ICNL

www.icnl.org
info@icnl.org

US Program Briefer

Protesting in an Age of Government Surveillance:

Legal Reforms to Protect Demonstrators

From women's suffrage to the civil rights movement, nonviolent protests have long been vital to bringing positive social change to the United States. Today though, protesters face a growing government surveillance. This briefer examines how new types of technology used by the government to surveil protests can lead to abuse and deter demonstrators from exercising their First Amendment rights. It then outlines how both courts and lawmakers can respond to this threat.[1]

Consider these examples in recent years that highlight the dangers of unchecked surveillance against protesters:

- Phoenix police used surveillance cameras, license plate readers, and drones to track leaders of a peaceful Black Lives Matter protest for hours, waiting for them to engage in any conduct that could provide a pretext to arrest them, such as stepping off the sidewalk onto a roadway during a demonstration.
- New York police used facial recognition software to track a protester to his home, where dozens of officers attempted to forcibly enter without a warrant because he allegedly loudly shouted into a bullhorn at an officer during a demonstration.
- President Trump's Acting Under Secretary of Intelligence and Analysis at the Department of Homeland Security ordered officials to develop dossiers on protesters in Portland, Oregon, that labeled arrested protesters "violent antifa

[1] This briefer examines the use of government surveillance at protests. It does not address the unique challenges raised by government surveillance of activists and protesters, including on social media, in anticipation of demonstrations, including how law enforcement engages in "threat assessments" of protests. Further, it does not address the issues raised by third party surveillance of protesters, which can sometimes lead to third party intimidation and even violence.

anarchists inspired" unless proven otherwise and to disseminate these dossiers to federal and local law enforcement agencies. These dossiers drew significantly on protesters' social media profiles and other online sources.

While there are important legal safeguards against certain types of government surveillance of protesters, courts have been too slow in clarifying the scope of constitutional protections and lawmakers have often failed to enact needed legislative protections. This underdevelopment of the law creates substantial gaps and gray zones that police can use in ways that stifle protected First Amendment conduct.

The Supreme Court's seminal 2018 decision in *Carpenter v. United States* is a good example of this problem. The Court found that under the constitution, law enforcement needed a warrant to obtain a person's cell phone location information because such information can be used to track the "whole of [a person's] physical movements," creating an "intimate window" into their life, including their "familial, political, professional, religious, and sexual associations." However, law enforcement agencies have sometimes bypassed this constitutional warrant requirement by buying cell phone data from third-party providers instead of obtaining a warrant to have cell phone companies provide this data. Further, the Court has not been clear on what other types of surveillance, like license plate readers or facial recognition technology, might meet the Supreme Court's standard of such invasive monitoring by the government that its use also requires a warrant.

The stakes in creating strong safeguards are high. The government has a long history of abusing surveillance tools to intimidate and undermine activists and social movements. In the 20th century, the FBI's COINTELPRO surveilled and attempted to discredit organizations and activists it considered "subversive," including Martin Luther King Jr. After 9/11, the federal government and local law enforcement surveilled and infiltrated Muslim American organizations, leading to unfounded law enforcement investigations and a climate of distrust and fear. More recently, both the federal government and local law enforcement have engaged in systematic surveillance of Black Lives Matter demonstrators. By 2017 the FBI started a new domestic terrorism program category called the "Black identity extremist movement," and local law enforcement has recently gained access to powerful new surveillance capabilities that they have repeatedly used to target Black Lives Matter and other demonstrators.

The use of government surveillance to target protesters can deter Americans from participating in their First Amendment right to peacefully participate in demonstrations as they fear the government may identify and track them at a protest and then use this chronicling of their activity against them in the future. Such targeting may include harassment through unfounded or selective investigations or releasing

their information to the public, creating the potential for third-party intimidation and violence.

Despite the diverse technologies covered in this briefer, they raise similar principles for regulation. Policymakers should ensure transparency in the use of surveillance technologies and create strict limits, such as warrant requirements or partial bans, on certain types of expansive or particularly intrusive surveillance technologies. They should also ensure that government does not use surveillance technologies to identify or investigate the actions of individual protesters engaged in First Amendment protected activity unless there is individualized, fact-based suspicion of wrong-doing.

Strong safeguards must be in place to check the use of government surveillance in all contexts. However, the potential for inappropriate and potentially politicized government surveillance during expressive activity like protests highlights some of the greatest dangers posed by government surveillance and should spur courts and policymakers to be vigilant and proactive against this threat.

Surveillance Methods

There is a broad set of surveillance technologies that law enforcement can use to track and identify demonstrators. While police have always engaged in the surveillance of protesters, new technologies significantly lessen the cost of doing so and increase the capabilities of law enforcement to track and identify individual demonstrators.

This section discusses dangers created by: (1) the proliferation of cameras to record protesters, including from drones; (2) the use of facial recognition technology to identify specific demonstrators; (3) the use of license plate readers to identify and track protesters; (4) access to geolocation data from cell phones to identify and track the movements of protesters; and (5) tracking of protesters using cell-site simulators. Once protesters are identified, technology allows law enforcement to build extensive dossiers on demonstrators, including by accessing their social media profiles, and to share these dossiers across law enforcement agencies, often tarring specific protesters with unfounded suspicion. Taken in part or together, these types of surveillance can be so invasive as to intimidate and deter people from exercising their first amendment right to peaceful assembly.

THE PROLIFERATION OF CAMERAS

With the ubiquity of cameras in U.S. cities and towns, protesters today are frequently being recorded at some point during a demonstration. Public CCTV cameras have been set up to surveil streets, sidewalks, and public squares, and law enforcement often can gain access to private security cameras that capture images of demonstrators. For example, in Chicago, law enforcement reportedly has real-time access, without the need for a warrant, to over 30,000 public and private surveillance cameras throughout

the city. Law enforcement will also often explicitly record protests, including through police body cameras, and frequently searches social media feeds and other websites for photos and recordings of protests taken by protesters themselves, media, or other observers.

Most people who attend a demonstration in the U.S. today likely assume a camera may record them in some manner. However, how they are recorded and whether the government uses this recording to specifically identify them significantly affects whether they feel their privacy is being violated or that these recordings may be used against them in the future, potentially deterring them from attending a demonstration.

For example, high-definition cameras have been attached to aircraft to monitor and track protesters. It was reported that the Department of Homeland Security deployed drones, planes, and helicopters to surveil protesters in at least 15 cities during the 2020 George Floyd protests, including using a predator drone in Minneapolis, MN. Meanwhile, the FBI used a sophisticated spy plane to monitor demonstrators during the 2015 and 2020 Black Lives Matter protests. In California, the state's highway patrol conducted aerial surveillance of George Floyd protests in at least 25 cities, recording images that could sometimes be used to identify protesters' faces or their signs. The ACLU's Jay Stanley noted the intimidating effects on protesters, stating, "There is something militaristic and dominating about a militarized police aircraft hovering over you when you're out there protesting police abuse."

Images or video feeds taken by the police of protesters can also be shared with the public, potentially endangering protesters. For example, in July 2020, the Police Department in Portland, OR, live streamed demonstrations on YouTube and Twitter, zooming in on many peaceful protesters' faces, allowing the public to identify them. Other cities have also released footage of clearly visible peaceful demonstrators, often claiming it was necessary to provide context for law enforcement action. However, this footage often shows nonviolent demonstrators and can be used by third parties to identify and harass people exercising their First Amendment rights.

FACIAL RECOGNITION TECHNOLOGY

Facial recognition technology allows law enforcement and others to compare recorded images of protesters to extensive databases of individuals to identify specific demonstrators. There has been concerning use of this technology. For example, as mentioned in the introduction, in 2020, New York police used facial recognition software to track an activist to his home, where dozens of officers attempted to forcibly enter without a warrant because he allegedly shouted loudly into a bullhorn at an officer during a demonstration. Police in Florida in 2020 used facial recognition to identify Black Lives Matter protesters, including protest organizers, despite no suspicion of wrongdoing as part of gathering "intelligence." In 2016, the Baltimore police

department contracted with a company that monitored social media feeds connected with the Freddie Gray protests. They ran protesters' faces through facial recognition software to identify demonstrators with outstanding warrants to alert police to arrest them.

The prospect of having oneself identified for simply attending a demonstration can be intimidating and deter participation. Further, the use of facial recognition technology by law enforcement can frequently lead to misidentification, particularly when used on images of people of color or where images are unclear.

In response to concerns about the potential for abuse of facial recognition technology, many states and cities have taken steps to ban or restrict the technology. As of 2022, over a dozen states have laws restricting the use of facial recognition software, including what crimes it can be used to investigate. Meanwhile, over fifteen cities, including San Francisco, Boston, and Portland, OR, have significantly restricted government use of facial recognition software by law enforcement.

That said, legislative restrictions on facial recognition technology are inconsistent and only present in a minority of jurisdictions. Further, some officers have circumvented restrictions that are in place, including using their personal devices to access Clearview AI. This service matches a picture of a face to an extensive database of billions of images from the internet.

LICENSE PLATE READERS

Law enforcement can use license plate readers to track and frequently identify protesters. These devices, which use cameras and computer software to scan every vehicle's license plate that passes in front of them, have become ubiquitous in U.S. cities. For example, according to a 2020 California state auditor report, the Los Angeles Police Department alone has accumulated over 320 million license plate scans.

Law enforcement can use recorded images or other surveillance to track protesters back to their vehicles and identify the license plate and who the vehicle is registered to when it passes a license plate reader. The International Association of Chiefs of Police has observed that license plate readers can cause people to "become more cautious in the exercise of their protected rights of expression, protest, association, and political participation because they consider themselves under constant surveillance." During a 2020 Black Lives Matter demonstration in Arizona, law enforcement used license plate readers to help identify protesters. They then labeled them as "targets" and tracked them during the protest in an attempt to catch them engaging in even a minor infraction of the law, like stepping into the street in a manner that could be interpreted as blocking traffic.

GEOLOCATION DATA

Protesters' cell phones transmit geolocation data that can be used by law enforcement to track protesters back to their homes, workplaces, or other locations to identify them. For example, in 2019, the *NY Times* used a geolocation data file it obtained from a private company to track a senior Pentagon official and his wife from the 2017 Women's march back to their home in Virginia to demonstrate how easily this data can be used to identify individual protesters. Similarly, after protests against COVID-19 restrictions in Michigan in 2020, a group supportive of COVID-19 restrictions bought and publicized cell phone data from the demonstrations to be able to track participants to their hometowns to claim that the protests were super-spreading events.

In *Carpenter v. United States*, the Supreme Court in 2018 banned the government from obtaining cell phone information from private cell phone carriers without a warrant. However, the government has effectively bypassed this ruling, interpreting it only to limit the government from compelling cell phone companies to provide this data and not limiting the government from purchasing cell phone data from private companies.

When the government has issued warrants for cell phone data, it has sometimes done so through the controversial practice of geofence warrants. For example, in Minneapolis, after a vandal damaged the windows of an auto parts store during the George Floyd protests in May 2020, the police issued a warrant that compelled Google to provide account data of anyone who was "within the geographical region" at the time. This request included peaceful protesters who were in the area for the demonstration. While the data provided by Google under these warrants are initially anonymized, law enforcement can then ask Google de-anonymize particular devices that it finds suspect. Several federal and state courts have recently found that this type of blanket request for information violates the Fourth Amendment. The use of geofence warrants has skyrocketed in recent years, with Google receiving about 11,500 geofence warrants in 2020 alone, increasing the likelihood of their use in the First Amendment context.

CELL SITE SIMULATORS

Cell-site simulators, or stingrays, mimic cell phone towers and trick cell phones into connecting with them. They can identify cell phones in a given area, intercept metadata such as the numbers and duration of calls, and track text messages and internet usage. In addition, they can target the cell phone of a specific individual or, in dragnet style, track all cell phones in the surrounding area.

One of the first police departments to purchase cell-site simulators was the Miami-Dade Police Department, which acquired them to monitor protests at the 2003 summit on the Free Trade Area of the Americas. There is also more recent circumstantial evidence that other law enforcement agencies have used cell-site simulators to track protesters in cities like New York, Chicago, and Baltimore. The ability of law

enforcement agencies to use cell-site simulators and similar technology to track protesters has caused civil liberties groups to recommend protesters turn off their cell phones at a demonstration. It may also deter some individuals from even participating in demonstrations if they worry that they may be inappropriately caught up in a police dragnet if a handful of demonstrators engage in illegal behavior or if police conduct an overly aggressive investigation.

While the U.S. Supreme Court has not yet issued a ruling directly related to the use of cell site simulators, several courts have ruled that their use constitutes a search under the Fourth Amendment and requires a warrant, including federal district courts in New York and California, as well as courts in Maryland and Washington DC. Several states, including California, Washington, Virginia, Utah, and Illinois, have enacted legislation requiring law enforcement to obtain a warrant before using a cell site simulator. That said, the legal framework for using stingrays is still geographically patchy and confusing, meaning some law enforcement agencies may be using cell-site simulators to surveil protesters without a warrant.

BUILDING DOSSIERS AND SHARING INFORMATION

It is not just surveillance through new technologies that present challenges for protesters' rights, but the ability of law enforcement to identify individuals, build dossiers, and exchange this information within and across law enforcement agencies, frequently creating unjustified suspicion towards demonstrators.

Consider Memphis, Tennessee. After a group of nonviolent activists protested in front of the mayor's residence in 2016, protesters were reportedly added to a "blacklist" of people who could not enter city hall without a police escort. In 2021, it came to light through a public records request that the Tennessee Department of Safety and Homeland Security was maintaining dossiers on over 50 activists who had participated in Black Lives Matter protests in Memphis in 2020, including a journalist and those who had never been arrested for any infraction. This information included names, addresses, social media pictures, familial relations, and even the identity of some of the activists' romantic partners.

In response to these and other surveillance concerns, a judge granted the ACLU a modified consent decree in 2021 that allowed the Memphis police department to attend protests with surveillance equipment, like body cameras. However, the decree barred the police from using the equipment to gather intelligence on First Amendment activity unless it was collected in the course of a lawful criminal investigation. The decree also required any investigation reasonably likely to involve the collection of information about the exercise of First Amendment rights must immediately be brought to the attention of the Director of Police or a designee for review and authorization. Finally,

the decree stated the police could not coordinate with any outside public or private agency to engage in conduct prohibited under the decree.

Civil liberties advocates have been particularly concerned about the federal government's role in collecting and dispersing information about protesters to federal and local law enforcement. For example, a Department of Homeland Security report released to the public in 2022 determined that during the 2020 racial justice protests in Portland, Oregon, the Department developed dossiers, or Operation Background Reports, on protesters arrested at Black Lives Matter demonstrations, including those "arrested for trivial criminal infractions having little or no connection to domestic terrorism." The information in these dossiers included "lists of friends, family, and social media associates." The acting undersecretary of intelligence and analysis at DHS called on analysts to label arrested protesters "Violent Antifa Anarchists Inspired" by default even though "specific facts" were never found "to support such a characterization." Analysts had to rebuff calls by top Trump officials to create dossiers "against everyone participating in the Portland protest," regardless of whether they had been accused of committing any crime.

Fusion centers, which act as a clearinghouse of information between local, state, and federal officials, have been frequently accused of being used to track nonviolent protesters and issue law enforcement bulletins mischaracterizing their activities. For instance, a federal fusion center was used in 2018 to investigate and disseminate information under "suspicious activity reports" on nonviolent protesters of a natural gas pipeline project in Oregon. Law enforcement reportedly built dossiers on pipeline activists that were not engaged in any criminal conduct, which included social media profiles and information provided by private security employed by the company constructing the pipeline project. Similarly, during the 2020 Black Lives Matter protests fusion centers repeatedly issued bulletins mischaracterizing nonviolent protests at threats, “often citing rumors or disinformation spread by anonymous social media posters or right-wing media sites.”

Safeguards against Government Surveillance

Government surveillance can violate privacy rights in any context. As such, many of the recommendations in this section apply to government surveillance in the U.S. of any person, not just of a protester or others exercising First Amendment protected activity. That said, surveillance during demonstrations can have particularly concerning effects, given the historical centrality of protests to U.S. democracy. This creates unique costs for U.S. democracy when surveillance chills protesters' voices. There are also unique dangers of law enforcement abuse concerning surveillance of demonstrations, as there are often greater risks of surveillance being used as part of a politicized strategy to engage in selective investigation or prosecution. In response, both the courts and

policymakers should center the risks to protesters' privacy and expressive rights as they take larger, more comprehensive, steps to restrict when and how government can engage in surveillance.

JUDICIAL PROTECTION

Even though protests generally occur in public places, that does not provide law enforcement unrestricted authority to surveil protesters. In particular, the Fourth Amendment's right against unreasonable searches and seizures protects against certain types of surveillance in public. As Chief Justice Roberts wrote for the Supreme Court in *Carpenter*, "A person does not surrender all Fourth Amendment protection by venturing into the public sphere." Specifically, in *Carpenter,* the Court found that law enforcement needed a warrant to obtain cell phone location information because such information can be used to track the "whole of [a person's] physical movements," creating an "intimate window" into a person's life, including their "familial, political, professional, religious, and sexual associations." In other words, accessing a person's cell phone location information without a warrant violated their right to privacy. Drawing on similar reasoning, in 2021, the Fourth Circuit found that the Baltimore Police Department's expansive aerial surveillance program, which could be used to "captur[e] everyone's movements outside during the daytime" in the city, violated the Fourth Amendment.

Building on this jurisprudence, courts should heed the dangers created by new technologies and be vigilant in guarding against potentially politicized government surveillance during expressive activities like protests. Today, it is far too easy to use surveillance technology to identify individual protesters and cross-reference this information with demonstrators' social media accounts or other available data to create a detailed picture of a protester. Borrowing the language of Chief Justice Roberts in *Carpenter*, this creates an "intimate window" into a protesters' life that violates Fourth Amendment protections. It also chills First Amendment activity as protesters become fearful of potential retaliatory actions by the government.

While the Supreme Court already requires a warrant for law enforcement to access cell phone geolocation data, civil liberties groups and academics have called on courts to require law enforcement to receive a warrant before using similar technology that can identify specific individuals and track their movements, such as facial recognition technology, historical data recorded by license plate readers, or cell site simulators. Importantly, scholars and activists have argued that courts should not allow law enforcement to bypass warrant requirements by purchasing or receiving this type of surveillance data from third-party companies. Instead, courts should make clear that a warrant is required for law enforcement to gain access to this information from any source.

Finally, advocates have argued that courts should require that law enforcement not release images to the public of demonstrators that can be used to identify them when those demonstrators are not engaged in unlawful conduct. If it is necessary to release footage, law enforcement should blur out the identities of nonviolent protesters. Otherwise, such video releases can create a chilling environment for First Amendment rights in which protesters may fear third-party violence, doxing, or other types of harm from members of the public who hold competing views.

LEGISLATIVE SAFEGUARDS

Courts should enforce strong safeguards to protect protesters' rights, but legislators also should enact measures to protect demonstrators and others from the potentially chilling impact of surveillance. Given broader concerns about government surveillance, many of these interventions will restrict government surveillance in any context, not just against protesters. Examples of these types of interventions include:

- **Transparency.** Many localities have enacted Community Control Over Police Surveillance (CCOPS) laws. The provisions of this legislation vary but generally include transparency requirements for the procurement of new surveillance technology by local law enforcement; a community advisory committee to create standards for procurement; reports on the technologies' anticipated impact; and ongoing reporting requirements on the use of this technology. For example, New York City enacted legislation that requires the police department to issue an impact and use report for surveillance technologies that is open for public comment. Additionally, the use of the technologies is periodically audited.
- **Restrictions on investigating protesters**. The practice of law enforcement compiling lists of protesters, or creating dossiers on protesters, can easily be used to target demonstrators with views unpopular to the government or law enforcement. Washington, D.C. has enacted legislation restricting police investigations of individuals engaged in First Amendment protected activity. For an investigation involving First Amendment activity, there must be reasonable suspicion of criminal conduct, a commanding officer must grant approval, and the investigations are time-limited unless reauthorized by the Chief of Police. Similarly, Oregon bans investigations of First Amendment protected activity unless it is directly related to a criminal investigation.
- **Restrict or ban the use of facial recognition technology**. Jurisdictions have taken a variety of steps to restrict facial recognition technology. Some cities, such as San Francisco and Oakland, have altogether prohibited facial recognition technology used by the government, and Vermont has enacted a near moratorium. Massachusetts enacted legislation prohibiting government

agencies from using facial recognition technology without a warrant. Some law enforcement agencies, such as Miami's police department, ban the use of facial recognition software during constitutionally protected activities, such as protests. Federal legislation has been introduced but not yet enacted. The proposed Facial Recognition and Biotechnology Moratorium Act would ban the federal government from using facial recognition technology unless explicitly authorized to do so by an act of Congress. Meanwhile, the proposed Facial Recognition Act would ban the use of facial recognition technology by law enforcement without a warrant and allow it only to be used if there were probable cause an individual committed a violent felony. It would also prohibit law enforcement from using this technology to create a record documenting protected First Amendment expression or activity, like a protest.

- **Ban accessing geolocation data without a warrant**. The proposed 4th Amendment is Not for Sale Act would require the government to obtain a court order to compel data brokers to disclose data, such as geolocation data of cell phone users. It also bans law enforcement from buying data on people in the U.S. if it was obtained from a user's account or device, such as a cell phone. Meanwhile, lawmakers in New York have introduced legislation that would ban law enforcement from using geofence warrants altogether.
- **Ban the use of historical license plate reader data without a warrant.** Civil liberties groups have advocated that law enforcement first acquire a warrant to search through historical license plate reader data.
- **Ban the use of cell site simulators without a warrant.** The proposed Cell Site Simulator Warrant Act would create a warrant requirement for federal, state, and local law enforcement to use a cell-site simulator. However, it does allow for emergency use of sting rays, requiring in those cases that law enforcement only go to court after the fact.
- **Restrict the use of drones and other aircraft for surveillance of protests**. Over fifteen states require law enforcement to obtain a warrant before using a drone for surveillance. For example, Vermont's legislation explicitly bars law enforcement agencies from using drones to "gather or retain information on private citizens peacefully exercising their constitutional rights of free speech and assembly." In addition, civil liberties groups have called for a ban on generalized aerial surveillance.

Conclusion

Courts and policymakers must address the dangers created by the use of new and evolving surveillance technologies. These dangers have multiplied as surveillance

technologies have become cheaper and more sophisticated, allowing governments much more capability to track and identify demonstrators. Moreover, once protesters are identified law enforcement can develop extensive dossiers on protesters using social media and other online resources, including through automated analysis tools that link databases of information together to create even more intrusive profiles of demonstrators.

Americans need confidence that if they simply attend a demonstration that they will not be identified by the government or have that information used against them in the future. Having a robust legal framework for government surveillance can help build this confidence. Sensible limits on the government's surveillance powers, like those proposed in this briefer, will help protect protesters' ability to continue exercising their constitutional right to have their voice heard without the fear of intimidation or harassment.

Additional Resources

There are a number of organizations that work on analyzing and reforming laws governing government surveillance in the United States. These include the following, many of whose resources were hyperlinked and relied upon in this report:

- American Civil Liberties Union
- Brennan Center for Justice
- Center for Democracy and Technology
- Defending Rights & Dissent
- Demand Progress
- Electronic Frontier Foundation
- Electronic Privacy Information Center
- Fight for the Future
- Georgetown Law Center on Privacy and Technology
- Project on Government Oversight
- Surveillance Technology Oversight Project (S.T.O.P.)

For more information contact Nick Robinson at nrobinson@icnl.org