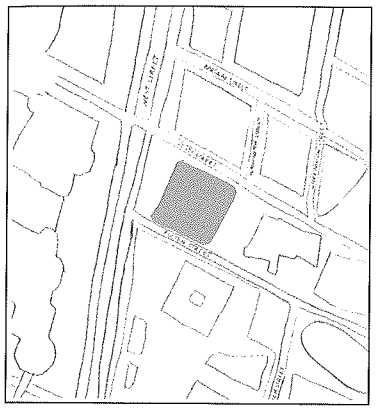
The original headquarters of AT&T and Western Union prior to the creation of 60 Hudson Street and 32 Avenue of the Americas. It was used as AT&T's offices between 1916 and 1978, and in 1927, the first transatlantic telephone call—between London and New York—took place here.

33 Thomas Street



Another AT&T Long Lines building, 33 Thomas Street, was completed in 1974. It was and still is mostly used for telephony services, but it's both a Brutalist monstrosity of a building and highly visible on the horizon from both 60 Hudson Street and 32 Avenue of the Americas, so it bears a quick mention.

140 West Street



Constructed in 1926 by the same architects as 60 Hudson Street and 32 Avenue of the Americas, 140 West Street was the headquarters of the New York Telephone Company, the predecessor company of Bell Atlantic and, later, Verizon. While today it only has a limited amount of switching equipment, it's notable in part because of the damage it incurred during, and repairs made after, the 9/11 attacks.

ABOVE GROUND

In this section, we'll look at objects that tend to be above eye level—mostly wireless devices transmitting signals across networks. Some of these networks are the hardest to see, since they either reside on rooftops or above traffic intersections (which, in New York, aren't exactly a good place to linger). But as more and more Internet usage moves to wireless devices like smartphones and tablets and as more and more wireless devices become part of the regulation and management of citywide logistics and public safety, wireless infrastructure becomes increasingly crucial to understanding how people live with the Internet—with networked objects in general—in cities.

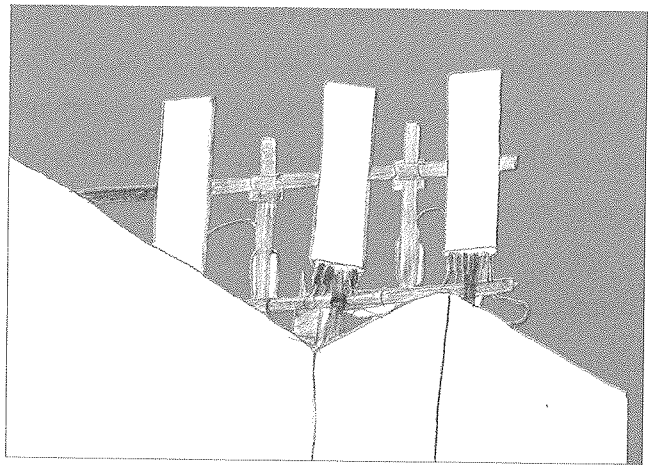
Some of the networks in this section are not the obvious ones typical users "connect to" regularly, like the public Internet. Surveillance cameras are perhaps one of the most noticeable—and contested—examples of non-Internet networked objects in public space. Traffic sensors are another. The public's "connection" to these networks is admittedly more oblique than connecting to a cell tower, but we do connect with them frequently simply by engaging with and in public space.

CELL TOWERS

When out and about on the street, more and more people connect to the Internet through wireless networks. For many, seeing the Internet on the street just means using a smartphone. Since those wireless operations happen at a level invisible to the human eye, it might be helpful to explain what exactly is going on when phones connect to cell networks.

To start with: cell phones are basically screaming all the time. We can't hear them screaming because they scream in radio waves, but they're constantly announcing their existence to other antennae via these radio signals. They're not saying all that much most of the time—more or less just "Hi! I'm here! I'm looking for a network to connect to!"

If the phone is close to a cellular tower with an antenna that connects to that phone's particular carrier, it connects to the network via that antenna. If the phone moves away from that antenna or gets out of range of it,

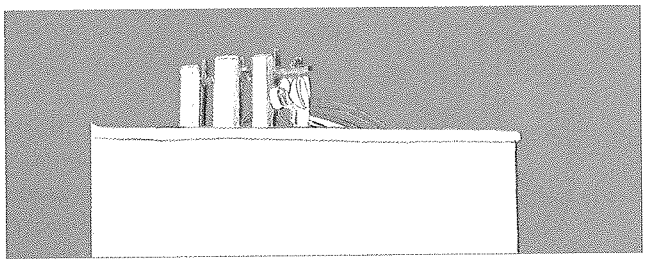


that's okay—the phone is still screaming. The next nearest antenna will pick up its signal.

After someone dials a number or opens an app on their phone, the cell phone sends a signal out to the nearest tower with the request for that call or that app (it's still screaming "Hi! I'm here!" but now also screaming "Bring me this app!" or "Call this person!"). The cellular antenna receives the request and sends it back into a fiber optic cable network, routing it through a much larger network (either of more cables or microwave antennae) and to the right server that can process the request (e.g., a call switching station or a Facebook data center). That server sends the requested data back through the network to the antenna *nearest* to the phone and that antenna sends the data back to the phone.

In New York, cell towers are generally pretty hard to see from the street—they're mostly on the tops of buildings. They're also often disguised, although their New York disguises (bricks on buildings) are pretty simple compared to cell tower disguises in other places (trees, church crosses, cacti).

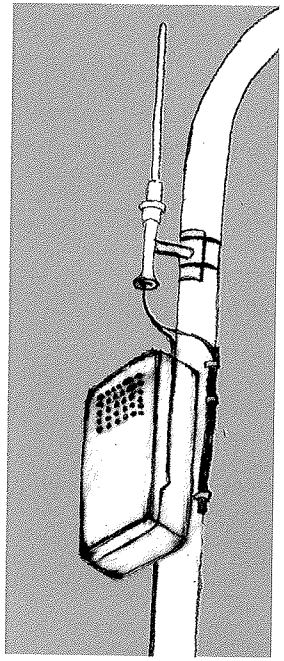
MICROWAVE ANTENNAE



While these antennae are damn near impossible to see most of the time from the street, it's useful to know about their existence. There are a small handful of wireless In-

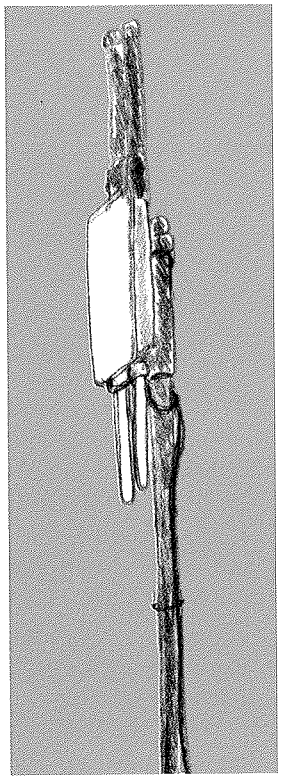
ternet service providers (WISPs) in New York City, who provide broadband services, mainly to businesses, through a network of antennae. At least one of these antennae is usually on the roof of a major carrier hotel, which is where data gets transmitted back into the global Internet. On other rooftops, they'll sometimes be alongside or attached to other antennae, as in the illustration above featuring a small microwave antenna affixed to a cell tower.

DISTRIBUTED ANTENNA SYSTEMS



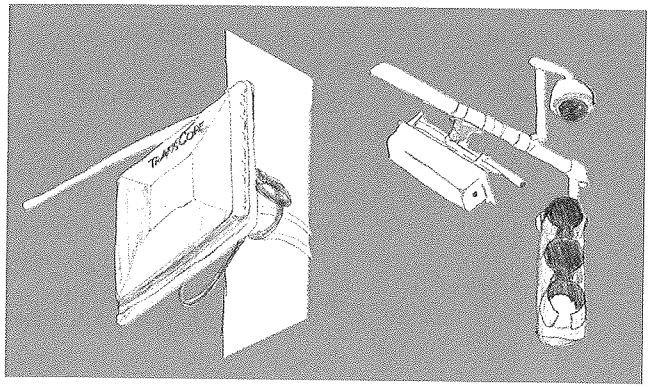
A Distributed Antenna System (DAS) is basically a way to expand a cell network's reach, adding capacity in undercovered areas. They're a little easier to find on the street because they're not on top of buildings—they're attached to street poles and linked to underground fiber optic networks. If you ever see an orange cable marking going into a street pole, look up. You'll probably see a DAS. There are seven companies with franchise agreements to maintain Distributed Antenna Systems in New York; however, three of those companies belong to one company as of 2015 (Crown Castle) and two appear to be subsidiaries of the same company (ExteNet Systems).

PUBLIC WI-FI ROUTERS



Throughout the city, there are a handful of parks that provide free, public Wi-Fi. This particular illustration is from Madison Square Park. Access to free Wi-Fi in New York City parks is partly brokered by the franchise agreement process. When a company receives a franchise to run cable throughout the city, the agreement usually comes with a caveat that the company has to provide the city with some municipal services and support. Starting in 2011, the New York City Department of Parks began making agreements with local franchisees (first AT&T, then Cablevision and Verizon) to bring Wi-Fi to public parks. The resulting rollout and reliability of that Wi-Fi has been pretty spotty to date, but even in parks where the Wi-Fi isn't readily available (such as the park where I spotted this router), artifacts of those networks remain.

RFID E-ZPASS READERS

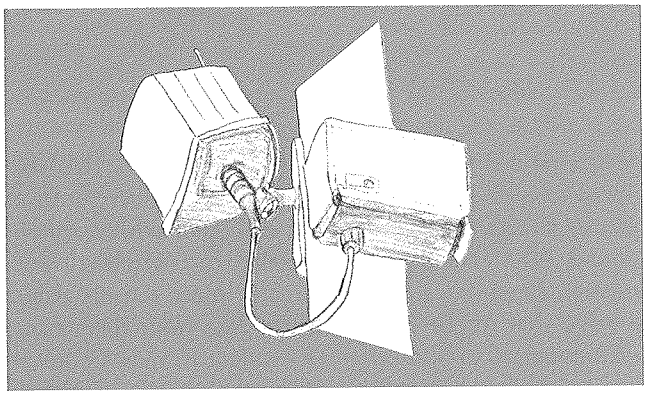


Most intersections in New York City have either one of these two antennae devices. Both devices broadcast and receive radio signals. In this context, they're used to read radio frequency identification (RFID) devices embedded in E-ZPass devices. Technically E-ZPass is used for toll collection, but E-ZPass Readers and other sensor devices also collect data from RFIDs for traffic monitoring purposes.

E-ZPasses work by registering drivers' travel through toll booths via the transponder, another word for the RFID that drivers keep in their car. When the E-ZPass is in proximity of an antenna that can pick up the transponder's frequency, the transponder transmits uniquely identifiable information to the antenna (like an E-ZPass account number). Once the antenna at a toll booth receives this information from the transponder, it relays that information back into a larger network, which is where the actual E-ZPass payment processing happens.

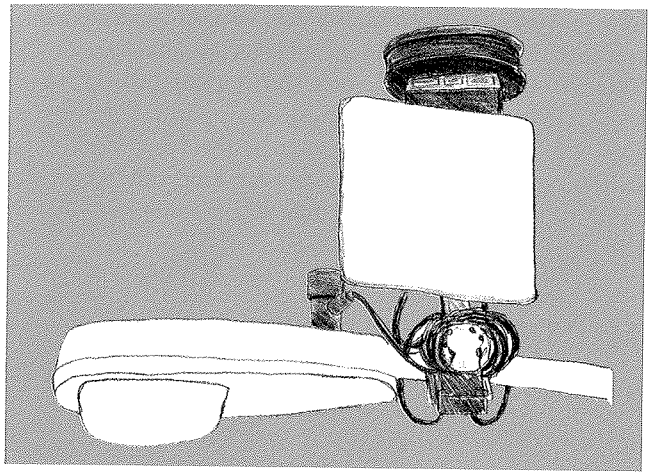
The E-ZPass readers above intersections in New York City aren't for toll collection at all. They're exclusively intended to monitor traffic patterns, measuring the number of cars passing a given intersection or road and adjusting traffic light patterns accordingly. Originally part of the "Midtown in Motion" smart traffic pilot project, these sensors are now present in many other parts of the city. A Freedom of Information request by the New York Civil Liberties Union didn't uncover how long data from the E-ZPass readers is stored or whether it remained only in the city's possession.

MICROWAVE RADARS



Another original component of the "Midtown in Motion" project, Remote Traffic Microwave Sensors (RTMS) are now used in many other parts of the city and are popular with transit agencies throughout the country as a low-cost, low-maintenance method of counting and tracking traffic in intersections. The RTMS detects motion and speed by measuring the distance of objects in its microwave beam's line of sight. Presumably these traffic sensors compensate for the number of non-E-ZPass-equipped vehicles that aren't picked up by the RFID readers.

SHOTSPOTTER



ShotSpotter is a company based in Newark, CA, that produces acoustic sensor technologies used to detect gunshots in city streets. The sensors are equipped with a microphone, GPS, and some processing and wireless transmission capabilities. When three or more sensors detect a noise that might be a gunshot, data from the sensors is transmitted to ShotSpotter's Incident Review Center in California, where analysts review the waveform pattern of the audio collected and listen to verify if the sound is, in fact, a gunshot and not something like fireworks or a car backfiring. The rationale for a sensor network to detect gunshots is essentially that many people don't report gunfire to 911.

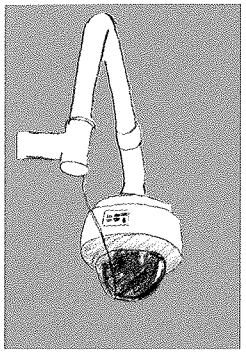
In July 2014, the New York Police Department entered into a $1.5 million contract with ShotSpotter to operate a pilot program using the technology in the Bronx; in March 2015, the program expanded to Brooklyn. The 2016 city budget allocated $1.8 million for the fiscal year and $2.5 million in 2017 to expand the sensor network from seventeen precincts to forty-five over two years.

Although the technology is used in more and more cities throughout the United States, ShotSpotter is not without controversy. In a 2012 case in New Bedford, MA, audio recorded following gunshots was used to identify a suspect in a murder case—which was the first indication that ShotSpotter's sensors could, in fact, record and store audio that wasn't necessarily from a gunshot. Some cities that have tried ShotSpotter, such as Trenton, NJ, and New Haven, CT, have questioned the effectiveness of the technology given the high rate of "false positives"—i.e., loud noises identified as gunshots and no indication of gunfire when police arrive on the scene. As of this writing, the NYPD hasn't released any updates on the success of the program and a bill introduced by Public Advocate Letitia James requiring the NYPD to publicly release ShotSpotter data has lingered in committee for over a year.

As far as networked devices go, ShotSpotter's sensors are tricky because they don't call that much attention to themselves. It would be easy to mistake a cluster of antennae and cables for some other traffic sensor or perhaps a part of the NYPD's camera network. And it's possible that they will become even more difficult to identify: the same year that the NYPD expanded its use of ShotSpotter to Brooklyn, the company entered into a partnership with General Electric Lighting to develop embedded gunshot detection sensors for GE's intelligent LED street light fixtures, which also monitor weather and traffic conditions.

SURVEILLANCE CAMERAS

TRAFFIC CAMERAS

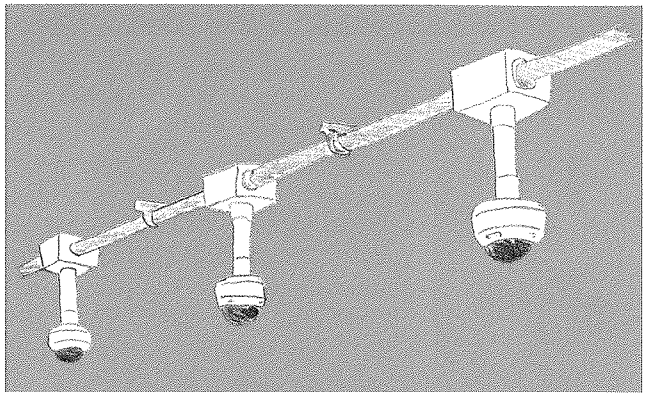


The New York City Department of Transportation (DOT) and the Metropolitan Transit Authority (MTA) operate traffic cameras at, respectively, 723 intersections and 20 bridge and tunnel entrances. These cameras are used for traffic monitoring purposes. The DOT cameras and MTA cameras both have live streams of their footage available online.

MTA SUBWAY CAMERAS

It's unclear, from what I've been able to find, exactly when the MTA began installing closed-circuit television cameras on some subway platforms, but efforts to expand that camera network ramped up dramatically after September 11, 2001. The MTA currently has more than 4,500 cameras operating throughout the transit system, with 1,500 of those cameras on city buses. Data collected by cameras feeds back to MTA Rail Control Center, located on 54th Street between Eighth and Ninth Avenues in Manhattan.

Following 9/11, security became a major priority for city agencies, and the MTA was no exception. Its 2000–2004 budget allocated $591 million for security projects, and in 2005 the agency issued a $212 million contract to defense contractor Lockheed Martin to provide a state-of-the-art security system for the agency. The system was to

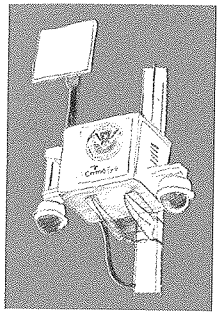


include 3,000 networked cameras and a network of sensors to identify suspicious packages or objects.

However, some of Lockheed's high-tech promises never really came to fruition, and in 2009 the contractor found working within the bureaucracies of the MTA so onerous that it sued to get out of its contract with the city. The MTA filed a countersuit shortly thereafter.

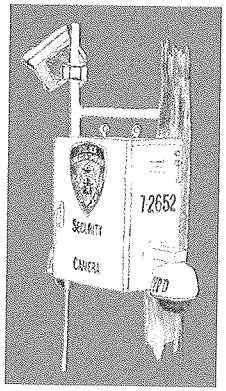
The MTA-Lockheed lawsuit couldn't have come at a worse time in the agency's history—by 2010, the MTA's finances were in such disarray that the agency ultimately had to cut services and institute its now-biennial fare increases. A 2010 article about the lawsuit noted that the $3.6 million the MTA had already spent in litigation was equivalent to the cost of the ten bus lines the agency planned to cut. The lawsuit remains in litigation as of this writing. New contractors continue to work on the electronic surveillance network.

CRIMEEYE CAMERAS



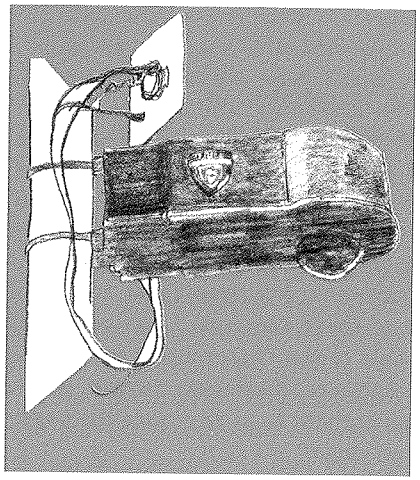
These cameras are sort of rare finds—they're visible mainly in Lower Manhattan and pretty much only around federal buildings. They appear to belong to the Department of Homeland Security and are manufactured by a company based in Suffern, NY, called Total Recall Corporation. (Not even joking, that's their name.)

NYPD CAMERAS



The New York City Police Department has a few thousand white, labeled surveillance cameras that, according to press reports, are part of a program called Argus. In Greek mythology, Argus was the name of a giant with one hundred eyes. Apparently, coming up with a clever name for a surveillance tool is really hard, so when searching for information about the NYPD's Argus, one pretty quickly finds other surveillance camera products with the same name and police departments calling *their* new exciting initiative Argus.

Earliest reference to the program dates back to 2006, when there was an initial install of five hundred of the cameras in the city. At the time, press reports noted one



interesting distinction about the new cameras: they communicate wirelessly. This communication happens via the white rectangular patch antenna attached on top of the white box. If you see one of these white patch antennae on top of an NYPD camera, look around the roofs of nearby buildings and other lamp posts in the area—chances are, you'll find another antenna. These antennae form a point-to-point wireless system, in which information from one device (in this case, a surveillance camera) travels wirelessly from its antenna to another node within its line of sight, at which point it's transmitted back to a wired network and some central location. While there are some wired cameras in the NYPD's network that were installed prior to 2006, wireless surveillance cameras offer the advantage of not requiring the installation or splicing of new cables for every new camera installed.

The antennae used on the NYPD's cameras are a product of Proxim Wireless, a company that makes wireless broadband networking systems primarily for large-scale, outdoor applications in business or municipal government contexts. The Argus camera system as a whole, however, is not built by Proxim.

These are another make and model of NYPD camera sometimes seen around the city. It's unclear what, if anything, distinguishes them from the white-boxed cameras.

The Domain Awareness System

Through tracking the installation of NYPD cameras through press reports and city council records approving new cameras, a piecemeal portrait of the city's camera network emerges, but getting a big-picture overview of the entire network is pretty difficult. The NYPD would probably prefer to keep it that way. When I filed a Freedom of Information Act request for the exact number and locations of these cameras, I was denied on the grounds that it would reveal "non-routine techniques and procedures"; furthermore, disclosure "would enable the planning of criminal activity so as to reduce the possibility of being caught on video."

Attempts by the public to track, count, or map surveillance cameras (police-owned or otherwise) have in general been pretty unsuccessful. Part of the problem of mapping out police surveillance cameras is the sheer scale of the network and the difficulty of organizing enough people to do the counting. But the other problem is that such an undertaking will always be incomplete, as it only reflects cameras that have been *labeled* by the NYPD. It doesn't begin to factor in the secret, unmarked cameras, the privately owned cameras that individuals readily turn over to police, or the privately owned cameras that feed directly into the NYPD's existing citywide surveillance network, the Domain Awareness System.

Not to be confused with Distributed Antenna Systems, the Domain Awareness System (also DAS) is the city's massive counterterrorism apparatus that collects and analyzes all of the information from police-operated networked devices previously mentioned in this field guide. Built in collaboration with Microsoft in 2012, the DAS allows police to connect content from camera feeds with arrest records, 911 calls, and license plate recognition technology. Under the terms arranged with Microsoft, New York receives a 30 percent cut of any sales Microsoft makes of DAS software to other cities. As of this writing, the most recent documentation I could find about how much money the department has made from this arrangement was a 2015 *Wall Street Journal* story, which noted that NYPD deputy commissioner of information and technology Jessica Tisch had framed and hung in her office the first of the checks from this profit-sharing arrangement, which amounted to $375,355.20 (although, for context, the NYPD's annual budget as of fiscal year 2016 is $4.8 billion).

The DAS isn't exactly a brand-new endeavor; it's more the current incarnation of years of post-9/11 initiatives to increase security in New York City. Some of the initial groundwork for this system dates back to the 2004 Republican National Convention in New York City, during which new cameras and the NYPD's existing Emergency Operations Center received major technical improvements and upgrades. In 2005, the NYPD launched the Lower Manhattan Security Initiative (LMSI), a project to tighten security specifically around Lower Manhattan similar to London's "Ring of Steel." The program was initially funded with $10 million from the Department of Homeland Security (DHS) and $15 million from the city and involved some contracting with IBM. The LMSI expanded its surveillance coverage and became the Midtown Manhattan Security Initiative in 2009 (with costs cited somewhere around $201 million, of which approximately 90 percent came from DHS). Estimates for the costs of the Microsoft partnership, created in 2012, range between $30 and $40 million. A number of the system's cameras belong to private "stakeholders" including the Federal Reserve, Goldman Sachs, and Pfizer, who have access to the DAS headquarters at 55 Broadway, an office building at the corner of Exchange Place.