STREET LEVEL SURVEILLANCE

SURVEILLANCE CAMERA NETWORKS

Surveillance cameras are one of the most ubiquitous and recognizable technologies used to watch us as we move about our daily lives. Government agencies and local business associations install networks of cameras, but the distinction blurs with the development of real-time crime centers that access both public and private video feeds. Camera technology is growing in sophistication: some cameras are capable of 360-degree video, infrared vision, or the ability to pan, tilt, and zoom. Some models can be equipped with real-time face recognition or license plate recognition software. Since many camera networks are also connected directly to the Internet, they have proven easy targets for malicious attackers.

Recognizing the Types of Cameras

Here is a visual guide to some of the types of surveillance cameras you may encounter day-to-day. This is not an exhaustive list, and it's important to note that some cameras may incorporate multiple features described below.

Bullet cameras

PHOTO BY MIKE KATZ-LACABE (CC BY)

A so-called bullet camera in the San Francisco Bay Area

Bullet cameras are compact and tube-shaped. The camera, lens, and housing are all packaged within a cylindrical-style body. These cameras face one direction and sometimes have infrared LEDs for use in low light. Bullet cameras are used both indoors and outdoors.

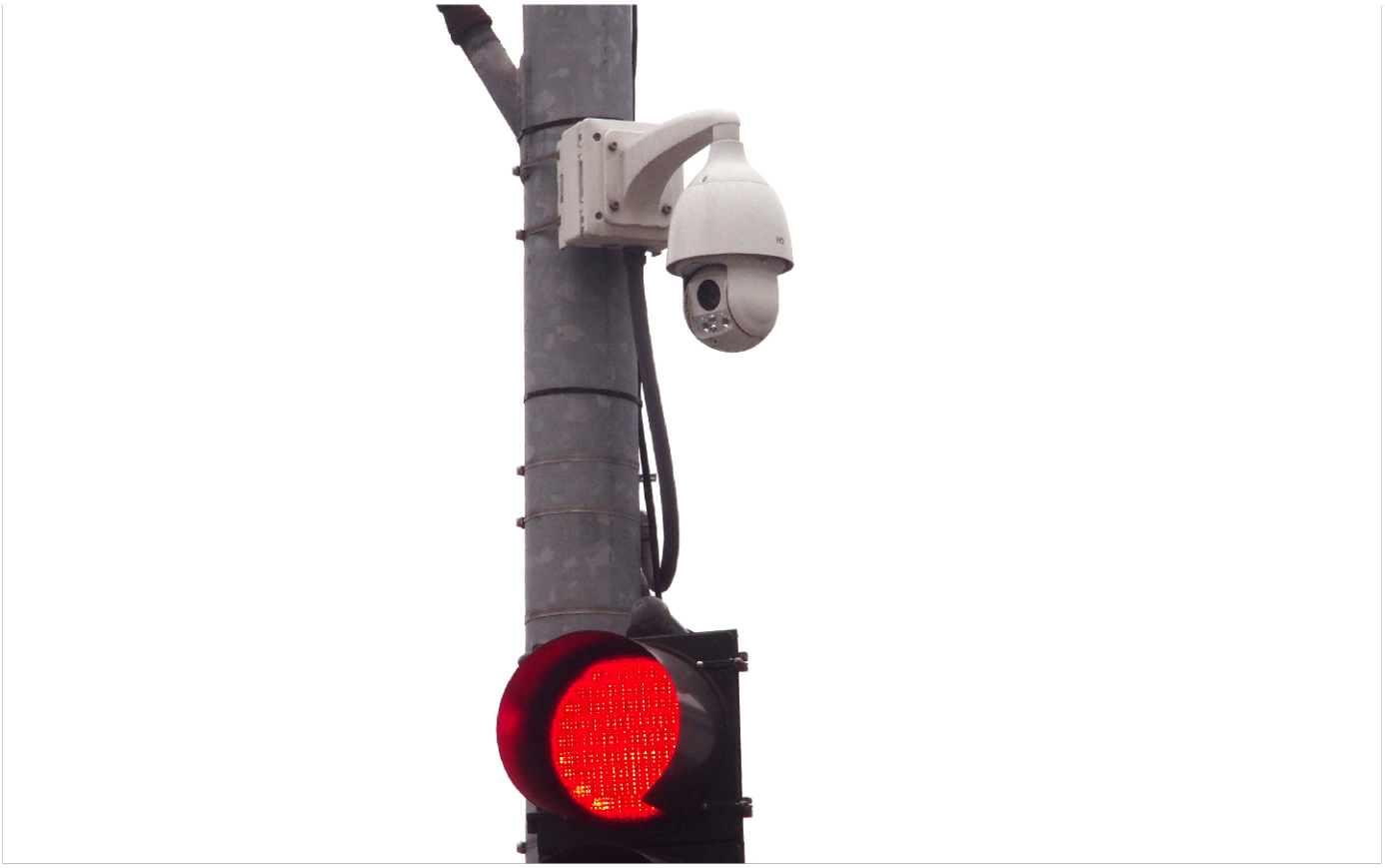
Dome cameras

ATTRIBUTION. SOURCE: EFF

Dome cameras inside the San Francisco Museum of Modern Art and outside a storefront in Union Square

Dome cameras are typically used for indoor surveillance, and are often mounted on ceilings. The camera's dome shape is designed to make it difficult to tell which direction the camera is facing. Dome cameras come with many optional features. Some have infrared light for night vision, some have tamper-resistant features, and some have varifocal lenses, allowing operators to adjust the focal distance of the camera lens.

PTZ (Pan Tilt Zoom) cameras



SOURCE: EFF

A pan-tilt-zoom camera affixed to a traffic light

Most surveillance cameras are fixed cameras—they face just one direction. PTZ cameras are remotely controlled, and allow the operator to pan (move left or right), tilt up and down, or zoom closer or farther away in order to follow people as they move. This lets operators zoom in on specific areas or track specific movements. The cameras can also run patterns or turn to a preset position.

Mobile Surveillance Towers/Poles

SOURCE: EFF

A 'Mobile Utility Surveillance Tower' at San Diego Comic-Con and a mobile surveillance pole in New Orleans French Quarter.

Not all surveillance cameras are static. Law enforcement agencies often acquire mobile surveillance units, such as manned towers that can be raised 25-feet in the air and unmanned trailers that can extend a pole with PTZ cameras in all directions. These systems are often used to establish situational awareness at public events and in high-traffic commercial areas.

Thermal cameras

SOURCE: EFF

FLIR dual-sensor thermal camera at the White House with pan-tilt-zoom capabilities

Most video captures images in the natural light or infrared spectrums. Thermal cameras can also capture video of a person's movements based on body temperature. These cameras are not always distinguishable from conventional security cameras. However, the brand name FLIR is often a tell-tale sign that the camera is capable of thermal imaging.

Automated license plate readers

PHOTO BY MIKE KATZ-LACABE (CC BY)

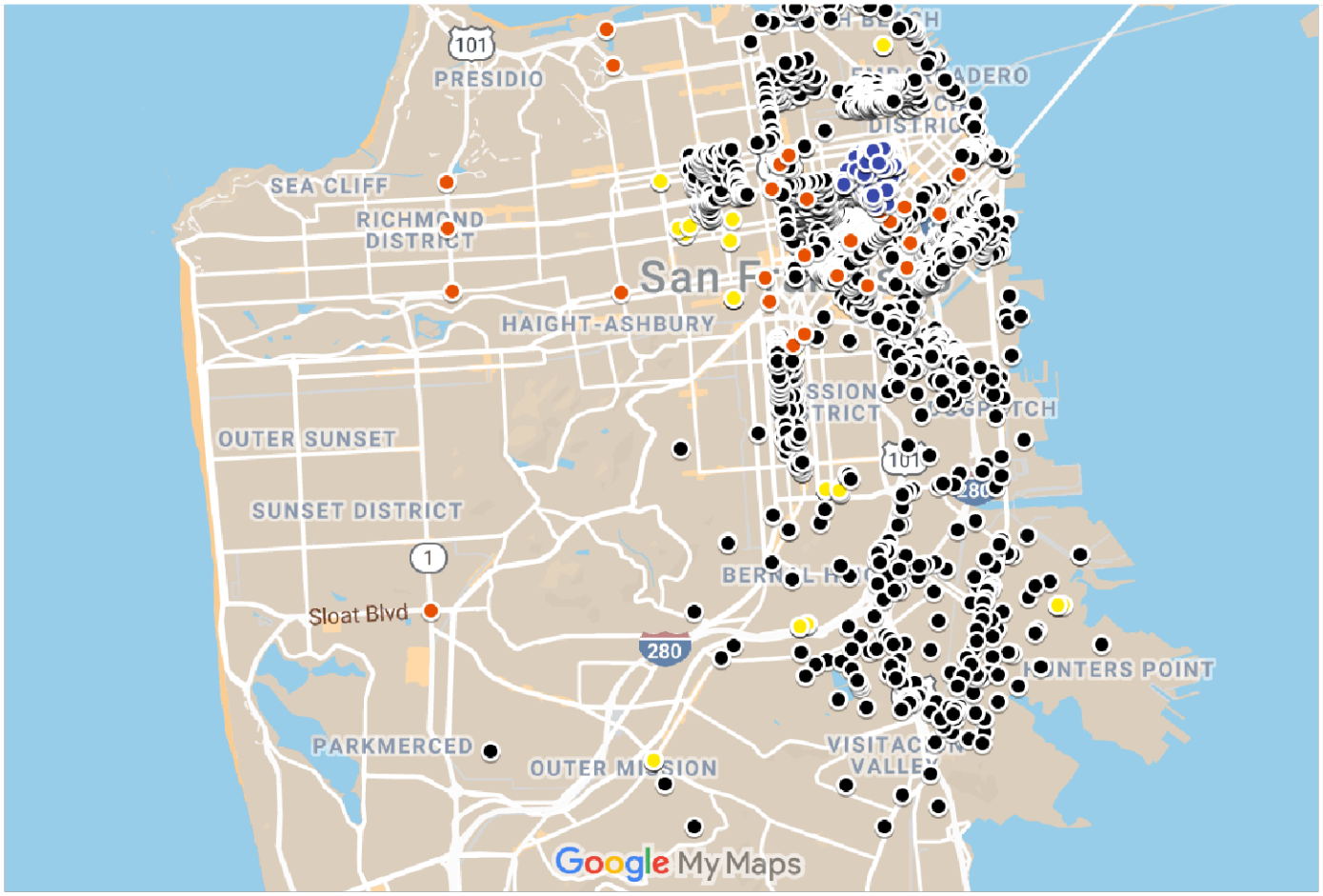
Automated license plate readers affixed to a streetlight

Automated license plate readers (ALPR) are computer-controlled camera systems that capture license plate numbers, as well as photographs of the vehicles and sometimes drivers and passengers. ALPR cameras include fixed cameras, often mounted on traffic lights, telephone poles, or other locations. They also include mobile cameras, which are typically attached to police patrol cars. Some agencies have mobile ALPR trailers that they can move to targeted locations.

Read more about automated license plate readers.

Data Sharing

Surveillance cameras often broadcast footage over the internet, allowing operators to monitor security camera feeds remotely. In some cases, cities pay for and operate surveillance systems. But in other cases, residents and businesses share surveillance camera footage with police officers.



SOURCE: EFF

In 2019, EFF obtained a dataset of surveillance cameras maintained by the San Francisco District Attorney's Office. Click here to launch in a new window or read the blog post.

Many law enforcement agencies have private security camera registration programs (sometimes called "SafeCam"), whereby residents and business owners can provide basic information about the cameras they own and where they are located. Then, when a crime is reported, police may search their database of cameras and contact the owner directly to obtain the footage. Some examples of this program include the Philadelphia Police Department (PA) and the Fultondale Police Department (AL). The Phoenix Police Department refers to its program as the "Virtual Block Watch."

In San Francisco, the Union Square Alliance, a local business improvement district, launched an outdoor security camera program in 2012 with just six privately owned cameras. Now, it consists of a network of over 450 surveillance cameras. Police regularly seek footage from these cameras when investigating potential crimes. Police also have

including for 8 days during the George Floyd protests in 2020. According to news reports, grant money pays for around 90% of the cost for the cameras in Union Square, and business owners who wish to participate pay the remainder.

Real-Time Crime Centers (RTCC)

SOURCE: FRESNO POLICE DEPARTMENT

Fresno Police Department's Real-time Crime Center

Several cities feed video surveillance into monitoring headquarters, often referred to as "domain awareness centers" or "real-time crime centers." Some hope to expand the footage they collect through their own surveillance cameras by also tapping into footage taken by private individuals and businesses.

As part of the Atlas of Surveillance project, the Electronic Frontier Foundation and students from the Reynolds School of Journalism at the University of Nevada, Reno have identified more than 80 RTCCs across the United States, with heavy concentrations in the South and the Northeast. In this report, we highlight the capabilities and

public understands how the technologies are combined to collect data about people as they move through their day-to-day lives.

In New Orleans, for example, live video feeds from more than 300 street-facing surveillance cameras are fed into a $5 million high-tech monitoring center created in 2017. The feeds are monitored 24/7. The mayor's office has continued installing additional cameras, and has integrated private cameras with the monitoring center. The city's automated license plate readers also feed into the RTCC.

In Birmingham, Alabama, nearly 100 surveillance cameras—24 PTZ cameras, 17 dome cameras, and 54 automated license plate readers have been installed on 64 power poles. The Jefferson County Metro Area Crime Center monitors the cameras. The ALPR data is uploaded to the FBI's Criminal Justice Information Services (CJIS) database, and the city obtains the content from the FBI's portal.

The starting cost of these RTCCs can range dramatically, from just a few hundred thousand dollars to as much as $11 million, as in New York City. This funding can come from a number of sources, including city budgets, voter-approved bonds, state and federal grants, private institutions, and wealthy individual donors. For example, the Atlanta Loudermilk Operation Shield Video Integration Center started with a $1-million donation from the Loudermilk family, who are real-estate developers, as well as $350,000 from the city. The price tag proved too high for the Fresno Police Department in California, which let go of its part-time RTCC staff in 2019 and ceased all real-time operations at the RTCC in 2020 (although police can still access stored footage from previously installed cameras after crimes occur).

Emerging Issues

On its face, video surveillance technology is already pervasive. But beyond the privacy concerns of law enforcement's widespread access to historical and real-time video footage lies the threat of breach. Since camera networks are typically connected directly to the Internet, they pose easy targets for bad actors.

For example, hackers attacked two-thirds of D.C.'s police surveillance cameras days before the 2017 presidential inauguration as part of a ransomware attack, causing more than 100 cameras to go dark.

In 2015, EFF learned that more than a hundred ALPR cameras were exposed online, often with totally open web pages accessible by anyone with a browser. In some cases, anyone could open a browser window and view a camera's live video stream and

sources in five different instances. Similar ALPR vulnerabilities were discovered in Boston by DigBoston and the Boston Institute for Nonprofit Journalism.

When combined with face recognition, surveillance camera networks raise serious additional privacy and civil rights concerns—in part because face recognition data is prone to error.

Read more about face recognition technology.

Face recognition, however, is only one form of video analytics deployed with surveillance cameras. BriefCam, for example, offers a sophisticated analytical software that can track individuals based on their clothing, glasses, or facial hair and is used at real-time crime centers.

One of the most important emerging issues in relation to police camera networks is their ability to connect to private security cameras on homes and businesses. In a quiet but rapid expansion of law enforcement surveillance, U.S. cities are buying and promoting products from Georgia-based company Fusus in order to access on-demand, live video from public and private camera networks. The company sells police a cloud-based platform for creating real-time crime centers and a streamlined way for officers to interface with their various surveillance streams, including predictive policing, gunshot detection, license plate readers, and drones. For the public, Fusus also sells hardware that can be added to private cameras and convert privately-owned video into instantly-accessible parts of the police surveillance network. In Atlanta, Memphis, Orlando, and dozens of other locations, police officers have been asking the public to buy into a Fusus-fueled surveillance system, at times sounding like eager pitchmen trying to convince people and businesses to trade away privacy for a false sense of security.

In short, the proliferation of surveillance cameras has rapidly reduced our ability to maintain anonymity in public spaces; and the advent of automated face recognition and other tracking technologies only accelerate this threat to privacy.

Most recently updated October 1, 2023

TECHNOLOGIES