Remarks As Prepared for Delivery by Senator Ron Wyden at the Cato Institute Policy Forum

January 26, 2011

Thank you, Jim, for that inflationary introduction, and thanks very much to the Cato Institute for inviting me to speak today about an issue that I care a lot about – getting the law right when it comes to new technologies. In the race to make it easier to communicate, to work from the road, to send pictures of your kids to friends, and so forth, our technological advances have often sped past our legal checks and balances. I've made it my personal cause to make sure that law enforcement and intelligence agencies can take advantage of these new technologies in a way that doesn't run roughshod over every American's right to keep the records of what they do every day private.

Tech companies are working fast and furious to come up with the latest hot gadget, and that's good for creating jobs and a healthy economy. I'm all for that. But it's important to make sure our laws keep up with the new challenges that these technologies bring. We can't run the Indy 500 of technology with rules designed for the horse and buggy. I've been on the Senate Intelligence Committee for ten years now, and I've spent a lot of time dealing with the ins and outs of criminal and intelligence surveillance laws. So let me give you a little background on the problems I see and then I'll tell you about how I hope to fix them.

Today, most people have some kind of handheld electronic devices, such as high-tech cell phones, digital assistants, and GPS navigation devices. They often carry them around everywhere they go, and subscribe to various services that support these tools or increase their capabilities.

But while everybody's talking and texting and emailing and googling, they probably aren't spending a lot of time thinking about the fact that private companies now log increasingly detailed information about where they're going and what they're doing. I don't want to make this sound like some nefarious plot. It's mostly a consequence of the success of American businesses in answering the needs of their customers. But the impact of this consequence needs to be taken seriously. These technologies make it possible to collect vast amounts of increasingly precise and accurate information about the American public. It is extremely important to ensure that this information is used in a way that protects public safety and protects the privacy rights of law-abiding Americans.

As I looked at the various aspects of the law that apply to handheld electronic devices, there was one question that jumped out at me as being particularly unsettled: now that there are increasing numbers of companies receiving data that reveals their customers' movements and locations, what do government agencies have to do if they want to go to these companies and get this information? Do they need a court order? If so, how much evidence do they have to show to a judge in order to get one?

I believe if you were to ask most Americans these questions, you'd get some version of the same answer. If there is strong evidence that somebody is involved in a crime, or is acting on behalf

of a foreign government or terrorist group, they'd want intelligence or law enforcement agencies to be able to track that person without a lot of unnecessary confusion or legal ambiguity. They also want laws that protect the privacy rights of law-abiding citizens, meaning if there isn't any strong evidence that someone is engaged in nefarious activities, most Americans think that their government should leave that person alone.

Justice Louis Brandeis once said, in regard to a surveillance case that had come before the Supreme Court, that "the most comprehensive of rights and the right most valued by civilized men" was the right to be left alone by their government. Leaving people alone means respecting individuals' privacy rights. Searching people's homes, tapping their phone calls and reading their mail all constitute intrusions on their privacy. That's what the Fourth Amendment is all about – the government has to show probable cause and get a warrant if it wants to do these things.

If you ask most Americans, I believe they would say that surreptitiously turning someone's cell phone into a tracking device – which is increasingly easy to do– and using it to monitor their movements 24/7 is a fairly serious intrusion into their privacy, comparable to searching their house or tapping their phone calls. And I believe most Americans would agree that secretly reviewing records to find out everywhere someone had gone over the last month, or six months, or year, would be an equally significant intrusion. And I believe they would also agree that monitoring a person's movements using a tracking device covertly installed by the government is essentially the same thing as secretly obtaining the records of their movements from a phone company. So that's how I arrived at the view that if a government agency wants to do any of these things, it ought to obtain probable cause before getting access to such personal information. Some might argue that tracking a person's movements, at least when they are outside of their house, is not comparable to searching their home or reading their mail, because when people are out moving from one place to another they are moving around in public, rather than private. I agree that if you drive from your home to the grocery store you obviously expect that other people might see you. But tracking someone's movements 24/7 for an extended period of time is qualitatively different than observing them on a single trip to the store. If you monitor a person's movements for several weeks, you can find out if they regularly visit a particular doctor or psychiatrist, or attend meetings of a locally unpopular political organization, or visit a particular house of worship, or often go to an AIDS clinic. And you won't just find out one of these things – you'll find out all of these things.

The Court of Appeals for the DC Circuit looked at this and made a point of distinguishing visual surveillance from electronic surveillance, and pointed out that it is often the case that different legal standards apply to different types of surveillance techniques. For example, a government agent doesn't need a warrant to stand across the street from someone's house and watch who goes in or out, but if the government wants to find out how many people are in the house by using a high-tech thermal imaging device, the government is going to need a warrant.

Also, in practical terms there is a big difference between visual and electronic surveillance. Tracking someone's movements with a surveillance team requires a significant amount of labor and resources, which means the use of these teams is generally limited to important cases. Tracking someone's movements with a GPS device or by monitoring their cell phone is already

cheap and easy, and it is getting cheaper and easier. So the resource barriers that act as a check against abuse of visual surveillance methods just aren't in place when it comes to these newer surveillance techniques.

It seems clear to me that the explosion of portable electronic devices in our society and their ability to track their owners' movements is a genuinely new phenomenon, and that this phenomenon raises serious issues for intelligence gathering, law enforcement, and the protection of individual privacy rights. The next question to ask is, are our existing laws adequate for dealing with this situation, or does new law need to be written? I believe it is time to modernize the law in this area.

Several months ago, I asked the Congressional Research Service to analyze the legal landscape that surrounds the government's ability to gather geolocation information and prepare a report. It seemed clear to me that this is a blind spot in the law and that courts are divided about how to handle it, but I was looking for an authoritative, nonpartisan evaluation.

The report from the Congressional Research Service makes it very clear that federal courts are collectively unsure about how to handle this issue, and that this has created confusion for law enforcement agencies. It cites case after case where government requests for court orders were denied because the government and the courts disagreed on how much evidence was needed to acquire geolocation information on individuals. And after lengthy legal analysis the report concludes that there isn't any consistency between courts around the country on how much evidence should be needed before the government starts rifling through someone's private life. I believe that lack of clarity endangers every American's privacy and makes it harder for law enforcement officers to do their jobs. When law enforcement and other government entities don't know what the rules are, they waste valuable time and resources trying to figure out how to operate. Because the law is being interpreted differently in different jurisdictions, government attorneys have to go to the trouble of figuring out what the standards for evidence are in the various places where they are operating. And if a particular judge or jurisdiction hasn't previously ruled on the question, then government attorneys are potentially put in the position of having to request a court order without knowing what standards or procedures the judge expects them to follow.

What ends up happening is that the government spends huge amounts of time and resources litigating and appealing what should be clear cut rules. And this has potentially dangerous consequences. It's almost too easy to imagine a case where government agents are stymied in their efforts to track a dangerous criminal or terrorist suspect because a government lawyer makes the wrong guess about how much information to include in his request for a court order.

And we have already seen at least one case, *United States vs. Jones* (also known as *United States vs. Maynard*) where a major drug conviction and life sentence were overturned because the government attempted to gamble on using outdated precedents and creative legal arguments, rather than simply relying on a valid probable cause warrant.

The obvious solution to these problems is for Congress to modernize these outdated laws and clearly and plainly lays out the rules for government acquisition of geolocation information, so

that law enforcement and intelligence agencies can get the information they legitimately need in a way that respects the privacy rights of law-abiding Americans. So that's the problem as I see it. Now here's my solution, and I hope you'll agree with me that it's the right one.

Over the past year, my staff and I have been working on updating the geolocation rules, in an attempt to bring clarity to this murky legal landscape, and we've sought input from a number of individuals and organizations represented in this room. As we've tried out various models and different language, I have focused on several key features that I believe should be part of any geolocation law.

First, the law should provide clarity. Members of the public deserve clarity – they deserve to know what legal procedures and protections apply to electronic devices that can be used to track their movements

Law enforcement and intelligence agencies also should not be mired in a state of permanent confusion about how much evidence they need to show to get a court order. Congress needs to help them out by making sure they have clear, straightforward rules to follow, not a crazy quilt of contradictory legal interpretations and jurisdictional conflicts. So the law needs to lay out an unambiguous standard that government agencies can confidently adhere to.
Clarity will also help private industry, where businesses can find themselves caught between a rock and a hard place because the law is so murky. The various commercial service providers that hold information on their customers' locations have a clear interest in complying with legitimate government requests, and at the same time have a clear interest in upholding their commitments to protect customer privacy. If they deny requests that government agencies believe are legitimate, then they risk being accused of undermining important law enforcement and counterterrorism efforts. But if they cooperate with requests that are arguably based on insufficient evidence, then they risk being accused of illegally violating their customers' privacy, and potentially held liable. So it is no surprise that many of these service providers have recently started weighing in publicly about the need for a clear legal roadmap to follow on this.

Second, the law should establish that government agencies need to show probable cause and get a warrant before acquiring the geolocational information of a person in the United States. You can't tell me - as some government lawyers have argued in the past -- that secretly tracking a person's movements 24/7 isn't a significant intrusion on their privacy, and can be done by meeting a lower standard of evidence, or even no standard at all. I believe that if you put this question to most members of the American public, they would consider it a no-brainer: if government agencies want to secretly monitor all of a person's movements they should meet the requirements spelled out in the Fourth Amendment and go get a probable cause warrant, just as they would do if they were searching that person's home or secretly recording their phone calls.
Third, the law should apply to all acquisitions of the geolocation information of Americans without their knowledge, including acquisitions from commercial service providers, as well as the use of tracking devices covertly installed by the government, such as a GPS unit secretly attached to someone's car.

I would argue that you're splitting hairs if you're trying to judge these two surveillance techniques as being substantially different, and I believe that anybody who looks at the question

from the perspective of the ordinary American citizen will agree. In the one instance the government causes the individual to unknowingly bring the device around with them, and in the other instance the individual voluntarily carries the device, without knowing that it is being used to track his or her movements. In my judgment this is a rather subtle distinction, and certainly does not justify different legal standards for the two methods.

Some of you may also be aware that there actually are some existing laws and precedents with regard to government-installed tracking devices. However, these laws and precedents now date back a few decades, and were written to apply to short-range radio-frequency homing devices. Today's technology is light years ahead of where it was in the early 1980s, and it raises new questions that did not need to be considered back then.

The DC Court of Appeals agreed with this viewpoint, and ruled last August that precedents permitting the warrantless use of short-range homing or beeper devices do not apply to the use of modern GPS devices to provide low-cost 24/7 surveillance. The question of what standard should be applied to today's technologies is no longer hypothetical, and it is time for legislators to confront it.

Fourth, I believe laws on geolocation tracking have to give guidance for both law enforcement and intelligence investigations. A lot of the people and organizations who have weighed in on this issue have been reluctant to address the question of intelligence investigations, and to be frank I think this is probably because a lot of those people feel that they know more about the criminal side of the equation, and less about the intelligence side. Also, because government practices – and even court decisions – regarding surveillance in intelligence investigations are generally secret, there isn't a lot of information available to people who want to research this aspect of the issue.

Speaking as a legislator who has served for a decade on the Senate Intelligence Committee, I can tell you that I believe it makes much more sense to address criminal and intelligence investigations simultaneously. For one thing, the laws governing the two types of investigations have developed in parallel and frequently cross-reference one another, so it is often much easier to update them in tandem than to try to modify one without affecting the other.

So, as I see it, the logical approach is to draft legislation that gives clarity to both law enforcement and intelligence agencies, by establishing a consistent probable cause standard for both types of investigations.

Fifth, the updated rules should apply to both real-time monitoring and the acquisitions of records of past movements. If government agencies are trying to say "tell us where John Smith is right now, and let us know everywhere he goes from now on", that request should be treated the same as a request that says "tell us everywhere that John Smith went in 2010."

Some people might argue that it makes more sense to treat court orders for prospective monitoring differently than court orders for records of past movements. This point is open to debate, but I'll tell you that I believe they should be treated the same, mainly because their impact on individual privacy will be nearly identical. And if you require different procedures

and standards for past records than you do for real-time monitoring, it will probably be a matter of minutes before some over-zealous government lawyer starts arguing that he isn't asking for authorization to engage in real-time tracking, but only for authorization to receive five-second-old records of a person's movements on a constant, rolling basis. The easiest way to head this off and keep the exception from swallowing the rule is to make the rules for record acquisition and real-time or prospective tracking the same.

Sixth, and finally, the law should protect all Americans, regardless of whether or not they are located in the US. As many of you know, during the congressional debate over the FISA Amendments Act of 2008, I successfully offered an amendment that for the first time required intelligence agencies to get a warrant if they wanted to deliberately target the communications of Americans located outside the United States. As I said at the time, in the digital age it makes little sense for an individual's relationship with his or her government to depend on the individual's physical location – no matter where an American goes in the world, it should always mean something to be an American.

I believe the best way to accomplish all of the goals I have just laid out is to do two things: modify the Foreign Intelligence Surveillance Act so that the collection of geolocation information is defined as electronic surveillance, and then create a new geolocation chapter in the US criminal code, based on the chapter that governs wiretapping for law enforcement purposes. This is an important and complex issue, and I believe this approach addresses it in the most straightforward and uncomplicated way possible.

This approach would also have the effect of regulating certain actions by private parties – it would require service providers to get permission from their customers before sharing their geolocation information with other businesses, and it would outlaw what I call the "stalker example." Right now, if a woman's ex-boyfriend secretly taps her phone, he is breaking the law. My approach would make hacking the GPS in her car to track her movements just as illegal – and give her one more protection against her stalker.

So with that, let me yield the floor and take any questions you have. I hope I've shed some light on what's been a murky part of the law, and helped you see how important it is to forge some serious legislation on geolocation, so that law enforcement and intelligence agencies can do their job, in a way that protects the privacy of every law-abiding American. I'd also like to introduce my staffer, John Dickas, who is sitting right here. Get a card from him and stay in touch as you have questions or ideas for us. John has been my lead staffer on this issue for over a year now, and has spent a lot of time poring over the various statutes and legal opinions, so if any of the policy wonks that I see in the audience want to ask a particularly nuanced or technical question, I may ask John to chime in.