CBS NEWS

What is the future of privacy, surveillance and policing technologies under Trump?

Kathryn Watson

June 22, 2017

For weeks, President Trump cried foul, repeating unverified claims that the Obama administration wiretapped Trump Tower to spy on him, accusations that remain unsubstantiated.

But Mr. Trump, with the power of the presidency and executive branch as a whole at his fingertips, has said little of how he intends to approach the authority he now wields over the country's surveillance policies. As developing policing technologies continue to outpace laws restricting their use, and as Mr. Trump and top members of his administration like Attorney General Jeff Sessions take a hard line against illegal immigration, terrorism and crime, experts in constitutional law and civil liberties fear the lack of an accompanying conversation on privacy protections could contribute to the erosion of Fourth Amendment rights.

"I think we will see a push from the Trump administration to expand surveillance powers, and that of course could directly implicate Fourth Amendment protections," said Christopher Slobogin, a professor at Vanderbilt University Law School who has studied and written on Fourth Amendment, privacy and surveillance issues for years.

"And they're going to push I think also for greater militarization of the police, which could affect Fourth Amendment issues," Slobogin added.

The American Civil Liberties Union is currently taking the Department of Justice to court to determine when the government notifies people they are under surveillance.

In May 2015, before announcing his bid for the presidency, Mr. Trump said he supported legislation allowing the National Security Agency (NSA) to hold bulk metadata, and later in the year reiterated he would tend to "err on the side of security." On the campaign trail, and after taking office, Mr. Trump has emphasized the importance of bulking up police forces and eradicating terrorism. Sessions fought against reforms of the Foreign Intelligence Surveillance Act (FISA) in 2012, and against limits on the NSA's spying powers.

"It's not as though this didn't exist before Trump, because it's all in this terrorism -- war on terrorism stuff," said Robert Bloom, a professor at Boston College Law School who focuses on criminal procedure and civil rights law. "We've loosened up on protections of individuals. But now you've really got an abusive executive. A president and attorney general who don't really give two whits about individual protection and about the Fourth Amendment."

The White House and Department of Justice did not respond to requests for comment for this story.

The Fourth Amendment guarantees the "right of the people to be secure in their persons, houses, papers and effects, against unreasonable searches and seizures." But guaranteeing that right has become increasingly complicated in the digital age. One longstanding legal theory dating to the 1970s, known as the Third Party Doctrine, asserts that once a person gives personal information to a third party, for instance, to a cell service provider, he or she loses the expectation of privacy, and the information can be given to other entities without the person's explicit permission -- without violating the Fourth Amendment.

The Obama administration placed some limitations on surveillance technology, but mostly through policy. The Obama administration required the Department of Justice and Department of Homeland Security to obtain warrants for the use of their 400 Stingrays or cell site simulators, devices that mimic cell phone towers, so all phones within a range connect to it instead of their cell phone provider's nearest tower, and the devices collect cell phone data. The IRS also acquired the technology in recent years.

"But that's the kind of thing that Jeff Sessions could do away with with the stroke of a pen," said Alvaro Bedoya, founding executive director for the Center on Privacy and Technology at Georgetown University Law Center.

Law enforcement agencies say Stingray technology helps them catch suspected criminals -- and it does. But privacy advocates fear the technology's ability to collect nearby cell phone owners' data without their permission or knowledge -- and often, without a warrant -- compromises Fourth Amendment rights.

Federal authorities have said the devices they use are not configured to collect the content of communications, but the capabilities of the technology aren't clear. That's partly because federal authorities have shrouded cell site simulators in mystery, sometimes dropping cases against criminal suspects rather than reveal their policing methods and agreements with private cell site simulator companies that swear the government to product secrecy in contracts.

The ability to put the warrant requirement "through the shredder" at any moment is why policy is an insufficient safeguard, said Matthew Feeney, policy analyst at the Cato Institute, a libertarian think tank.

"We're relying heavily on government policy rather than law, and that I think is a problem," Feeney said.

Many states also use automatic license plate readers, technology that can scan hundreds of plates per minute. In the 2008 election cycle, Virginia State Police used automatic license plate readers on attendees' cars at political rallies for Barack Obama and Sarah Palin, the ACLU revealed. Alone, license plates may not amount to much information, but police have the ability to check those plates against other records, and -- over time -- can observe patterns about a driver's habits, the ACLU argued.

Meanwhile, the federal government is quietly ramping up its surveillance approach at airports, using technology that was, "in most cases developed for the battlefield," Bedoya said.

U.S. Customs and Border Protection began testing facial recognition software -- called Biometric Exit -- at Dulles International Airport outside Washington, D.C., in 2015, and pilot programs are expanding to other large airports. The software -- the concept of which was first required by Bill Clinton-era legislation in 1996 -- is intended to check visa holders entering or leaving the country through facial matching systems. That scan can be checked against a person's passport. As Mr. Trump looks to toughen immigration policies, it's a timely tool.

But Bedoya worries the technology's use won't stop there.

"There aren't many people talking about biometric exit, when it might fundamentally change the way we travel," Bedoya said.

It's unlikely the technology will only be used on foreign nationals, Bedoya said. Many airports mix international and domestic terminals, and it's more practical and realistic to use the technology at the main Transportation Security Administration (TSA) checkpoint, Bedoya said.

"That means you have a flow of both domestic and international travelers," Bedoya said.

Once it's in place, facial recognition software -- like other kinds of policing technology -- can be used to match other federal databases and tell a story.

"We shouldn't forget that all of these tools can be put together," Feeney said.

"Drones can be used to mount a license plate reader," Feeney said. "Body cam footage could be linked to drone footage."

Congress has made some efforts to strengthen privacy in recent months. In February, the House passed the Email Privacy Act, which would require a warrant for any access to stored digital communications. But the Senate has yet to take any action on it, and threats of terrorism may easily quash any momentum on similar legislation, Slobogin said.

"If we have an event like Manchester in the United States -- or Manchester itself -- that might push Congress in the other direction," Slobogin said.

Absent much guidance from Congress in the way of laws, the courts are deciding the future of surveillance as it pertains to the Fourth Amendment, Slobogin said.

"Some of the lower courts have looked at warrants and searches and things of that nature, but the Supreme Court really hasn't weighed in on those kinds of issues," Bloom said.

Slowly, that's changing, as cases work their way up to the highest court in the land.

This year, the Supreme Court will decide United States v. Carpenter, on whether the warrantless seizure and search of historical cell phone records revealing location and movements of a person over the course of months is constitutional.

"That is arguably going to be the most significant Fourth Amendment case in decades," Feeney said.

The Third Party Doctrine theory "needs to be grappled with significantly," and could be reviewed in that case, Bloom said.

The lack of legal protection against an expanding availability of policing technologies may not concern law-abiding citizens, but it should, Feeney said.

"At the moment, we seem to be mostly concerned about radical Islamic terrorism," Feeney said.

"Maybe in 15 years it's progressives, or libertarians, pro-life people or pro-choice people," he added.

This, Feeney said, is the fundamental question people should ask themselves: "Would I be happy with the state of the Fourth Amendment if my enemy is in charge?"