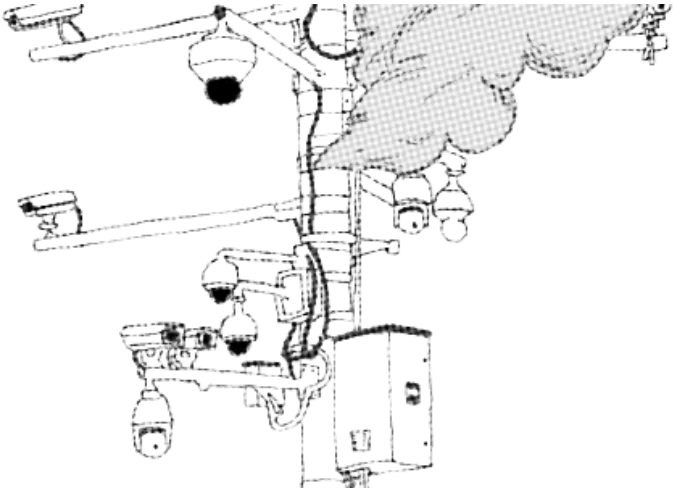
You Can't Catch What You Can't See

Against Video Surveillance



You Can't Catch What You Can't See: Against Video Surveillance

Original text in French

Pas vue pas prise : contre la vidéo-surveillance

pasvuepasprise@riseup.net

2023

infokiosques.net/spip.php?article2019

Translation and layout

No Trace Project

notrace.how/resources/#catch-see

Note from the No Trace Project:

This text is a case study of video surveillance in France, and most of its content is based on the French context. However, we believe it can be useful to an international audience because understanding how video surveillance works in France can help to understand how it works in other places, and because a lot of technical, general information is scattered throughout the text.

Some sections of the original zine that we felt were too focused on France have not been included in this translation.

Contents

Introduction

In just a few years, video surveillance has become an inescapable part of daily life. Cameras were once reserved for a city's main streets or the aisles of a supermarket, but now they are found everywhere. They have become so commonplace that we mostly don't even notice them. However, for some of us, it is difficult to forget the weight of these little machines in our lives and methods of action. They make the areas caught in their field of vision more hostile, because being constantly spied on naturally makes people wary. We end up wondering if we look sketchy and censor ourselves. One characteristic of surveillance is this push towards normalization, making us control our own behavior out of fear of potential repression.

"Security" through repression and control is one of the pillars of the State, which is always looking for new ways of entrenching and consolidating its domination. Video surveillance, despite being just one tool among others, plays an increasingly important role in the modern security toolbox. This is especially true because cameras support other systems that States rely on, given they don't have an infinite supply of police. By constantly increasing their field of vision and their effectiveness by installing new cameras and using higher performance automated surveillance software, the police can increase their capacity without having to increase their numbers. But let's be clear, the increasing use of video surveillance in the public space does not mean there are fewer police patrols in the streets.

In addition to being a pillar of repression, video surveillance is also, by its nature, an excellent tool for discipline. Its panoptic character—meaning the sense of being potentially observed everywhere and at all times—encourages conformity. This is even more true when we know that video surveillance software is increasingly trying to detect "abnormal" behavior, like stopping in an area where you should walk, wandering when you should know where you're going, sitting when you should be standing, gathering when you should be alone, etc. Combatting video surveillance means demanding the ability to live without having to increasingly ask ourselves what norms to comply with when we would like to do away with them all. It is a mistake to only see the cameras in the street. Power's

gaze is increasingly intruding in every place where the forces of control seek to assert themselves, like workplaces, schools, prisons, the hallways of apartment buildings, public transportation, etc. Everywhere, the State and its auxiliaries want to strengthen their presence and remind us of it. And how can we forget about the people who install cameras at their homes and whip out their smartphones at the slightest unusual thing? Whether in a demo or on a hike, there are few places or moments when we don't have to worry about being spied on by a little snitch.

And as we experienced during the lockdown, not even peaceful beaches, forests, and mountains are safe from the arrogant buzzing of drones.[1]

The massive rollout of cameras, improvements to them, and the promise of new uses are terrifying. It is staggering. But we don't want to simply resign ourselves to it. The omnipresence of video surveillance doesn't mean we can't challenge and attack it. Simply put, we refuse to get used to it.

Despite how it seems, these systems are far from infallible. They have weak links, cracks, and there are many ways of getting around them. The goal of this project is to put our knowledge, tips, and practices in common in order to feel stronger, giving ourselves some tools to deal with video surveillance. So it doesn't beat us down in our daily lives or stop us from acting.

Knowing where the cameras are, how they work, how the footage is transmitted and viewed, and how these technologies are evolving is a way of concretely giving ourselves the means to go after video surveillance and the interests they protect.

This project is based on knowledge acquired from all over by various people and is therefore not the work of technicians or experts. That means it can't claim to be completely exhaustive or error-free and that, given that the situation is constantly evolving, there will always be additions and modifications to be made. But this also means that there is a lot of information available to those who want to see the rubber meet the road in the struggle against video surveillance.

[1] *No Trace Project note:* During COVID-19 lockdowns in France, police occasionally used drones to enforce lockdowns in rural areas.

"The State is watching us. Let's put its eyes out!"

From the streets of Levallois-Perret to the 2024 Olympics

A brief history of video surveillance

The first video surveillance system was created in 1942 during World War II in Germany. It was installed to surveil the launch of ballistic missiles against England. In the late 1960s, systems of this type started being developed and commercialized for civil uses, notably to surveil the public space. In 1968, the city of Olean in the United States was the first to install cameras to surveil its streets. Then, in the 1980s, the United Kingdom generalized urban video surveillance systems following attacks by the IRA (an Irish armed independence group).

In France, the first street cameras were installed in Levallois-Perret at the start of the 1990s by Mayor Patrick Balkany, in a context of uncertain legality. The initiative was vigorously critiqued, and several complaints were made to the Commission nationale informatique et libertés (the national commission on digital technology and liberties, CNIL) despite the fact that policies aimed at security were widely supported by residents of the town. Also the system, made up of 96 cameras, was expensive and hard to use. Regardless, this first experiment unsurprisingly led to the entry of video surveillance into the French political landscape. Not long after, in 1995, a law was passed to establish a legal framework governing the installation of cameras in public spaces. Gradually, video surveillance cemented its position as an issue of public policy. During the 2001 municipal election, safety was a major theme, and the installation of cameras was presented as a key part of many electoral platforms. Following that, this trend only became more pronounced, especially following the September 11, 2001, attacks on the World Trade Center in New York.

In 2006, Nicolas Sarkozy, then Minister of the Interior, put forward a motion framed in terms of anti-terrorism that loosened the conditions for using video surveillance in the public space. The popular fear of terrorism

was also used as a justification for the 2007 launch of a national plan for setting up "video protection." It's worth noting the semantic shift which, although having no effect on the reality of video surveillance, shows the effort to make it more acceptable or desirable. Everyone would rather be protected than surveilled, after all.

The same year, an interministerial crime prevention fund was launched with the goal of encouraging municipalities to install cameras in the public space. This fund—with money coming from fines—allowed the State to subsidize, among other things, the installation of cameras and their connection to Urban Supervision Centers (see "Urban Supervision Centers (USC)", p. 34) run by the police and the gendarmerie. In 2007, there were about 20,000 surveillance cameras on public streets. According to the Ministry of the Interior, between 2007 and 2014, 2,820 municipalities and 173 intermunicipalities were subsidized through the fund, leading to the installation of 26,614 new cameras.

The multiplication of video surveillance systems went along with their normalization. On the one hand, the legal framework was refined, such as with the "Loppsi 2" bill that was passed in 2011 to provide direction and timelines for improving national security performance. It added to the list of outcomes that can justify the video protection of public spaces and allowed prefects (government officials in charge of security) to temporarily install cameras during demonstrations. On the other hand, cities that had no cameras up until then came under more and more pressure to install them. For example, the municipality of Villeurbanne, singled out by Sarkozy as a "dark spot" and urged on by neighbouring cities, gendarmes, business owners, and citizens, ended up installing its first cameras in 2018 and had 105 by 2021.

After the attack on Charlie Hebdo and the November 13, 2015, attacks, the terrorist threat served once again as a pretext for putting new control measures in place. With a state of emergency declared, the expansion of video surveillance accelerated. In Paris between 2015 and 2022, the number of cameras in public streets quadrupled. But an increasing number of small municipalities are also installing video surveillance.

When an attack occurred on July 14, 2016, Nice was already the most heavily video surveilled city in France. According to local authorities,

the fact that the cameras failed to prevent the massacre just meant there weren't enough. The rhythm of new installations increased, leading to their number growing from 1,300 in 2016 to 3,300 in 2020. In parallel, the city ran a project called "safe city," which means a connected city where video surveillance and big data watch over everyone's safety by means of automated surveillance software in partnership with the Thales corporation. In 2019, Nice tried out facial recognition. In the flurry, the CNIL moved to demand a legal framework for this technology. We see clearly here the way this institution serves first and foremost to democratize ever more effective methods of control.

Public investment in the sector unsurprisingly attracted a cohort of private companies eager to make money in this booming market. Among the leaders in the sector, there are Axis and Hikvision for installation and Engie Ineo and Briefcam for data processing and analysis. These companies are, of course, helped out by the State, which ensures that the law aligns with their economic interests and favours public-private partnerships. In 2020, the combined sales of manufacturers, distributors, and installers of video surveillance equipment (materials and logistics) working with the public sector reached 300 million euros (about 330 million USD). Some companies even held promotions to sell their products to local governments.

With the COVID-19 pandemic, many security companies seized the opportunity to offer digital surveillance solutions. For instance, in Cannes and Paris, during the lockdown, the company Datakalab tested software for detecting whether a person was wearing a mask. Once again, the CNIL pushed for the existing rules to be adapted to legalize tools like this by pointing out that they do not comply with the law. Elsewhere, the pandemic brought about the expansion of thermal cameras for checking people's temperature at the entrances of airports, schools, businesses, and government offices. Other cities sent out drones to play messages and support police operations by filming from the sky (see "Types of cameras", p. 15).

The terrorist threat and the war on crime or on COVID were all scarecrows that the authorities held up to make video surveillance more acceptable and to speed up its spread. That said, it is likely that even without the attacks

or the pandemic, the tendency would have been basically the same. This is because, in any case, the State sees video surveillance as an incredible boon for strengthening one of its main functions: controlling individuals. It routinely seeks to push the limits of acceptability when it comes to control over our lives by following a familiar path: its pioneering experiments provoke a backlash, critiques are developed and then integrated into a law that legalizes the new measures while making us think that nothing has changed, that we are just as free as before.

The development of video surveillance did not occur without resistance. Although we can't say there was a large movement in opposition, neither can we ignore the initiatives and struggles against cameras. Much of this resistance has taken (and continues to take) a legalistic perspective, such as associations of local residents or human rights organizations that denounce the installation or presence of video surveillance through public campaigns and/or legal action.

With the increasing number of cameras, other forms of contestation have emerged. One technique for fighting video surveillance is to map the cameras in public spaces so that they can be avoided or sabotaged or just to demonstrate their number. More discretely, during their installation, there have been sabotage campaigns, and after their installation, they are routinely destroyed or damaged, sometimes in highly visible ways like during a demonstration (see “Dodging and sabotaging cameras”, p. 68). These struggles have been accompanied by numerous poster campaigns against video surveillance.

The video surveillance olympics

Today, the security industry is gleefully watching the approach of the 2024 Olympic Games in Paris, which is yet another pretext used by the State and local authorities to reinforce their control over the streets and the public space. We have seen this in other countries, such as in Tokyo during the 2020 Olympics, when facial recognition was authorized in certain spaces. In France, it was also authorized on an experimental basis in 2019 and was tested repeatedly with varying levels of success, notably in 2020 at the entrance to the Metz stadium and during the French Open

tennis tournament. It is still illegal to use in France, but companies in the sector, who have seen their annual earnings grow considerably in recent years (Thales, Idemia, IBM, XXII, etc.), have been pushing for the laws to be relaxed. Ultimately, facial recognition will not be used during these Olympic Games, but the second Olympics bill[2] will make it legal to use automated video surveillance on an experimental basis, which is a technology that, as we will see in "Automated video surveillance", p. 47, is already widely used, despite what these legislative wranglings might lead us to believe.

This law does not only deal with the time period and the infrastructure around the Olympics as, for instance, it immediately reduces the reach of the CNIL. Although certain measures are intended to apply only during the Olympics, we can expect them to be used in advance or to continue being used afterwards. This might be the case for the body scanners being installed at the stadium entrances (despite their large price tag that could even dissuade the Olympic Committee), facilitating work on Sundays, loosening the rules around advertising, the appointment of the Paris prefect as the sole person in charge of security for the entire Île-de-France region, the increase in investigations into workers and participants in the Olympics, and also automated video surveillance.

[2]The first Olympics bill in 2018 was mostly about the financial and city planning aspects of the games.

"2024 Olympics. Neither here, nor anywhere else."

Other bills that were justified to varying degrees by the upcoming Olympics have already allowed for security measures that involve video surveillance, such as for instance the "Drone 2" bill (see "Types of cameras", p. 15). But this new bill opens up fresh possibilities for experimentation with automated video surveillance.[3] This is all thanks to artificial intelligence algorithms that allow for the detection of "abnormal situations, fires, abandoned items, bottlenecks of people," "by targeting those people who meet certain criteria or even certain categories of actions, like damaging public property." This software would be able to issue an alert about these behaviors and analyze the footage. What constitutes a suspicious behavior and what areas are affected will be decided by decree. It will certainly be based on the same criteria the police use when stopping people in the street, by, for instance, automatically identifying people who hangout for a long time in the same area or in groups.[4] This affects the areas that will

[3] See the text from Technopolis "Paris 2024 : les olympiades sécuritaires du gouvernement"[a] (*Paris 2024: The Government's Security Olympics*).

[a] https://technopolice.fr/blog/paris-2024-les-olympiades-securitaires-du-gouvernement

[4] As during other Olympics, people living on the street were displaced momentarily or permanently or were even jailed at certain times. This software will definitely be

host the Olympic competitions as well as the rugby world cup in 2023, which is being considered a security test in the lead-up to the Olympics. The prefect could also authorize the use of video surveillance for any sporting or cultural event or celebration that requests it, which would then be approved by decree. The footage taken during the experimental period will be kept for one year.

Footage taken by drones will also be usable by automated video surveillance systems. And automated video surveillance will also be usable by public transportation companies (like the SNCF, the national train company, and the RATP, which runs the Parisian metro and bus lines) on their existing camera networks. The implementation of this software will first require a live test phase in these places and during these events or by using any video surveillance footage from these events, and it could then be put in place until the end of March 2025, despite the fact that the Olympics only last two months. But, like many exceptional or experimental measures, they will then become long-lasting and get legalized.

The Olympics and this law are opportunities to sell software, to arrange financing, and to integrate them into video surveillance systems in many cities. It is hard to imagine any municipality having a reason to get rid of it afterwards.

Also, many municipalities where the Olympic Games will take place are preparing to strengthen their public safety arsenal with the help of the State, which generally covers 50% of the cost of cameras in cities through dedicated funds (the SEPD in rural areas, the interministerial crime prevention fund in cities) using equipment that is often delivered with automated video surveillance software. In Saint-Denis, a brand new urban supervision center was opened in 2021. Its network, which counted 93 cameras in 2022, will be expanded to over 500 cameras by 2024, and local politicians are planning to equip the video surveillance system with artificial intelligence to automate the reporting of infractions. The Ministry of the Interior has announced that it wants to add 500 new cameras in Paris and 330 in Marseille (where the boating events will take place),

widely used before and during the Olympics to police people living on the street and prevent encampments from being established.

for a total of 44 million euros dedicated to the interministerial crime prevention fund.

Down with the Olympics!

Types of cameras

There are a huge number of different types of video surveillance cameras that vary in several ways: appearance, resolution, mobility, mode (infrared, thermal…), field of vision, zoom, and so on. We can, however, identify a few broad categories of camera.

- **Directional or fixed cameras**

They surveil a single plane of varying size and may have a zoom. Their shape gives a sense of the area they surveil. They are often used to surveil places that people have to pass through, such as a hallway or an entryway.

- **Mobile PTZ (pan, tilt, zoom) cameras**

They can pivot 360°, tilt up or down up to 180°, and have an optical zoom. Because of their characteristics, they are often used to surveil wide areas.

- **Fixed and mobile dome cameras**

Dome cameras are cameras installed inside a semicircle of glass. They are widely used because they are resistant to "vandalism" and because their dome is generally opaque and so does not allow you to see where the lens is pointed. They are marketed as being more discreet. These cameras can be either fixed or mobile (pivoting 180° and tilting up or down).

- **Panoramic, multi-sensor cameras**

Multisensor cameras are cameras that have several sensors in a single body and so allow for a panoramic view within a given angle (up to 360°) by presenting the images from its different sensors side by side. This means it is several cameras in one (because of its multiple sensors), which is an "advantage" from a technical perspective—only one camera to install —and from a surveillance perspective—it gives a panoramic view. These cameras are widely used in airports, transit stations, intersections, public squares, and anywhere a panoramic view is useful.

The following image shows a camera with four sensors that allows for a 180° view. A selling point of these cameras, according to their manufacturers, is that they offer a panoramic view without a loss of image quality. In fact, compared to cameras with a single wide-angle lens, panoramic cameras with multiple sensors allow for a higher quality panoramic view.

The next image shows a camera that looks like a spaceship or a flying saucer that is becoming more and more common in urban areas. The upper part of the camera is shaped like a crown and has between four and eight sensors that provide a panoramic 360° view in high quality. But in addition, it also has a PTZ camera (in the semicircle under the crown) that allows it to get "clear and detailed close-ups that are very useful in court."

The final image shows a type of camera that is very common in Paris. The cops call them "Plater." With cameras that look like an animal's nipples or a bunch of grapes, they can also get a 360° panoramic image using the various cameras spread out above as well as high-quality close-ups of specific scenes with the PTZ camera underneath.

- **Nomadic cameras**

Their distinguishing trait is that they can be moved very easily. They are of various types according to the specific needs, and so can be fixed, dome, 360°, or others. Most often, they are attached to a street light so as to tie into the electrical supply. They are equipped with a battery (the white box above the globe) which recharges at night when the street light is turned on. They operate autonomously during the day using the electricity stored in the battery. They can also record to storage and have a means of wireless transmission, which can be wifi, 3G, 4G… These cameras serve to provide temporary surveillance in a given space: "important works that require surveillance, events, time-limited security problems in an area, illegal dumping, demonstrations," etc.

- **Drones**

In the last several years, first at borders and then in the streets during demonstrations or during the first lockdown, a new type of surveillance camera has made an appearance, one that is extremely mobile and can be deployed rapidly according to the needs of the police. These are drones, or "aircraft travelling with no one aboard" as they are defined in law. Although they were in use long before a legal framework existed, the State recently passed legislation regarding their use by the police following a complaint from the group "Quadrature du net" and France's Human Rights League. This was first attempted in 2021 in the global security bill, but was overturned by the constitutional oversight committee. A few months later, the same provisions were inserted in another law, this one dealing with "criminal responsibility and national security" also known as "Drone 2", with a few modifications to make explicit the conditions under which drones can be used, and it was passed successfully in January 2022.

Excluding the municipal police, cops can now officially use drones to film during specific timeframes and in specific locations with authorization from the prefect. The list of situations where they can be used is limited but sufficiently vague to be applied anywhere and anytime: "The prevention of threats to the safety of people and property, the safety of gatherings in public streets, the prevention of terrorist acts, traffic regulation, border

surveillance, aid to persons," and for the needs of a police or judicial investigation into serious crimes or certain lesser offences.

Drones are very discreet, but they still make an easily recognizable noise that sounds like the buzzing of a huge swarm of bees.

- **Body and vehicle-mounted cameras**

There are other kinds of highly mobile cameras that are worth mentioning. For instance, there are those that police wear on their chests, so-called bodycams, that they can turn on and off with a single click. They record sounds and images which are stored for six months, and they can also transmit directly to the police station. These cameras show a green light when they are running and red when they are recording, and it is worth noting that it is not necessarily the cop wearing the camera who turns it on, since they can be activated at a distance. Be careful, because the device can store up to two minutes of footage before it is activated and two minutes after it is turned off. Although they were not widespread and had poor quality until recently, in 2021 the national government announced they would be generalized to all police forces and to all officers (both police and gendarmes) in the whole country. The company Motorola won the public contract, which is worth an estimated 15 million euros for 30,000 devices, to increase and modernize the stock. The use of bodycams was also expanded by recent laws to include forestry officers and public transit fare inspectors on an experimental basis, for now.

It is also planned that by 2023 all police vehicles will be equipped with a vehicle-mounted camera. The general security law also allows for tests of front-facing cameras mounted on trains and buses that are, for the moment, intended to analyze any accidents that occur.

Image quality

Video surveillance undeniably increases the State's capacity to control, but to what extent does it actually help those who want to spy on us? The footage isn't helpful if it isn't usable! It is therefore important to understand the technical performance of the various cameras in terms of image quality while also grasping their limitations. They are able to detect "abnormal" activities and trigger police action, but only in their limited field of vision. They can help to identify individuals, but only within the limits of their precision. They can provide colour images by day, but generally not by night… All these limitations are constantly being addressed by their manufacturers as the technology improves.

How precise are surveillance cameras?

How far away can a camera, and therefore also those behind the screens, see us? Obviously, there are as many answers to this question as there are types of cameras with their own performance specifications. Still, French municipalities logically all tend to install equipment with similar capacities, following the same offers on the video surveillance market and the same expert opinions. Based on broad trends, we can begin to provide an approximate answer to the question posed above.

The precision of a camera depends primarily on two technical specifications: image resolution—namely the number of pixels that make up the image—and field of vision—the larger it is, the less precise the image.

As with television screens, manufacturers are racing to have the highest resolution, and cities update their equipment accordingly. If full HD (1920 × 1080 pixels), or 2 million pixels, remains the most common resolution today, more and more cameras with four, five, or even six million pixels are being installed to film wide areas. Panoramic multisensor cameras are currently migrating from 12 megapixel definition (four lenses with three million pixels each) towards 20 or 32 million pixel definition. The spaceship-like cameras made up of four to eight fixed cameras arranged

in a crown with a motorized PTZ camera in the center increasingly have 40 million pixels (5 × 8 million). These are the new standards for the installation or replacement of cameras, but such projects also have limits based on price and data storage. Many video surveillance systems are still equipped with full HD cameras (2 million pixels) or even just HD (1280 × 720 pixels). That said, PTZ's with full HD are still precise enough to read licence plates with their zoom.

If we know a camera's resolution, we can get a general sense of its ability to spy on us in daylight. More specifically, using optical formulas, we can calculate the maximum distance within which surveillance operations can be carried out without complications. These calculations should be done in three steps.

Step 1: Knowing the minimum pixel density required for the images to be usable

This is called spatial resolution. For instance, if the cops want to read a licence plate, the image of the plate must be made up of a minimum number of pixels or else it won't be readable. In the same way, identification through facial recognition requires that the image produced have at least 80 pixels between the face's eyes. The camera's spatial resolution, or its pixel density, can be expressed as the number of pixels in an image that correspond to a meter in reality. Here are the spatial resolutions, in pixels/meter, recommended by the Geneva Security Forum (a professional association for the sector) in 2016 on one hand, and by the judicial wing of the national gendarmerie on the other, to achieve different objectives:

- To "roughly understand an event in order to decide whether or not to trigger an intervention":
  - Geneva Security Forum: Between 1 and 30 pixels/meter
  - Gendarmerie: 30 pixels/meter
- To "verify the materiality of an event that has been the subject of an alert: differentiate between individuals, understand their interaction, see in which direction they are moving, in order to trigger an intervention or not":

    - Geneva Security Forum: 30 pixels/meter
    - Gendarmerie: 100 pixels/meter
- To "recognize an individual or object if it has been seen before":
    - Geneva Security Forum: 50 pixels/meter
- To "read license plates":
    - Geneva Security Forum: 100 pixels/meter
    - Gendarmerie: 200 pixels/meter

We can well imagine that these recommendations are intended to push municipalities towards ever more advanced equipment. They should be understood as requirements for optimal video surveillance conditions rather than as thresholds below which the various operations listed stop being possible. As can be seen, the guidelines of the Geneva Security Forum on this subject are much less stringent than those of the judicial wing of the national gendarmerie.

To get an approximate sense of the State's capacity to spy, it is better to base it on the lowest requirements in terms of spatial resolution, as these refer to conditions that are less than ideal for police work but where it is still possible. So we will use the numbers given by the Geneva Security Forum.

Step 2: Estimating the width of the maximum field of view that the camera can film while still maintaining the pixel density level given above

This is the horizontal field of view. For a given total number of pixels, the higher the pixel density required, the narrower the field of vision. To measure it, we can apply the following formula:

> Horizontal field of vision in meters = 2 x horizontal image definition in pixels / spatial resolution in pixels per meter

The horizontal image definition is the maximum number of pixels in an image on the horizontal axis. For example, the horizontal definition of an image in full HD (1920 × 1080 pixels) is 1920 pixels. In HD (1280 × 720 pixels), it is 1280 pixels.

Step 3: Measuring the maximum distance between the lens and the target of observation within which the camera captures an optimal image for the purpose of a given surveillance operation

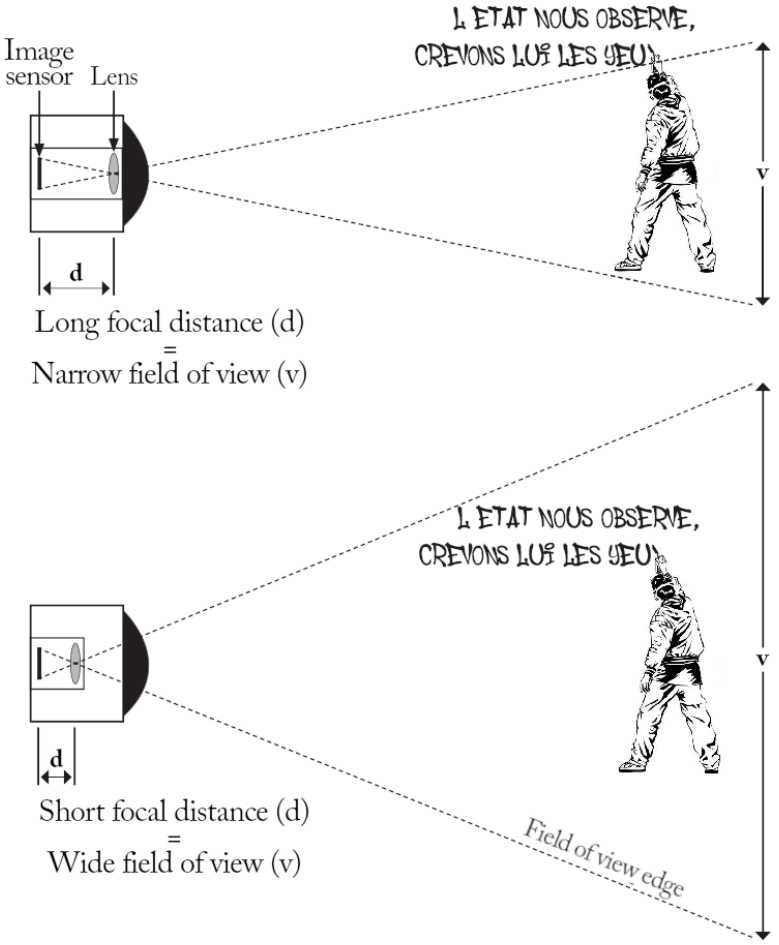
To measure this distance, we can use the following formula:

> Distance in meters = focal length in millimeters x horizontal field of vision in meters / height of the image sensor in millimeters

The image sensor inside the camera is a photosensitive surface shaped like a rectangle that captures the image. The larger this surface, the wider the field of vision. For video surveillance cameras, its size varies from 6 millimeters to 11 millimeters on the diagonal. For our calculations, we will take the largest value (11 mm), given that a wide angle is required for surveilling public space.

The focal length is the distance between the image sensor and the camera's lens (see the following diagram). The shorter it is, the wider the field of vision and the lower the image precision, since the pixels are more dispersed for a given number of pixels. And in fact, the focal length for cameras in cities is usually small (around 3 millimeters) in order to get a wide view on a section of street, an intersection, or a square. However, cameras are increasingly equipped with a variable focal length, which is commonly known as a zoom. Cameras like PTZs have a zoom that generally allows the focal length to increase from 2.8 mm to 12 mm, but more powerful zooms exist and are becoming more common, some of which allow the focal length to be increased 43 times.

Focal length diagram



How to find out the resolution and focal length of a street camera?

Knowing the technical data for a particular camera may be tricky, but it's possible to obtain some general information that will give you some pointers.

Depending on the year of installation, we can guess at the maximum resolution of a camera. A camera installed before 2019 will most likely have a resolution of no more than full HD (1920x1080 pixels), according to the experts at AN2V (the French national association for video protection) in their “Pixels” guides.

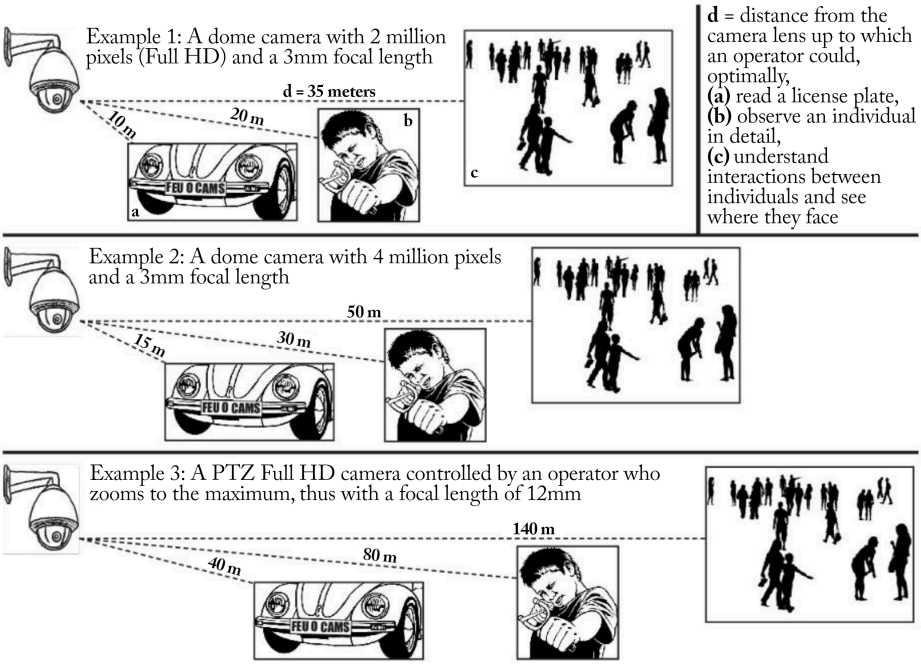
Depending on their shape, PTZ cameras, that have variable focal lengths, can sometimes be distinguished from dome cameras, that have fixed focal lengths. PTZ cameras are often larger and systematically suspended from a horizontal arm. In the case of multi-sensor cameras, the central lens is probably a PTZ with a zoom lens, or at least a PTZ camera.

Depending on the camera's position, when its focal length is fixed, you can guess its value. In a large space, such as a square or crossroads, the focal length will be reduced, often to around 3mm, for wide shots. In a narrow street, the focal length will usually be higher, to optimize image quality.

Depending on the brand, which in some cases is printed or indicated with a sticker on the camera, you can find technical information, or even the model, by consulting the product catalog on the Internet.

Three examples of commonly used cameras

For each of them, we can estimate the distance beyond which the image is no longer optimally useful.



The calculations in the diagram here are theoretical and should not cause us to ignore the full range of possibilities, in particular when it comes to recognizing or identifying an individual. In certain cases, a low-precision image might be enough to recognize a person if the local police already know them well. And also, even when the images themselves are not enough, they can still provide different levels of detail, such as the colour of someone's hair or the brand of their shoes which, in certain circumstances, can lead to the positive identification of an individual when paired with other information (such as testimonies). In particular, interpreting images to identify a person or to determine what they are doing relies on the judgment of the police who are running the investigation and the judge at trial. The police can claim to have identified someone by using other evidence from the investigation.

Can cameras really see at night?

One of the main difficulties with video surveillance is getting usable images when light levels are very low or very high (backlighting). Yet, municipalities are often only able to install traditional daytime cameras that rely on street lighting to continue filming in colour at night. In such cases, image quality is greatly reduced once darkness falls. The poor lighting conditions cause the image to be affected by what is known as "digital noise," which refers to many lighter and darker patches that give the image a grainy look.

Still, there are a number of technologies that can be used to optimize image quality in twilight and at night. Many cameras are now equipped with WDR (Wide Dynamic Range) which allows them to simultaneously correct over- and underexposure. To get a sense of how this works, the latest developments in WDR have a level of performance approximately equal to that of the human eye when dealing with backlighting and they are significantly better in twilight. However, WDR still only allows for black and white images at night.

To film at night, many video surveillance systems are equipped with cameras called "day/night." These have integrated infrared LEDs that are usually spread around the image sensor and produce a faint but visible red glow. At night, their footage is based on the infrared lights reflecting off people and objects. When the sun comes up, a visible light detector activates a mechanical filter that covers the image sensor. This prevents the infrared light from reaching the sensor, which would distort the colours in footage captured using visible light. The filter gets removed when the sun goes down again.

Although this technique allows for much clearer images at night by eliminating digital noise, it still has an important limitation: images produced using infrared LEDs are black and white (greyscale). Without colour, it is naturally more difficult to recognize an individual's clothing, bike, or car.

Tips and tricks for infrared LED cameras!

Materials with certain reflective properties, such as shiny clothing (or the reflective strip on a yellow vest), can sometimes be captured in unexpected shades of gray by infrared cameras. For example, a black jacket of a certain material might appear in a much lighter shade, and vice versa.

You could also create your own infrared overexposure to make yourself anonymous. Some say that self-lighting with infrared LEDs creates overexposure of the camera sensor at night, just as when taking a photo with back-lighting. For example, a cap fitted with infrared LEDs on the visor would prevent the cameras from recognizing faces at night.

If you're not sure whether it's a camera with infrared LEDs, you can check with your own camera. Camera lenses, like those installed on some smartphones, are capable of capturing wavelengths longer than those of the visible spectrum, including infrared. So when you take a photo of an infrared emitter, infrared appears on the screen.

Furthermore, the range of these types of cameras is often quite limited, since the quantity of infrared light emitted is not sufficient to create usable images beyond a distance of about 30 to 40 meters. The smaller the number of LEDs, the lower the camera's range. To increase their range, infrared floodlights are sometimes installed alongside. These are a sort of spotlight with a white or black screen that turns on automatically when it gets dark. The use of these powerful LEDs alongside cameras can provide a clear image at a distance, but at very close range (a few meters), it can result in overexposure, which can make it impossible to make out a person's face.

Another kind of camera capable of filming at night is so-called thermal cameras. In fact, these are heat sensors that are sensitive to the infrared heat emitted or reflected by bodies and other objects according to their temperature, regardless of the lighting conditions. They are not used to

recognize or identify people, because their resolution is low (generally 352 × 288 pixels or 704 × 576 pixels), but rather to detect the presence of people in a wide area. They can be found on military sites, industrial facilities that handle toxins, and critical industrial infrastructure as well as on the gendarmerie's helicopters and at certain border crossing points.

Thermal cameras for border control

For several years now, cops on the beaches of Nord-Pas-de-Calais, France, have been using thermal imaging cameras to detect migrants wishing to cross the English Channel.

In 2021, the Greek state installed thermal cameras along its entire border with Turkey. Spain plans to do the same at Mellila (a Spanish enclave in Morocco), in an attempt to prevent the regular attacks on the three eight-meter-high fences by migrants wishing to reach Europe.

Example of an image captured by a thermal camera, rendered in black and white.

Maintenance challenges and technical difficulties

To optimize their field of view and to protect them from a well-placed hammer blow, cameras are often installed at the top of a street light or post, about 7 or 8 meters off the ground. But this comes with several drawbacks for their operation, in particular the maintenance challenges that result. Even a small technical problem means bringing in a lift truck, which can be expensive. This leads to many cases where cameras don't

function as well as they could because they are not cleaned or repaired in a timely manner.

For instance, it is not unusual that day/night cameras with infrared LEDs get stuck in either day mode or night mode because the visible light detector is dirty, leading to the infrared filter staying on or off. If the filter is permanently in place, then the camera will film in black and white during the day and at night. If it is permanently deactivated, then the images shot at night are full of digital noise. A buildup of dirt on the LEDs can also greatly impact the quality of the footage, since the infrared lighting is partly blocked. Additionally, the heat of the LEDs attracts insects, in particular moths, that fly in front of the lens.

When installed up high, the camera's field of view might be blocked by tree branches, which can make the images less usable, as can weather, like rain, fog, snow, and low-angle sunlight.

Example of an image captured by a camera after raindrops have accumulated on the camera's lens.

Sticking cameras on top of a pole might protect them from vandalism, but it exposes them to another difficulty that, although minor, is still interesting to mention, and that is the degradation of the images due to the movement of the pole. The higher the camera, the more its footage is affected by the pole's movements. Is it possible that a strong wind can help us stay anonymous? In any case, thermal cameras are particularly sensitive to movement, and image processing software doesn't tolerate a difference of more than 0.015 millimeters between each point in the transmitted image.

Camera service life

While most cameras are designed to operate optimally for at least five years, infrared LEDs may only last for 20,000 hours, i.e. just two years of use if they are left on all the time, day and night. Replacing the LEDs every two years seems a complicated and costly maintenance operation, and one that may not be carried out on a regular basis.

Urban Supervision Centers (USC)

Most public video surveillance systems have an Urban Supervision Center (USC) where the footage from each camera is sent. There are some cities that don't have them, though. In those cases, either the video surveillance is only being used as research after the fact as part of a criminal investigation and is therefore not being watched in real time, or the footage can be watched directly in the city's police station. Apart from this latter case, surveillance typically goes through the Urban Supervision Center. Their modes of operation are not standardized nationally, and so it is worth learning about how they work in your city, which may be different from others. In this section, we will examine how USCs work: Who is watching the cameras? How? Using what equipment? And with what goal?

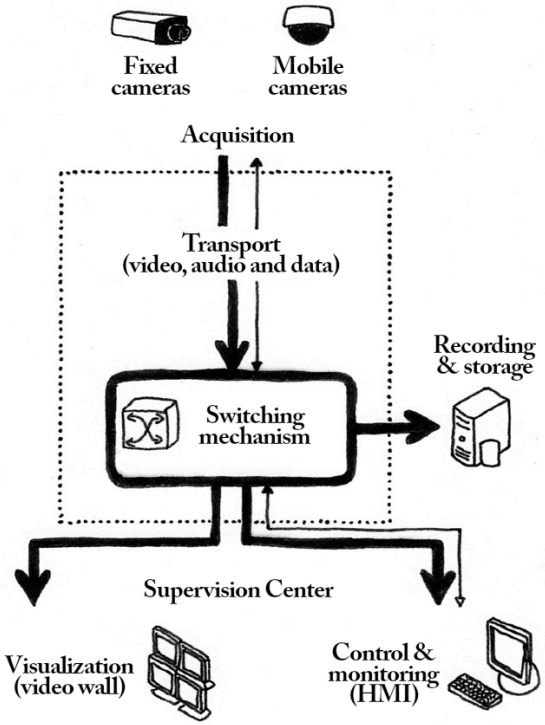


Image transmission from cameras to USCs

In recent years, digital cameras ("IP" cameras), which use the Internet to transmit images, have gradually replaced analog cameras, which use coaxial cables or radio waves (RLAN network: 2.4GHz and/or 5GHz frequency bands). In large cities, IP cameras are often connected to the fiber-optic network, enabling large quantities of video data to be transported to viewing stations and storage locations. In neighborhoods and municipalities where there is no fiber optic network, IP cameras are networked with Ethernet cables, or by wireless means such as WiFi or 3G/4G/5G networks. In Nice, for example, images are transmitted via the fiber-optic network, and by radio waves in areas where there is no fiber-optic network. In Strasbourg, data transmission is with Ethernet where no fiber is present. While wireless means of transmission have the advantage of reducing the risk of cable sabotage and facilitating camera installation, they are more limited in terms of data flow and open the door to other types of sabotage. For some years now, installers have been praising the virtues of 5G, which could partially solve this problem, with a transfer rate 14 times faster than 4G. The optimization of video surveillance is even one of the arguments put forward for the deployment of the 5G network.

USC operators

Every USC has a person who is legally responsible for the system. For public video surveillance systems, this is almost always the city's mayor. It is pretty easy to figure out who this person is by looking at the city's administrative newsletters and then it is possible to put pressure on them in one way or another. In terms of the other people and companies involved in the maintenance, installation, or communications of the system, more

research is required and the information won't always be available. In addition, the USC has “operators”. These are the people responsible for watching the footage from the cameras and triggering alerts. They might alert about anything from a fire to property crime, and could be involved in regulating traffic or issuing video tickets.

There are three things about the operators that we feel deserve attention. The first is the legal question of who can surveil public roads. It is currently illegal to entrust the surveillance of public roads to the personnel of a private company or to send public footage to a private company for analysis. In other words, the municipality is responsible for recruiting operators. In fact, municipalities need to recruit agents for this work or else assign the work to their existing agents. This is why most of the bootlickers who work in USCs are municipal cops and traffic enforcement officers. Also, the installation of video surveillance systems in cities is quite often accompanied by the creation of a municipal police force—in such cases, the USC is likely found in their headquarters. It is also worth noting that there is not, for the moment, a common training for video surveillance operators in France.

The second point deals with the ratio of cameras to operators. It is safe to say that there are generally too many cameras for the number of operators to watch them all. Video surveillance companies typically say that a single agent can't effectively watch more than five to eight screens at once. If we look at Nice's USC for example, which is the largest in France, we can see that the operators are understaffed. There are 2,510 cameras, which means they would need to always have between 314 and 592 operators, 24 hours a day, seven days a week, so that all the cameras can be constantly and effectively surveilled. But this is not the case, since only about a hundred operators work there, which means that under normal circumstances there aren't more than that. In Paris, according to 2020 numbers, there are 427 operator positions for 4,000 cameras. The same trend holds for smaller cities. For instance, Poissy (39,000 residents) has only three surveillance monitors for its 80 cameras and seven operators to watch them 24 hours a day, seven days a week. In these cases, the operators are watching between three and five times too many cameras to be “effective.” We also know that, in many smaller cities, the USCs are not staffed at night, except for on

certain specific days like December 31. Others have reduced staff at night, which further reduces the likelihood, which is already low during the day, of getting caught in the act during these hours. The footage may also be transmitted to the police station during the night. There is no standard practice in terms of when the cameras are being watched.

The third point deals with an operator's typical workday. According to one study, operators carry out a number of defined tasks during their workday. First of all, they carry out rounds of passive surveillance, which means quickly switching between all the cameras in order to catch anything unusual or any technical problem. Then, they carry out active surveillance, which means actively searching for crimes in progress. The operators often focus on cameras that show areas considered "at risk" and on individuals who are also seen this way (obviously, these are poor people, racialized people, youths, groups, people who are running, and so on). Also, in most USCs, the operators have to take notes about their activities and about information relayed by the police, which takes up a considerable portion of their time. Finally, operators spend a lot of their time not doing surveillance. Whether they take breaks or look at footage for reasons other than surveillance (one study describes an operator who was constantly looking at their own car to check that it hadn't been vandalized or stolen and another operator who spent his time checking out women and commenting on their appearance). This is why all the literature about the operator's work constantly emphasizes the fact that it's a shitty, boring job with high turnover. It isn't easy to take this information into account for our own activities, but we can at least be reassured that, despite the impressive technology in place, the human element can still fuck it all up. In this perspective, a study from 2010 states that during the 120 hours that "anthropologists" were watching the operators work, there were "no criminals identified either in real time or after the fact." Although we should take into account that how rare it is for operators to catch crimes in progress might have changed since 2010, they still don't have the ability to observe everything that's happening in the video stream they are watching. In a later section, we will discuss how the goal of automated video surveillance is to improve the efficacy of video surveillance.

The supervision area

Every surveillance station is equipped with a few things: a computer with a "human-machine interface"; two screens: a small one for the graphical user interface (often a map showing all the surveillance cameras) and another that shows the footage; a steering joystick for mobile cameras; and a means of communication for contacting emergency services (cops, firefighters, and so on). From these basic elements, each USC is organized in its own way based on its size and its surveillance goals.

Let's look at the example of Nice's USC again, as it is the "vanguard" of video surveillance, to see one way that a supervision center can operate and be set up. In 2020, the USC handled footage from 2,510 cameras. It operates 24 hours a day, seven days a week. It is located in the municipal police station. About a hundred operators work there. From an equipment perspective, the USC is made up of three rooms with a total of about 90 screens. The first room handles events related to public space. Its goal is to prevent crimes against people and property in progress. The images can be relayed in real time "to the national police, the border police, or the gendarmerie." The municipal police boasts that its CSU has led to 4,227 arrests in just under nine years, which works out to a little more than one arrest a day. This room is also responsible for "preventing natural or technological hazards, helping people in need, and fire prevention." The second room handles "the protection of schools and public transit

(streetcars and buses)," and we know that the streetcar system has 900 cameras and that there is a camera in front of every school. The third room is dedicated to video ticketing and traffic control. In addition to cameras, Nice's USC is connected to the alarm system in public buildings and to a system that allows business owners and other citizens who have been trained by the municipal police to send SMS alerts.

What do these operators do?

Remote control of cameras

Concretely, operators have a map in front of them that shows all the cameras, a viewing monitor, and a joystick. The operations they can carry out are basically as follows. They select a camera on the map. They view it on the viewing monitor. They can then zoom in or aim the camera, if it has a zoom and is mobile, by means of the joystick in order to carry out more precise surveillance. If the operator notices an "offence" or "uncivil behavior" in the view of a camera but the target leaves the camera's view, they can try using the graphical interface to track them. They then take control of the next camera. It is important to note that this operation is only possible when there are lots of cameras.

Automatic programmed operations

In addition to the operators' basic surveillance described above, they can also program the cameras in four different ways:

Dynamic masking: They can mask parts of a camera's field of view, often those parts that a camera is not allowed to observe. This function is often used to mask private spaces that are captured by public cameras. Legally, this is always supposed to be done.

Prepositioning: This function involves assigning positions to a mobile camera. It is possible to assign several positions on a timed cycle. The camera then spends so much time on one area and so much time on another according to its program.

Memorizing a frame: When an operator is steering a camera, they can memorize a point of interest (a frame) so as to be able to return to it through a simple action at their convenience after having moved the same camera or after setting it to cycle.

Freezing a camera: This function involves the use of a command to freeze a camera on a given frame. The camera will only be released following another command from the operator.

Alerting the police

One of the major operations carried out by operators is to alert the police (excluding video ticketing where operators are authorized to issue tickets independently after having identified a vehicle's licence plates).

Once an illegal activity or an "unusual" individual has been identified, the operator's role is to issue an alert and potentially follow the police's response in real time or even guide them. In the latter case, the operator does not only alert the police about an incident, but follows the individual in order to guide the police.

In some USCs. such as in Vitrolles, a system is in place to relay live footage directly to the police. This makes it possible for the police to follow someone themselves rather than going through the USC. In police stations that have these systems, it is possible for the police to not only access live footage, but also "take over the camera and steer it autonomously if necessary." In some cities, such as Crépy-en-Valois and Bagnolet, the municipal police have direct access to all the surveillance cameras in the city on their electronic tablets thanks to an "ultrasecure" wifi network that gives them access to the footage on demand. It is thus clear that there are multiple procedures for issuing alerts and passing along live footage. Sometimes the operators issue the alert and do the follow-up while other times there are systems in place to transmit images or allow for cameras to be steered by the police themselves.

Video ticketing

Video ticketing enables authorized operators to identify traffic violations filmed by a camera on their control screen. Images of the vehicle, its license plate and potentially its occupants are captured to prove the offence. The operator then electronically issues an official report, which will be used to issue a fine at the home address of the holder of the vehicle registration document. The following offences may be identified:

- Failure to obey signals requiring vehicles to stop (red lights, stop signs, etc.)
- Failure to comply with speed limits.
- Failure to respect safety distances between vehicles.
- Use of lanes and roadways reserved for certain categories of vehicles, such as buses and cabs.
- Failure to wear seat belts.
- Use of hand-held cell phones.
- Driving, stopping or parking on emergency lanes.
- Overlapping and crossing solid lines.
- Non-compliance with overtaking rules.
- Failure to respect bicycle lanes.
- Failure to wear a helmet on a motorized two-wheeled vehicle.
- Since 2019, the offence of not having insurance is also subject to fines.

Integrating video surveillance systems

In the past several years, many politicians, managers, and other boosters of technologies of control have been encouraging the development of methods of integrating video surveillance with the goal of reducing costs and surveilling wider areas. Sometimes, their desires have run up against legislation that was a bit too restrictive for their liking. But, since the

2007 crime prevention bill and the 2021 global security law, the final barriers to this have fallen. Today, different levels of local governments, regardless of their type, can acquire, install, and maintain an integrated video surveillance network. These networks transmit footage taken on public roads or in areas open to the public in their member municipalities to a regional USC. Then, by means of centralized mechanisms for viewing recordings, the footage is used by municipal police and regional officers.

Departmental and regional governments can also set up video surveillance systems around public buildings and structures in their sector that they are responsible for (schools, roads, administrative buildings).

However, integration of this kind is the exception rather than the rule. But the national video protection association (AN2V) is already running a campaign to encourage the spread of video surveillance by convincing local representatives to join integration projects. In their words, it is a matter of avoiding "gaps in the security continuum," notably by being able to track someone's movements between municipalities. They also see it as a way of combatting "passive cameras" whose footage is not watched and can only be used after being requisitioned by the police or the gendarmerie, whereas with a USC and its agents watching the monitors, the police and the mayor can be alerted in real time. One of AN2V's targets are the approximately 35,000 municipalities of fewer than 10,000 residents in France, mostly rural or suburban, that don't have the funds to get their own USC. To convince them, AN2V is relying on increasingly sophisticated forms of automated video surveillance. This allows them to reduce the number of operators, as they won't be required to observe a large number of screens, but rather just receive alerts from the computer.

In the meantime, there are already some examples that can give us a sense of what integration allows for (integration between Paris and the surrounding cities will be discussed in "Video surveillance in the Paris area", p. 64).

The "Plaine vallée" agglomeration (18 municipalities with 183,806 residents) in the Val-d'Oise, is a pioneer in this area. Since 2007, it has established a regional video protection system made up of 212 cameras covering the whole territory (75 km^2) as well as 18 nomadic cameras.

Twenty-three operators split between two USCs provide coverage 24 hours a day, seven days a week.

Seine-et-Yvelines Numérique (SYN) is a mixed, open association that counts two departments in the Île-de-France region among its members (Hauts-de-Seine and Yvelines) as well as thirty municipalities in those departments, nine agglomerations of municipalities, and organizations like SDIS 78 (the Yvelines emergency fire service). Their mission includes integrating the video protection departments of public institutions. This started with the cameras on 116 middle schools, 70 administrative buildings, and 43 fire stations in the Yvelines department. More than 1,900 cameras have been installed to date. Because of the global security law, SYN is now planning to integrate the video protection systems in the public space, which involves linking together each city's systems. This was piloted in a few cities and agglomerations in 2022 before being opened up in 2023 for more cities to opt in.

The Centre de supervision de l'Eurométropole de Strasbourg (supervision center for the European urban area of Strasbourg) manages 426 cameras on public streets in 25 municipalities as of early 2022 as well as 300 in spaces that are open to the public. And other municipalities that do not have their own equipment are on the verge of being integrated into the system. In 2014, sensors were installed in Strasbourg on an experimental basis. But, as is often the case, they have remained in place. They are capable of detecting the sound signatures of "situations that threaten to disrupt the peace in public spaces at night" and of alerting the agents who are watching the cameras.

The Centre intercommunal urbain de vidéoprotection (urban area video protection center) in Nîmes is an integrated network of almost 1,000 cameras with 20 operators who watch them 24 hours a day, seven days a week, across the 22 municipalities of the Nîmes metropolitan area. Behind a mosaic of 33 screens that can each show footage from 24 cameras, five teams of four operators watch in turn.

Building lobbies

Real-time viewing of cameras in the halls of residential buildings can be passed on to the cops by decision of the co-owners in the event of occupation of common areas. In the event of an "emergency" following an alert from the building manager, the cops can dispense with the owners' authorization.

Footage in the courts

We've covered cases where footage is watched in real time. But in terms of footage that is watched after the fact in the context of a legal proceeding, there are several things to note. First, footage is only saved for a maximum of thirty days, beyond which time it must be erased unless courts have requested for it to be kept. Each USC sets its own timeframe for saving footage (generally between fifteen and thirty days). Also, the footage can only be sent to the police if it is part of certain types of investigations, such as a flagrancy investigation, a preliminary inquiry, or a judicial investigation. There is an exception to this in the law that deals with "emergency situations or heightened risk of terrorist acts." However, in practice, video surveillance departments sometimes pass along footage outside of any legal framework. One example is Alexandre Benalla, a former security officer for the French president, who got access to video surveillance footage without a judicial request.

There are criteria for how footage can be turned over to the police: it needs to be given directly to them in hard copy; there cannot be any cutting of the footage; it is generally done using a medium that can't be rewritten (like a USB key or a CD); and the footage is in a format that can't be read using standard market software. The police then describe the footage in a written statement that can include screenshots, which is included in the judicial file (along with the sealed physical copy).

It is important to note that private video surveillance footage can also be used in criminal proceedings. Banks, businesses, individuals… These kinds of video surveillance cameras are rapidly increasing. Technically, they need to be authorized by the prefect before they can be installed with an explanation about why, for instance, it's necessary to surveil the area around the building. Cameras owned by individuals are not allowed to film public roads, but in practice this is increasingly the case. It is possible that the use of such footage by the police could be challenged in court.

In any case, private footage can be requisitioned by the police or they can be spontaneously passed on by zealous property owners. It is important

to remember to be wary of intercoms equipped with cameras, as some of these film constantly or are motion activated, have night vision, or can save footage. In the United States, Amazon's Ring has made agreements with the police, who can contact any user of their smart doorbells within 400 meters of a crime. This lets them collect up to 12 hours of footage without a warrant. Things haven't reached this point in France, but there have been cases where intercom footage was provided after the fact to police, such as Ivan's case in the Paris area in 2022.[5] The length of time that footage from private cameras can be stored is in theory limited to 30 days, as is the case with public cameras.

An example of doorbell cameras.

[5] See "Some Initial Notes on the Investigation File Against Ivan".[a]

[a] https://notrace.how/resources/#quelques-premiers-elements-du-dossier-d-enquete-contre-ivan

Automated video surveillance

Types of automated video surveillance software

Automated or algorithmic video surveillance, which is also called augmented or smart video surveillance by those who market it, is presented as the future of the field. Everyone involved agrees that the increase in the number of cameras, following current trends, needs to go along with automated video surveillance. This is because, although the number of cameras is increasing, the number of operators is not keeping pace. As we have seen, there are never enough operators to watch all the cameras live, especially not effectively. Without automated video surveillance, increasing the number of cameras per operator reduces the quality of the surveillance.

Automated video surveillance software is thus trying to make it so that all camera footage gets analyzed according to certain criteria in order to alert the operators who then assess the validity of the alert. In other words, automated video surveillance allows for the number of cameras to increase without overwhelming the operators with too much footage.

Because it is so important, more and more software of this kind is being marketed by companies. It involves adding a layer of algorithms to "classic" video surveillance cameras. The goal here is to automate the analysis of camera footage which has thus far been analyzed by humans.

Most smart software can be added to any array of existing cameras—there is no need to have a certain kind of camera or infrastructure, it is just a matter of adding the software to the video surveillance interface.

Until the second Olympics law (see "From the streets of Levallois-Perret to the 2024 Olympics", p. 7), there was no legislation specifically governing automated video surveillance. That said, it was not illegal to use it. In an opinion published in July 2022, the CNIL made a distinction between legitimate and illegitimate uses. They considered it legitimate to be used for statistical purposes as long as the results were anonymous. For example: "A system that serves to calculate the number of people in a subway train in order to show travellers which lines are least busy so they can use them."

It was considered illegitimate if used to identify or prosecute crimes. An example is the software used in Marseille to detect damage to street furniture. Also, they pointed out that in any case, the rules around data protection include the right to opt out of being processed by an algorithm, which is absolutely not applied or even applicable in almost all cases. This opinion by the CNIL might leave you thinking they were opening the door to banning this technology which is, as we know, already used in "legitimate" and "illegitimate" ways in at least fifty cities across France. But this was clearly not the case as, on the contrary, the CNIL called for the immediate creation of a new legal framework for automated video surveillance. The second Olympics law is the first step. In other words, rather than pushing to outlaw uses that don't conform to the laws in place, the CNIL wants to begin legalizing them.

These are the software features that we are sure are actually being used in cities in France:

Automatic licence plate recognition (ALPR)

This technology identifies vehicle licence plates using optical character recognition. To film licence plates at night, the cameras emit infrared light. The software automatically reads the licence plates and sends an alert if it detects a plate number that is found in a predefined database. These readers allow for an alert to be generated when a positive link is made between a licence plate and these files. The cameras capture and store images of the licence plates and of the vehicles as well as the date, time, and location of each vehicle photographed before transmitting that information to the police. When a vehicle is not linked to the database, these details and images are saved for a maximum of eight days; if there is a positive link, they can be saved for up to a month.

The database in France that is used for comparisons and alerts is made up of files from the FOVeS files (record of objects and vehicles reported stolen) and the SIS files (Schengen information system). The SIS includes people who are wanted for arrest or extradition, missing persons, some people who are banned from a given area, and objects that are sought in the context of a seizure or a criminal case. In France, it brings in data

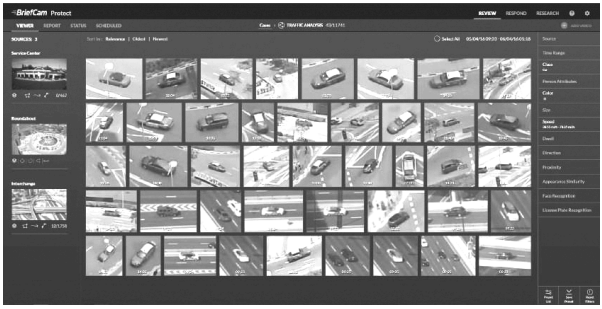
from the FPR (database of wanted persons) which lists people with arrest warrants, those with driving prohibitions or who are under court-ordered conditions, and those who have been flagged as dangers to national security (the famous “fiches S”, or S list). We aren't sure of this and don't have any examples at this time, but it seems possible that automated licence plate readers could alert the police to the presence and movements of people on the S list (if the vehicle of the person on the list is included in their file).

The cameras used for ALPR look either like directional cameras or like a sort of box. In the latter case, there are lights on the side that project the infrared light needed for the cameras to work at night as well as by day. In addition to these cameras that we can find in the urban space, the gendarmes and police at the national and municipal levels have vehicles equipped with automated licence plate reader cameras that are inside the car and in the roof lights. These systems function as follows: when the vehicle is turned on, the cameras automatically read all the licence plates in their field of vision. If a plate is found in the FOVeS or SIS files, it results in an alert that includes the reasons for the alert and the actions to take.

In 2020, during an investigation into arson attacks against relay antennas, the police looked for licence plates captured overnight by an automated licence plate reader owned by a private security company in a village some twenty kilometers away from the site of the fire. We don't know if this installation was legal, but it shows that private actors can also have plate readers and that the police don't hesitate to make use of them.

Searching and extracting footage from an archive of video surveillance using keywords

Let's imagine that some windows were broken by a person dressed in blue in front of some cameras. Using this automated video surveillance module, the cops can search the stored footage of nearby cameras. They would enter the corresponding keywords (height, gender, clothing colour, movement speed) and the software would then try to filter all the footage to present any that included people dressed in blue. This would allow them, if there were enough cameras, to more easily follow the path of the person to identify them.



This service is offered by the Israeli company Briefcam which, although it only provided equipment to 35 French cities in 2020 (Nîmes, Nice, Aix-Les Bain, Vannes, Deauville, Woippy, Roubaix, La Baule-Escoublac, Gex, Vaulx-en-Velin, Vienne, Moirans, Caveirac, Vitrolles) provided equipment to 200 of them in 2023. The French national train company (SNCF) uses their software in Paris and Marseille. In 2019 in Nîmes, shape-identifying software was used for 1,085 footage requests as part of investigations! (An article that we happened to find states that the Paris police department has shape-identifying software created by Briefcam. This is the only place where we have seen this information, so it needs to be confirmed.)

This company sells not only this software but facial recognition software as well. All it takes is a simple change in the settings of Briefcam's software for it to start recognizing not only a person's direction of movement and clothing but also their face. From a technical standpoint, in the cities where this software is in use, we are only a click away from facial recognition.

The French company Two-i, based in Metz, also offers software that allows searching in an archive of video surveillance.

Predictive analysis

The "Map revelation" software created by the company Sureté globale, based in Angers, carries out predictive analysis and also graphical and geographical analysis on "delinquency, incidents, sales, events…" Using an algorithm, the software is intended to predict future crimes using data collected by the police. The idea is to use these predictions to better guide the cops' actions. It can lead to, for instance, more police patrols in a given location at a given time because past statistics have shown that it is likely

that something will happen. Although it is not technically automated video surveillance, this software is nonetheless designed so that it can incorporate different types of sensors, including video surveillance and alarms, into its maps and interfaces. In Montpellier, the data is provided by both the national police ("car thefts, break-ins, armed robberies…") and the city ("abuse investigations, social service involvement, complaints in social housing…"). The cities of Montauban, Colombes, Lille, Angers, Villeurbanne, Lyon, and Montpellier, as well as organizations like the national gendarmerie, the Paris police department, and the border police all have this kind of software.

Sound identification

There is software that can detect noises that are considered suspicious. This involves, for example, identifying "a sound signature corresponding to a situation that threatens to disrupt the peace in public spaces at night". Through its connection to the video surveillance system and the USC, an alert issued by this technology can then be confirmed using cameras located near the microphone either manually or by automatically orienting the cameras in the right direction. The sound signatures in question generally correspond to events like yelling, breaking glass, car horns, alarms, and paint being sprayed.

Although this technology was banned by the CNIL in 2019 in Saint-Étienne following an outcry by local organizations that claimed it amounted to "unlawful processing of personal information," it is widely

used in France. In fact, the company Sensivic claims to have signed a contract with the Ministry of the Interior to provide "security services" for the 2024 Olympic Games and that its equipment is deployed in at least 25 French cities, mostly in the southern Provence-Alpes-Côte d'Azur region and in Yvelines. The city of Orléans also has these kinds of sensors and they continue to be used despite local organizing against them. It seems like the company considers the technology legal, stating that it is impossible to "use the microphones to get access to voices or conversations and that any data that might be considered personal in nature is not accessible."

Detecting theft in supermarkets

Automated video surveillance is also used in supermarkets in order to facilitate the pursuit of "thieves." In this case, the software issues an alert when it detects suspicious movements that might indicate a theft. These practices are not legal, as the CNIL pointed out in 2020. Once again, this did nothing to stop the use of this technology. Products made by three companies seem to be marketed and used in France:

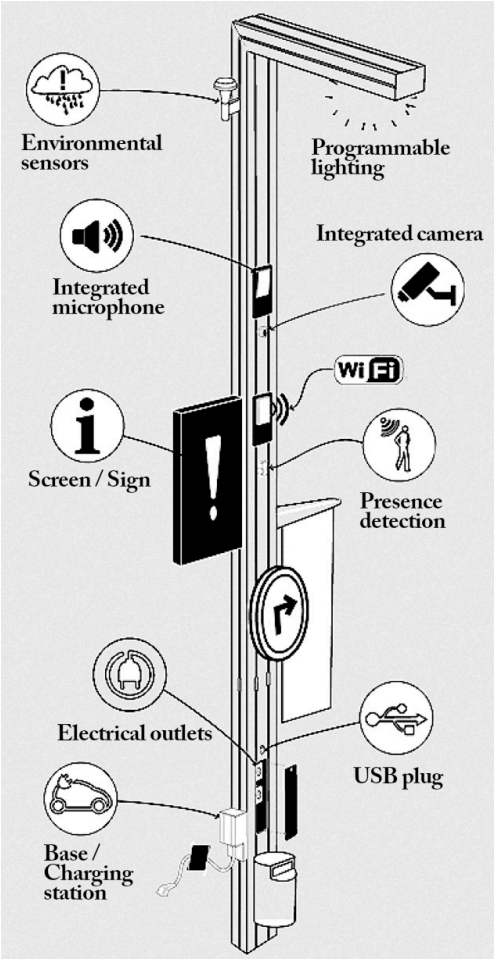
Anaveo, a 320-person company, specializes in video surveillance for big stores. Its software "SuspectTracker" promises to process footage from cameras to analyze "suspicious behaviors," such as "movements towards a stroller, backpack, or pants or coat pocket." Their marketing casually mentions that the thefts it detects will be added to its database so as to continually improve the algorithm. We don't know precisely how many or which stores this company serves, but we know it has at least sold its software to a Carrefour Market in Bourges and to an Intermarché in Artenay.

Oxania, a startup founded in 2019, created software called "Retail Solutions" that is able to "recognize the gestures associated with theft in real time, detect behaviors, dangerous situations, customers' journeys, and much more." The product launch video calmly admits it carries out biometric analysis of those present in the store: body heat, movements, bodies…

Veesion, a Paris-based startup that sells a "gesture recognition" software made up of "one software component that identifies people, another that localizes the limbs on the body, another that identifies objects of interest…" which it uses to issue an alert on the telephones of the store's employees. As a bonus, Veesion offers to analyze "your theft history and to provide personalized recommendations." We know that this company has sold its software to more than 120 stores in France, including certain Monoprix, Franprix, Carrefour, Super U Express and Bio c'Bon.

Smart water misters with integrated cameras

This is not technically an example of automated video surveillance, but rather of "intelligent all-in-one posts" that demonstrate the current "smart city" dream: an ultraconnected city loaded with technologies that integrate artificial intelligence. The water mister designed by the French company Technilum, in addition to its refreshing function, also includes "discrete 180° video surveillance cameras, differentiated motion detectors (pedestrians or vehicles) that can adjust the brightness or trigger an alert, weather and pollution sensors, vibration detectors (in the event of attempted vandalism), interactive screens, and also loudspeakers, plugs for electric vehicles, and, of course, internet access (Wi-Fi and Li-Fi)." Technilum has provided its super water misters to a city on the outskirts of Cannes, Mandelieu-la-Napoule. This company offers as well a whole range of smart light poles in addition to the misters.



Smart water mister designed by the French company Technilum.

Counting

Some software allow counting the number of people in a space at a given time. For instance, the French national train company (SNCF) has tested these kinds of tools in Paris in the "Bibliothèque François Mitterand" station, in 11 stations on the RER line C, and in the Antibes station.

Loitering detection

There is software that can identify people who spend a certain amount of time in the same spot, which allows for tracking poor people who occupy the public space. This kind of technology was notably used in the city of Suresnes. Similarly, the company that operates the Parisian metro experimented with a system in 2017 to detect people who stayed still for more than five minutes. The results were rather inconclusive, since it tended to detect "users who were waiting to meet someone or who were looking up how to get to their destination."

Crowd detection

Several cities in France have software that issues an automatic alert any time a crowd gathers.

Detecting suspicious objects

Software exists to detect objects that have been abandoned in public transit or public spaces.

Detecting weapons

The French company Two-i sells software that, among other functions, can recognize weapons.

Detecting social distancing

Two-i's software allows to automatically calculate the distance between individuals in a camera's field of vision. This makes it possible to analyze and record instances where social distancing for COVID-19 is not being respected.

Detecting "loss of verticality"

This allows detecting people who fall.

Fire detection

This allows detecting fires.

Perimeter protection

This software can spot any intrusion into a defined area. This could be a building's property or the area around a bank machine.

Detecting mask wearing

The software we have discussed so far is actually in use in cities across France, but from now, we will list software that has only been tested or that has been formally banned after testing.

The city of Cannes and the Parisian metro used software by Datakalab to do this. In Cannes, between April and May 2020, it was used to "assess mask wearing before the end of the lockdown" by counting those wearing and not wearing a mask. The software was first used in three markets in the city, and then in buses. In Paris, the software was used for three months starting on May 11, 2020, in the station Châtelet-les-Halles. A dozen cameras were used to send texts and emails to the transit company about changes in the percentage of people wearing masks over the course of the day. These experiments were ultimately "put on hold" by the CNIL. Although the CNIL said the software was respectful of personal information due to its anonymization system, it ultimately decided that "this system does not allow users to express their consent—shaking your head to indicate refusal is insufficient." This ultimately left the company to think of another way for transit users to show their refusal.

Analyzing emotions

In 2019, the city of Nice decided to use software from the company Two-i to analyze the emotions of streetcar passengers. This software claimed to detect stress, peacefulness, anxiety, joy, or even depression. In the words of the company, "real time emotional cartography reveals potentially problematic or dangerous situations. Deploying security guards dynamically in an area where people are feeling tension and stress can be a simple strategy for avoiding problems." In other words, this software analyzes the emotions of individuals or groups and issues alerts if they are related to behaviors considered to be "at risk" in order to "identify potential suspects before they act." This dystopian project was finally abandoned for technical reasons, the transit company's computer network not being robust enough.

Volunteers (snitches) sending cellphone footage to USCs

In early 2018, the city of Nice tested a system to allow volunteers of the neighbourhood watch variety, neighbourhood associations, and municipal workers to send footage using their cellphones to the USC in order to report on crimes, "uncivil behavior", and so on. Reporty is an application developed by an Israeli startup founded by the former prime minister Ehoud Barak which allows for the real time sharing of images with the municipal police's USC which can then geolocalize the phone's position to facilitate police intervention. In March 2018, the CNIL banned this application, noting that "this system is disproportionate and poses serious privacy risks" notably due to "its weak protections against misuse."

Multimedia dissuasion cameras with sound and light

In Cannet since 2015 and Hyères since 2019, there were already cameras equipped with loudspeakers through which the police can speak and reprimand "uncivil behavior" (like telling someone to keep their dog on a leash or to point out illegal parking). Now, new smart cameras are being designed that can automatically identify behavior considered suspicious using artificial intelligence, whether by video or audio. These cameras are

equipped with microphones, artificial intelligence, flashes, and speakers. Once the behavior has been detected, the camera can emit flashes in the direction of whatever triggered it while also broadcasting a message. For example, if the behavior detected is a group of people making noise, the message automatically emitted from the loudspeaker would be "You are in a video protected area and security is on the way."

Automatic detection of fare evasion in public transportation

From May to July 2022 in Besançon, two Keolis bus lines were equipped with sensors made up of two cameras and software that could estimate the amount of fare evasion. The stated goal was to "combat fare evasion in public transportation through behavioral science." The software counted the passengers as they boarded while also tracking the number of fares paid, then carried out a subtraction before displaying on a screen in real time the number of people who didn't pay. In addition to displaying in real time the number of potential fare evaders, the screen also displayed one of three messages based on the level of fare payment: "Congratulations, you are great" when the amount of fare evasion was low, "Play along" with subdued warnings when the rate of fare evasion increased, and finally an alert when the number of people not paying was high. The company that advised Keolis in the use of this technology was NF Etudes. They present themselves as consultants, support, and testers specializing in social psychology and behavioral science. Despite its designers claims that the "fraud-o-meter" aims to "encourage individuals to change their behavior without coercing them," it also generates statistics about when and where fare evasion is occurring which allows them to adjust enforcement schedules or even to send a patrol of fare inspectors in real time if the amount of nonpayment is high.

Facial recognition

Although it is certainly related, facial recognition is not a form of automated video surveillance. It is a tool that matches each face to a unique "signature"

by measuring the distance between different selected points on the face, which allows for the recognition or identification of a given person in an image.

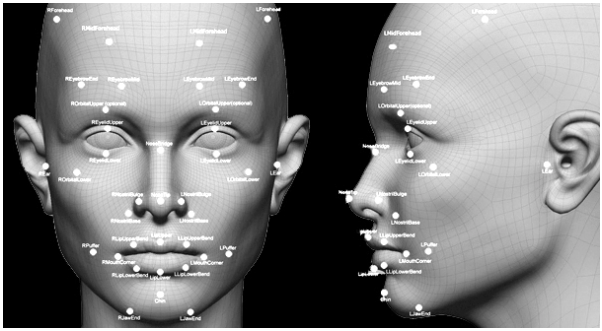
Facial recognition is emerging everywhere as an inevitable horizon in surveillance technology. It has become a recurring topic in recent years—facial recognition technology has really gotten people talking. In the mass of information on the subject, it is increasingly difficult to understand its uses and, especially, its capacities at a given place and time. This is doubly true because the actors in this field often have a reason to exaggerate or minimize its development based on their position (a niche startup that wants to brag about its product or a public body that wants to reassure citizens who are worried about individual liberties) and the context (reticent citizens or a political campaign about security). In discussions on this subject, China often serves as a scarecrow, warning us of a possible future in which facial recognition technology is used in classrooms and train stations, databases connect people's photos with their social credit (on which is then based their access to various public services and their social and economic rights), and cops wear glasses that are equipped with facial recognition. These dystopian tools obviously give us the chills, but let's not forget that their repressive power also depends on the fear they generate, and if we are to one day endure the future promised to us by bad sci-fi films, currently, facial recognition is limited by the technology and infrastructure it relies on.

In France, its use is still limited, but we would be naive (and uninformed) if we believed we are being spared, because facial recognition is indeed here, and the State and private companies aren't holding back. For instance, facial recognition using the TAJ (police records system) has been authorized since 2012 and was used on average a thousand times per day in France in 2019 and more than 1,200 times a day in 2020. These numbers represent the number of times the system was used, not necessarily the number of times that its use led to meaningful results for the cops (often, the quality of the image being searched is insufficient to identify someone or the person is not in the database, which leads to the facial recognition process failing).

Facial recognition can have two functions: one is authentification, which means it serves to confirm someone's identity by comparing an image of their face to another one saved in a file (an example is using facial recognition to unlock a smartphone, for instance) and another is identification, which involves recognizing and following a person across several images without necessarily knowing their identity (finding and following a person in a crowd).

The bulk of facial recognition applications in France so far deal with authentification. Several databases contain photos that are used for facial recognition. The largest is the TES which contains photos from ID cards and passports. For the moment, it is meant to be used only to verify that the person being screened is the same as the person on the ID. It is a database that is mostly used at border crossings, and it cannot legally be used by police or the courts in other contexts. However, the TAJ is also used for facial recognition, especially by the police. This database contains the personal information of people who have had dealings with the police (who were detained, witnesses, or victims) and includes photos (in 2018, this database contained 19 million files and 8 million photographs of faces). From there, the police can take a person's photo during a stop and compare it with the TAJ using facial recognition to see if they find their identity, and they can also use snippets from video surveillance or images found online, on a phone, or on social media as part of their investigations.

And if it was still generally possible to refuse to have your photo taken while you were detained before, a new law in April 2022—which allows the police to take pictures and fingerprints by force if the charges carry a maximum sentence of at least three years—means it is becoming harder and harder to do.



In terms of the use of facial recognition with video surveillance, it generally serves to identify people. In theory, a trained operator or even a piece of software could follow a person across a city's network of cameras using a photo extracted from a database or even one taken by the cameras (as long as they are of good enough quality to be usable). The more technology for identifying people advances and the more gaps in the camera network are closed, the more the police will be able to precisely follow anyone's movements. Today, real time facial recognition is encountering legal hurdles that are keeping it from widespread and indiscriminate use as part of video surveillance systems. That said, the technical capacity exists, and so we are only a few laws and a few infrastructural changes away from seeing these kinds of systems put in place. In Nîmes, for instance, the deputy mayor even bragged about being "just one click away from facial recognition" (the software they have is already capable of it, it just needs to be activated). In recent years, there was reason to worry that the 2024 Olympic games would be used as an excuse to implement or test facial recognition in public spaces, but the government ultimately announced this would not be done, although it did open the door even wider to automated video surveillance. Let's not have any illusions about the fact that the government, the police, and the security industry are impatiently awaiting the right moment to reopen the debate. We need to then expect that in the next few years, they will try again to authorize the use of facial recognition in video surveillance systems, likely following the classic pattern for security measures: it will first be used within a restricted framework to reassure civic-minded people while also taking a first step towards normalization and wider acceptance (like a congressperson tried

to do in 2017 by proposing to use facial recognition only from the “S list”, a list of individuals deemed security threats).

Video surveillance in the Paris area

Since 2009, the camera network in the city of Paris has developed in accordance with the PVPP plan (Paris video protection plan), also known as the "1,000 cameras" plan. This plan involved determining the location of cameras, their functions, and who watches them as well as setting the terms with the company that installs them and the one that maintains and upgrades them and their network of 600 km of dedicated fibre-optic cable.[6] It falls under the responsibility of the Paris police department, and it also involves viewing some footage from the public transit companies responsible for the metro, buses, and trains.

A second plan, PVPP 2, was adopted in 2015 (for 6.3 million euros) and was motivated in part by the attack on the offices of the newspaper Libération in 2013, in which video surveillance played a prominent role in tracking down the person responsible. It involves new cameras, including the ones that look like a bunch of grapes (see "Types of cameras", p. 15) and an increased presence in redesigned or newly built neighbourhoods, which brings the total number of cameras to 4,171 (according to the group "Quadrature du net"). These new installations will make Paris's 1st district the most heavily surveilled part of the city, with one camera per 315 residents. Another argument used to justify the implementation of this second plan was to combat air pollution. According to the local government, cameras allow for more enforcement on streets that are closed or restricted to traffic.

It is also expected that by 2026, the number of police dedicated to video ticketing will increase.

The 2024 Olympics will serve as a pretext for the installation of new cameras (see "From the streets of Levallois-Perret to the 2024 Olympics", p. 7). As part of the PVPP, the Paris municipal government anticipates installing 320 new cameras by 2026, half of them before the Olympics and

[6] A contract between the national government and IRIS-PVPP, a subsidiary of GDF Suez, established in Courbevoie and financed jointly by the national government and the City of Paris for 5 million euros over 15 years.

a third near Olympic sites. For their part, the Paris police department has promised to install 415 new cameras near Olympic sites and on roads that will be reserved for the Olympics in 2024. For the 500 cameras announced by the Minister of the Interior, it is not clear if those will be in addition to these already too numerous new installations.

At the end of 2020, there were a total of 37,800 cameras in the Île-de-France region around Paris that were linked to various USCs within the PVPP framework. Among those cameras, there are the permanent cameras on public streets, some of which belong to the city (such as the 300 that were formerly dedicated to video ticketing and whose footage is kept for the same amount of time as other cameras) and others to the national government. Nomadic cameras (see "Types of cameras", p. 15) are also connected to this network, and they can be added at a moment's notice by the Paris police department, as can, more recently, body cameras. In addition to this, there is "third-party footage" which broadens the cameras' coverage to other places open to the public through 102 partnerships with public and private companies. Within this network of cameras are those of the company responsible for the Parisian metro and bus network, of the national train company (SNCF) in the Paris area, the Gerfaut traffic network, the Louvre Museum, the Louvre Carrousel, the Paris Congress Centre, the Porte de Versailles, Villepinte, and Bourget exhibition centers, the Parc des Princes, the Stade de France (the region's largest stadium), and the following shopping centers: Aéroville, the Forum des Halles, Beaugrenelle, Rosny 2, Créteil Soleil, the 4 Temps, and Printemps Haussman.

The number of interconnected cameras is also due to certain municipalities in the inner suburbs—Seine-Saint-Denis, Val-de-Marne and Hauts-de-Seine—sending along their footage to Paris police department's PVPP to be used operationally by the "agglomeration police".[7] But it is not known which municipalities made the choice to participate. This is different from integrating cameras, as the footage is all centralized in the Parisian command centers but it is not clear whether, conversely, the suburban USCs have access to footage from Paris.

[7]Since 2009, the Paris police department has had this authority over the cops of the near suburbs within the framework of "the Greater Paris Area."

In 2013, as part of the PVPP, more than 4,600 officers were trained to watch footage. This number has increased, notably since 2019, when several police officers, soldiers from the fire service, military employees who work in the information and command rooms of the police department as part of the national anti-terrorism plan, as well as the police, customs enforcement, and the gendarmerie all started getting access to footage and recordings depending on what was going on. Starting in 2022, footage from cameras in Paris could be watched by municipal employees in certain circumstances (to protect buildings, regulate traffic, or carry out traffic enforcement).

To watch all of these cameras, there are 427 operator positions covering 50 video walls across 85 processing sites, including command posts installed in each of the twenty district police departments in the capital. The footage is available 24 hours a day, seven days a week.

As for the network controlled by the bus and metro company, there are nearly 20,000 video cameras on buses and streetcars and about 10,000 in the metro and the regional train lines, and these can be consulted in real time at the company's security command posts (established in 1995) and by the police. The footage is saved for 72 hours and can be accessed in this time only upon request from the prosecutor's office. It is possible that the choice to keep footage for less time than the legal limit is due to infrastructural limitations for storing the data from a very large number of cameras. But the company's agents who watch the footage can decide when it is relevant to keep footage longer, storing it for the legal maximum of 30 days.

Also, the new generation of subway cars and trains are equipped with video equipment. Footage is saved on a hard drive and can also be watched, depending on the equipment, by the conductor.

At the national train company (SNCF), the use and storage of footage is similar to what we just described. There is a national security command post and five footage processing centers in Île-de-France.

In July 2022, a USC that deals specifically with public transit in Île-de-France was launched—the center for operational security coordination (CCOS). Its goal is to coordinate the activity of the various transportation companies' security services and of the government by relying on the

125,000 cameras in their “France Mobilités” network. A 1,000-square-meter office was set up on the “Île de la cité” in the heart of Paris, inside the Paris police headquarters, and it is active twenty-four hours a day, seven days a week. The CCOS brings together the regional transportation police's subdirectorate, the national gendarmerie, and the transit companies' internal security services (the SNCF's SUGE and the RATP's GPSR) in coordination with all the divisions of the police department.

Dodging and sabotaging cameras

When the State seeks to extend its control, to position its eyes everywhere, there are many people who would rather avoid them. Sometimes this is out of opposition to video surveillance itself, but more often it is to continue with illegal activities.

Despite the breadth of the net, there are still blind spots. The collaborative mapmaking site OpenStreetMap[8] has an option to display cameras on public streets that have been tagged by users. However, it is almost impossible to never cross the automated gaze of the police. In light of this, there are two things at play: not being recognizable and not being trackable.

Tricking the camera is a matter of timing, clothing, body shape:

- Get changed in a blind spot then come out in a different outfit some twenty minutes later.
- Wear a ball cap, a COVID mask, sunglasses, and oversized, shapeless clothes and carry an umbrella.
- Pass through areas with multiple exits, change up your method of transportation, take illogical routes.

To resist surveillance, we logically end up asking how to render cameras ineffective. Here are a few sabotage techniques that we've seen in recent years. Evidently, this is neither objective nor exhaustive, and trying it for yourself leaves room for experimentation!

Attacking cameras

Obstructing

On August 20, 2020, in Portland, USA, during one of many anti-racist and anti-police demonstrations, the building of the U.S. Immigration and Customs

[8]https://openstreetmap.org

Enforcement (ICE, a border control agency under the U.S. Department of Homeland Security) is spray-painted, its windows smashed and two cameras obscured by cones placed on top of them.

Some people have tried wrapping them in plastic bags, sometimes using a pole and slipknot if the camera is high up.

Painting

A little bit of spray paint on the lens will often do the trick and blind the cameras long enough to act. This is very practical for cameras in bank machines or ones that are in reach in general. For less accessible cameras, there have been instances where a brush attached to a pole was used to paint a camera.

Moving

Directional cameras can often be moved on their axis such that they film a wall or the sky rather than what they were pointed at originally. Again, if they are not accessible, a broom handle might help turn them to look elsewhere.

Breaking

During the nights of August 28 to 31, 2022, 7 of the 15 cameras installed by the municipality of Torcy, in Saône-et-Loire were destroyed. Cops and the mayor speak of "groups of 2 to 6 youths" who destroyed the cameras "with a hammer and by throwing stones". The bold saboteurs even smashed the cameras at the municipal police station. The bill would amount to 50,000 euros.

A good old-fashioned hammer will often do the trick if the globe is in arms reach. Many modern models are designed to be resistant to attacks and so are made of plexiglass rather than glass. But if you are persistent, you will eventually get the job done, and if the camera holds up, often its support will break. Sometimes, their support poles are equipped with cladding covered in spikes to prevent climbing. With a bit of dexterity, it is also possible to use projectiles.

Towards 1:30 a.m., on July 27 2022, people in Nantes heards six or seven gunshots and a man with a rifle was apparently seen and a camera was destroyed.

Going after their supports

Tearing off

It is possible to loop a cable between the camera and its base, then perhaps bring the two ends together with a knot, and pull. This could be done in a demo with lots of people around, or a vehicle could be used to put more force on the cable. Often, the connection between the post and the camera will break, but it's possible the posts themselves will fall down!

Sawing

Ten video protection posts sawed this summer [2022] in Nagis, the bill amounts to about 250,000 euros.

Battery-powered angle grinders. This technique is slow, onerous, and noisy, but devilishly effective. If the saboteurs cut the pole, then the entire structure needs to be rebuilt.

Ramming

It's just after midnight on the night of January 8 to 9, 2022, when the police are called to intervene in the Gabelle district of Fréjus. There, individuals are using a small mechanical excavator to smash a video surveillance camera installed in front of residential buildings. Others try to cover the lens with paint by shooting paintballs at it. They also try to set fire to the excavator and a scooter.

Slamming into the pole with construction equipment or any vehicle means the vehicle can then be set on fire at the foot of the pole if the ramming didn't work. Urban planners typically install barriers and other obtsacles to avoid this kind of attack.

Sabotaging their power supply and data cables

There is quite often a hatch in the pole at human height. Sometimes it is raised, so you need to find a garbage can or some sort of ladder to reach it. The hatches are about 30 centimeters by 10 and, depending on the model, can be opened with a size 5 or 6 Allen wrench or a triangular electrician's key (which can sometimes be replaced by a socket wrench, generally a size 10). If the lock seems too complicated, the latch is often not very strong, and so, using a flathead screwdriver and a crowbar, it might be possible to bend it or force it to turn. It is commonly the case that the hatch is welded shut or even nonexistent on certain models. For those, you will need to find the closest hatch in the ground. Often, in the city, the trenches in the pavement that the cables run through are visible, so it's easy enough to follow them and open the plate on the ground. Sometimes, they lay concrete slabs overtop to make them harder to open.

Cutting

Sharp bolt cutters will be able to cut the cables. You will need cutters with plastic handles no matter what, and the longer the arms, the safer you are. It is even better to use insulating gloves! To reduce the risk of electrical arcs, the power can sometimes be cut off by turning off a breaker inside the same hatch. Cutting a cable while electricity is flowing through it will make a muffled noise and a flash that can temporarily blind you. It is possible that power will be cut to the whole street. Cutting it flush at the top and bottom makes it more difficult to reconnect, especially if you also cut the fibre-optic cable, if that is the method of transmission being used. It is a thinner cable that is not rigid and is made of dozens of microscopic threads that a technician will have to reconnect one by one, or else pull through a new cable. In addition, cutting the fibre-optic cable doesn't make an electrical arc or any noise.

Burning

An action claim published on the Internet tells us that during the night of October 17 to 18, 2022, 8 cameras were destroyed by fire as part of a coordinated action in the center of Marseille.

On the night of July 22 to 23, 2022, in Chatellerault, two cameras were damaged by garbage can fires at the base of the post supporting them.

On April 23 2022, in Roubaix, at around 2 a.m., the municipal police on duty witnessed a rather incredible scene. On their screens, they saw a drone with a "burning rope" attached flying around a camera in an attempt to destroy it.*

Opening the hatch in the pole and inserting a flammable object is a rather effective technique, since the pole acts as a chimney. You need to leave the hatch open so air can get in to avoid smothering the fire.

Burning garbage cans under the camera can also sufficiently weaken the pole while causing enough smoke so that the camera can't see.

When the hatch is in the ground, if it is not full of water, the same technique can be used. The goal is to have the rubber sheaths catch fire by using, for instance, fabric covered in fuel.

Following the cables

Limoges, on the night of September 9 to 10, 2022. At around 1:15 a.m., one of several individuals allegedly set fire to underground cables by lifting up plates on the pavement and to electrical boxes of buildings, near Manet street. This arson disrupted the traffic lights and, in particular, rendered the local video protection cameras unusable, which was probably the aim of the operation.

It is possible to find the switches for the street lights in a neighbourhood, which often share an electrical terminal. This has the benefit of keeping you out of view of the target camera while plunging the area into darkness, as a bonus. If, by misfortune, the electrical circuit is not the same, the lack of lighting still makes it harder for the cameras to see.

Depending on the city, the footage is centralized in a USC. Starting from a camera's data cable and following it back, or starting from the USC and looking for a hatch where the data from all the cameras in the city converges is one idea. Often, there is a dedicated network, which is sometimes even written on tags around the cables. This is not always very clear, but it can be deduced. In the worst case, the area is liberated from the alienation of the Internet, and with it of remote work and digital payment, as a bonus!

Looking elsewhere

On May 23, 2021, in Saint-Denis (a suburb of Paris), Nathalie Voralek, the city's deputy in charge of security and public safety, discovers that the windshield of her car has been smashed. It wasn't the first act of vandalism, as the elected official has also had the tires of her car slashed. A dedication that is not random according to her. This new damage comes just two days after the official opening of the city's new Urban Surveillance Center (USC) and its 93 cameras.

Some might also choose to look even further upstream by sabotaging the installation process before the cameras are operational, seeking out the companies that install them and attacking their supplies, visiting the elected officials who finance video surveillance and make the decision to spy on us…

Mapping

Although the collaborative mapping site OpenStreetMap (OSM) allows users to map many things, including cameras, cameras are not always visible on the base map. That's why we have to go through sites that extract the data from OSM to show all the cameras on a new, separate map.

"Surveillance under surveillance"[9] is one such site. Every hour, it automatically extracts data on cameras around the world that are referenced in OSM. By zooming in on an area we can see the exact location of the identified cameras. Of course, the data comes from observations in the field, and some areas may be well documented while others are not. So the absence of cameras on the map doesn't mean that there are no cameras in reality. But it still gives an idea, especially since at the time of writing this zine in 2023, several thousand cameras in the Paris area have been reported by a large number of people. It is also possible to print camera maps, for example with MapOSMatic.[10]

So how can you contribute to this collaborative map? There are smartphone apps like Vespucci that allow you to map directly on your phone, but it's also very easy to take precise note of cameras on a paper map before recording them later on a computer, using Tor[11] and an anonymous OSM account.

You will need to create a dedicated OSM account. There are small tutorials to get you started with mapping, and especially with adding cameras. But basically, you can add a camera by zooming in on the appropriate area on your preferred background map (satellite image or standard

[9]https://sunders.uber.space
[10]https://print.get-map.org
[11]https://torproject.org

map). Then click on “Edit”, click on “Point” and click on the map to add a point at the exact location of the camera. A window will appear allowing you to fill in the attributes of the point, in this case you must select “Surveillance camera”. It's then possible to add more information such as the type of camera, its orientation, or whether it's a city or private camera. But even without all these details it is useful to reference a camera. Once you have referenced one or more cameras, taking care not to change the rest of the map, you need to save your changes. A new window will open, allowing you to add an optional comment and review your changes to make sure you didn't make a mistake. Click on “Upload” and that's it, your submission is sent to OSM. Soon it will appear on “Surveillance under surveillance”. Well done!

Knowing where the cameras are, how they work, how the footage is transmitted and viewed, and how these technologies are evolving is a way of concretely giving ourselves the means to go after video surveillance and the interests they protect.

No Trace Project / No trace, no case. A collection of tools to help anarchists and other rebels **understand** the capabilities of their enemies, **undermine** surveillance efforts, and ultimately **act** without getting caught.

Depending on your context, possession of certain documents may be criminalized or attract unwanted attention. Be careful about what zines you print and where you store them.