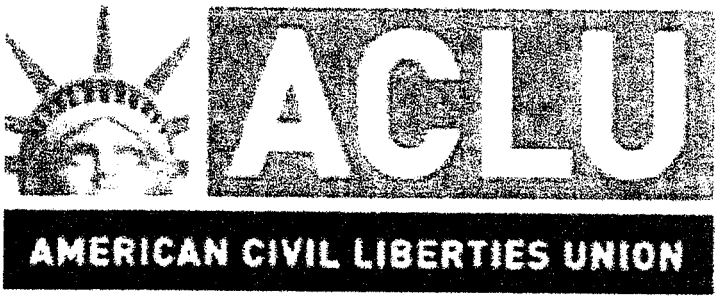

Statement of Catherine Crump, Staff Attorney

American Civil Liberties Union

On

Government Use of Surveillance Technologies and the Balance of Law Enforcement Purposes with Individual Rights of Privacy

Before the House of Representatives Committee on Civil Law

January 28, 2014

Thank you for the opportunity to testify on behalf of the American Civil Liberties Union and the ACLU of Minnesota. The ACLU has 8,500 members in Minnesota and more than half a million members nationwide, as well as countless additional activists and supporters. Our mission is to defend civil rights and liberties under the United States and Minnesota constitutions.

Today more than ever before, the American people are both aware of the powerful new surveillance technologies available to law enforcement agencies and concerned about how these technologies are being used. While the National Security Agency's mass collection of Americans' phone call records is the most prominent example, it is not just the federal intelligence agencies that are taking advantage of these new tools.

In fact, the most significant impact of new surveillance technologies is taking place at the state and local levels. New surveillance technologies make it possible for state and local law enforcement agencies to engage in surveillance that used to be prohibitively expensive. Tracking the movements of a single vehicle around the clock used to require teams of agents. Now it can be done through installation of a single GPS device. Recording the movements of vehicles on a mass scale used to be a technological impossibility, but through the use of automatic license plate readers law enforcement agents can record all passing vehicles and retain those records for months or even years.

Let there be no mistake: the ACLU is not against the use of advanced technologies in policing. The work of our law enforcement agents is important and we all have an interest in it being done effectively. However, many new surveillance technologies reveal sensitive private information about individuals. Others cast wide dragnets that capture information about hundreds or thousands of innocent people to identify a single criminal suspect. New legislation is necessary to ensure that Americans' privacy rights are adequately protected.

There are many novel surveillance technologies we could discuss, but today I will focus on four powerful technologies that enable law enforcement agents to monitor and record our movements to an unprecedented degree. These technologies are GPS tracking, cell phone tracking, automatic license plate readers, and drones. Together, they provide law enforcement agents with powerful and inexpensive methods of tracking individuals over an extensive period of time and an unlimited expanse of space as they traverse public and private areas. People can be tracked for days, weeks, or even months at a time with little difficulty or expense. While some tracking technologies target specific individuals, others make it possible to engage in the mass surveillance of Americans' movements. While each technology raises the prospect of significant invasions of Americans' privacy, the good news is that legislative fixes are possible that would both allow legitimate uses of these technologies to go forward, and ensure that Americans' privacy is not needlessly diminished.

I. Tracking People's Movements Invades Their Privacy Because It Reveals A Great Deal About Them.

Where a person chooses to travel reveals sensitive, private information. By watching someone's movements, it can be possible to learn the identity of his friends, what medical practitioners he visits, where he chooses to worship, and how he chooses to spend his time. As U.S. Supreme Court Justice Sonya Sotomayor wrote in a case involving GPS tracking, location tracking can reveal "trips to the psychiatrist, the plastic surgeon, the abortion clinic, the AIDS treatment center, the strip club, the criminal defense attorney, the by-the-hour motel, the union meeting, the mosque, synagogue or church, the gay bar and on and on."[1] And tracking someone's movements for a prolonged period of time makes it possible to uncover not just one such fact but all such facts. It can reveal the routines of a person's daily life—and every deviation from that routine.

While law enforcement agents have always been able to monitor a person's location by following him down a street or tailing his car, today's location tracking technologies are vastly more powerful than such primitive methods. People's movements can be logged for weeks, months or even years at a time with little difficulty or expense. While some tracking technologies target specific individuals, others make it possible to engage in the mass surveillance of people's movements in a town or city.

There have always been facets of American life that have been uniquely safeguarded from the intrusive interference and observation of government. Location tracking threatens to make even those aspects of life an open book to government. To quote Justice Sotomayor once more, "awareness that the Government may be watching chills associational and expressive freedoms. And the Government's unrestrained power to assemble data that reveal private aspects of identity is susceptible to abuse."[2]

The Supreme Court has just begun to address the extent to which technologically enhanced location tracking is covered by the Fourth Amendment's prohibition against unreasonable searches and seizures. In *United States v. Jones*, the Supreme Court held that a Fourth Amendment search occurred when the government placed a GPS tracking device on the defendant's car and monitored his whereabouts nonstop for 28 days.[3] A majority of the Justices also stated that "the use of longer term GPS monitoring . . . impinges on expectations of privacy" in the location data downloaded from that tracker.[4] As Justice Alito explained, "[s]ociety's expectation has been that law enforcement agents and others would not -- and indeed, in the main, simply could not -- secretly monitor and catalog every single movement of an individual's car, for a very long period."[5]

---

[1] *United States v. Jones*, 132 S. Ct. 949, 955 (2012) (quoting *People v. Weaver*, 12 N.Y.3d 433, 442 (N.Y. 2009)).
[2] *Id.* at 956 (Sotomayor, J., concurring) (quotations omitted).
[3] *Id. at* 954.
[4] *Id.* at 953-64 (Sotomayor, J., concurring); *see also id.* at 964 (Alito, J., concurring).
[5] *Id.* at 964 (Alito, J., concurring).

Unfortunately, the Supreme Court's decision leaves two key questions unresolved. While it concluded that attachment of a GPS device to a car to gather information about its movements is a "search," it did not resolve whether it is the type of search that requires a warrant based upon probable cause. Also, the case dealt with attachment of GPS devices to vehicles only, leaving for another day how it applies to other technologies such as cell phones, license plate readers and drones.

Given the serious privacy implications of these technologies, this body should not wait for the courts to sort it out, a process which will surely take many years. Instead, this body should act now to establish rules to protect citizens' privacy while allowing legitimate law enforcement uses of new technologies to go forward.

II. Today's Powerful Location-Tracking Technologies

Recent technological developments make it possible to obtain location information about Americans with great precision, in both real time and historically. While the technical details and exact capabilities of these new technologies vary, all confer unprecedented power on law enforcement agents to track Americans' movements.

A. GPS Tracking

Most Americans now understand that law enforcement agents can track their vehicles through GPS. As discussed above, in *United States v. Jones,* law enforcement agents installed a GPS device on a vehicle and it remained there for 28 days. During this period, the GPS device allowed agents to track the location of the car at every moment. It had an antenna that received signals from satellites; the device used these signals to determine its latitude and longitude every ten seconds, accurately pinpointing its location to within 50-100 feet. Law enforcement agents connected that data to software that plotted the car's location and movements on a map. The software also created a comprehensive record of the car's locations. The detailed picture of a person's every movement this technology can generate demonstrates why legislation is needed to resolve the question of whether a full probable-cause warrant is needed for GPS tracking by putting such a requirement into law.

In addition to physically attaching a GPS device to a car, when cars have navigations systems built in, it is possible for law enforcement agents to make use of these systems to track a vehicle's movements.[6] While it appears the primary use of GPS tracking is to follow the movements of cars, such devices can also be installed on other vehicles such as boats or planes, and on other objects.

B. Cell Phone Tracking

[6] *See, e.g., United States v. Coleman*, No. 07-20357, 2008 WL 495323, at *1 (E.D. Mich. Feb. 20, 2008) (discussing issuance of court order requiring car navigation company to disclose location data to law enforcement).

Today virtually every American owns a cell phone. Cell phone technology has given law enforcement agencies an unprecedented new surveillance tool. With assistance from cell phone carriers, the government now has the technical capability to track any cell phone owner, for 24 hours a day, for as long as it likes. Through so-called "tower dumps," it can also identify all of the individuals whose cell phones used a particular tower—allowing law enforcement agents to infer who was present at a location days, weeks or months after the fact. There is even technology available that allows the government to locate a cell phone without any phone company involvement.

Cell phones yield several types of information about their users' past and present locations: cell site location data, triangulation data, and Global Positioning System data. The most basic type of mobile phone location information is "cell site" data or "cell site location information," which refer to the identity of the cell tower from which the phone is connected and the sector of the tower facing the phone. This data is generated because whenever individuals have their cell phones on, the phones automatically and frequently scan for nearby cell towers that provide the best reception. The carriers keep track of the registration information to identify the cell tower through which calls can be made and received.

In addition to cell site information, law enforcement agents can obtain location data at a higher level of accuracy by requesting cell phone providers to engage in "triangulation," which entails collecting and analyzing data of the precise time and angle at which the cell phone's signal arrives at multiple cell towers. Current technology can pinpoint the location of a cell phone to an accuracy of within 50 meters or less anytime the phone is on. Also, a cell phone that has GPS receiver hardware built into it can determine its precise location by receiving signals from global positioning satellites. Current GPS technology can pinpoint location when it is outdoors, typically achieving accuracy of within 10 meters.

Law enforcement agencies can request historical data, which can be used to retrace previous movements, or prospective data, which can be used to track the phone in real time. The availability of historical information and the length of time this information is stored depend on the policies of the cell phone company. According to a U.S. Department of Justice document, Verizon stores the cell towers used by a mobile phone for "one rolling year"; T-Mobile keeps this information "officially 4-6 months, really a year or more"; Sprint and Nextel store this data for "18-24 months"; and AT&T/Cingular retains it "from July 2008."[7]

Law enforcement agencies can obtain data regarding the movements of one or more persons over time, or they can obtain data regarding all of the people whose phones were using a particular tower at a particular time. This latter method of obtaining cell site location information is often referred to as a "tower dump." Because tower dumps obtain

[7] U.S. Department of Justice, *Retention Periods of Major Cellular Service Providers*, available at https://www.aclu.org/cell-phone-location-tracking-request-response-cell-phone-company-data-retention-chart

the information of everyone whose phone was using a particular cell phone tower, by their nature they sweep in vast quantities of data about innocent people who will never know that their location data was shared with the government.

In addition to obtaining cell location information through mobile carriers, there are devices on the market that allow law enforcement agents to obtain certain information without any carrier assistance. In fact, recent media reports and inquiries by members of this body show that Minnesota law enforcement agencies own at least two such devices. "Stingray" is the name for the Harris Corporation's line of "cell site simulator" devices, also called "IMSI catchers," in reference to the unique identifier – or international mobile subscriber identity – of wireless devices. An IMSI catcher masquerades as a cell tower, prompting wireless devices to communicate with it. Stingrays are commonly used in two ways: to collect unique numeric identifiers associated with phones in a given location or to ascertain the location of a phone when the officers know the numbers associated with it but don't know precisely where it is.

Both of these uses pose special privacy challenges. Collecting unique identifiers of all phones in a particular location inherently collects location data on a lot of innocent people. Using an IMSI catcher to ascertain the location of a cell phone can reveal that it is in a constitutionally protected place, such as a home, that has traditionally been immune from search unless law enforcement agents obtain a warrant based on probable cause.

C. Automatic License Plate Readers

Automatic license plate readers are cameras mounted on stationary objects (telephone poles, the underside of bridges, etc.) or on patrol cars. The cameras snap a photograph of every license plate that passes them by – capturing information on up to thousands of cars per minute. The devices convert each license plate number into machine-readable text and check them against agency-selected databases or manually-entered license plate numbers, providing an alert to a patrol officer whenever a match or "hit" appears. When an automatic license plate reader system captures an image of a car, it also meta-tags each file with the GPS location and the time and date showing where and when the photograph was snapped. And often, the photograph—not just the plate number—is also stored. The system gathers this information on every car it comes in contact with, not simply those to which some flag or "hit" was attached.

When used in a narrow and carefully regulated way, automatic license plate readers can help police recover stolen cars and arrest people with outstanding warrants.

Unfortunately, automatic license plate readers are, for the most part, not being used in a narrow and carefully regulated way. The systems routinely store information on the location of innocent people. The scanning and storage capabilities of these cameras and data systems have grown exponentially since their introduction. And thanks to falling costs and the availability of federal grants, automatic license plate readers' ubiquity has also grown exponentially. Over time, these devices create a treasure trove of personal data – searchable logs tracking the movements of innocent Americans going about their

private business. This technology can be used to track the movements of people who attend a protest or political event, attend a particular church, or visit a particular doctor. In New York City, police officers have reportedly driven unmarked vehicles equipped with license plate readers around local mosques in order to record each attendee. We recently released a report detailing the use (and abuse) of license plate readers, reflecting the results of our coordinated public records requests in 38 states and Washington DC. More details on what we learned can be found in our report available at www.aclu.org/plates.

Keeping track of suspected wrongdoers is one thing, but clear regulations must be put in place to keep authorities from tracking those who have done nothing wrong. State law should prohibit automatic license plate readers from storing data where there is no match to an offender list or other evidence of wrongdoing.

D. Drones

Unmanned aircraft carrying cameras raise the prospect of a significant new avenue for the surveillance of American life. Many Americans are familiar with these aircraft, commonly called drones, because of their use overseas in places like Afghanistan, Pakistan and Yemen. But drones are coming to America. Under 2012 legislation, the Federal Aviation Administration is required to "develop a comprehensive plan to safely accelerate the integration of civil unmanned aircraft systems into the national airspace system."

This legislation has dramatically accelerated the deployment of drones and pushed this issue to the forefront. At the same time, drone technology is quickly becoming cheaper and more powerful while our privacy laws have not kept up with the technology. Aerial surveillance from manned aircraft has been with us for decades. But manned aircraft are expensive to purchase, operate and maintain, and this expense has always imposed a natural limit on the government's aerial surveillance capability. Now that surveillance can be carried out by unmanned aircraft, this natural limit is eroding.

Drones can be thought of as a location tracking technology—but they also post a whole host of other privacy risks as well. High-altitude drones raise the prospect that it will be possible to track the movements of everyone in an area the size of a medium-sized city. The PBS series NOVA, "Rise of the Drones," recently aired a segment detailing the capabilities of a powerful aerial surveillance system known as ARGUS-IS. This system, which includes a super-high, 1.8 gigapixel resolution camera mounted on a drone, demonstrates many of these capacities. The system is capable of high-resolution monitoring and recording of an entire city, including monitoring the movements of discrete vehicles. To witness a demonstration of this capacity, please see: http://www.youtube.com/watch?feature=player_embedded&v=13BahrdkMU8

But in addition to location, except for possibly the very lightest craft, drones can carry the full range of advanced surveillance technologies that have been developed—and are likely to be developed. Drones will certainly have capacity to gather more and better

information than the unaided human eye through the use of high powered zoom lens, infrared and ultraviolet imaging and perhaps even technology that allows for see-through imaging.

III. New Laws Are Needed To Put Privacy Protections In Place.

In light of the serious privacy risks posed by each of the technologies discussed above, it is important that this body enact legislation to update the law by putting privacy protections in place. The ACLU of Minnesota supports:

- For GPS and cell phone tracking, the ACLU supports legislation that requires law enforcement agents to demonstrate probable cause and obtain a warrant before using these tools (with reasonable exceptions, such as for exigent circumstances). Location information is too sensitive for law enforcement agencies to be accessing it in criminal investigations without a warrant.

- For automatic license plate readers, the ACLU supports legislation that limits the amount of time that plate data that does not generate a hit can be retained. While it is legitimate to use license plate readers to check plates against "hot lists" of cars that are stolen or associated with individuals for whom an arrest warrant has issued, data pertaining to innocent individuals should be purged as soon as possible. Also, the location of ALPR cameras should be publicly available.

- For drones, drone activity presents a serious threat to privacy from domestic surveillance and a probable cause warrant should be required prior to law enforcement drone use.

Conclusion

Thank you for the opportunity to testify today. As Justice Alito has written, "In circumstances involving dramatic technological change, the best solution to privacy concerns may be legislative." The ACLU would be delighted to work with you on legislation on any of these issues moving forward.