Liberty and Security Committee Statement on Location Tracking

A REPORT BY THE CONSTITUTION PROJECT'S LIBERTY AND SECURITY COMMITTEE

September 21, 2011

The Constitution Project
1200 18th Street, NW
Suite 1000
Washington, DC 20036
(202) 580-6920 (tel)
(202) 580-6929 (fax)
info@constitutionproject.org

www.constitutionproject.org

LIBERTY AND SECURITY COMMITTEE STATEMENT ON LOCATION TRACKING

Increasingly in the Digital Age, powerful surveillance technologies are being developed or converted for law enforcement use. Global Positioning System (GPS) and other technologies present law enforcement with various surveillance tools that make it possible to track an individual's location "24/7" with relative ease. Similarly, most people today constantly carry with them personal tracking devices in the form of cell phones and other handheld electronic devices. Indeed, private sector technologies that enable constant monitoring of individuals are moving inexorably forward, and as they are developed, law enforcement agencies inevitably seek to use these new surveillance tools. These include not only GPS devices and cell phones, but also laptop and notebook computers, location based services like OnStar, and technologies yet to be developed. Use of these surveillance devices presents serious challenges in terms of compliance with Fourth Amendment protections. While these technologies enhance the ability of law enforcement agents to accomplish their important work, it is also critical that we carry forward Fourth Amendment safeguards into the Digital Age.

The Fourth Amendment to the Constitution establishes the "right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures," and generally requires that searches and seizures be supported by a warrant issued by a court and substantiated by probable cause.[1] In determining the scope of this protection, the U.S. Supreme Court has required that the individual claiming the protection of the Fourth Amendment have a legitimate expectation of privacy. *See Katz v. United States,* 389 U.S. 347 (1967). In general, the Court has held that there is no legitimate expectation of privacy in information that an individual voluntarily makes public. Thus, typically there is no legitimate expectation of privacy in a public place, although what a person "seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected." *See Katz,* 389 U.S. at 351. When applying this doctrine to travel on the public roads in *United States v. Knotts,* 460 U.S. 276 (1983), the Supreme Court held that police officers were not required to obtain a warrant before using a radio-signal beeper to track an individual on a single trip, as he travelled by "automobile on public streets and highways." However, the Court stated that it was not addressing the Fourth Amendment implications of twenty-four hour "dragnet-type" surveillance, which it expressly left for another day. *See* 460 U.S. at 283.

That day has now arrived. The Court has thus far been hesitant to examine these questions, noting that "[t]he judiciary risks error by elaborating too fully on the *Fourth Amendment* implications of emerging technology before its role in society has become clear." *City of Ontario v. Quon*, 130 S.Ct. 2619, 2629 (2010). But tracking technologies have now advanced well beyond the use of radio-signal beepers. These technologies, including tracking of cell phone location information and the use of GPS technology, are now far more sophisticated and precise, and more significantly, they are capable of providing continuous monitoring and the compilation of vast databases of information about individuals' daily movements. The Supreme Court recently granted review of a decision of the U.S. Court of Appeals for the District of Columbia Circuit holding that continuous GPS monitoring of a car's every movement for four weeks straight does infringe on a reasonable expectation of privacy.

[1] U.S. Const. amend. IV.

See United States v. Maynard, 615 F.3d 544 (D.C. Cir. 2010), *cert. granted sub nom. United States v. Jones,* 131 S. Ct. 671 (2011).

We believe that such transformative changes in technology must be recognized in the law to ensure that Fourth Amendment protections continue to apply. Therefore, as outlined more fully below, we, the undersigned members of The Constitution Project's Liberty and Security Committee, have concluded that a warrant should be required before the government may track an individual's movements using these technologies for more than a 24-hour period, and before installing such a tracking device on an individual's property regardless of the tracking period. In addition, even if the Supreme Court disagrees with our constitutional analysis, we urge that Congress should adopt legislation to implement these limits. We also recommend that Congress should amend the Electronic Communications Privacy Act (ECPA) to require the government to obtain a warrant based upon probable cause in order to access cell phone location information. GPS and other powerful electronic tracking tools should be available to law enforcement when they have probable cause and obtain a warrant; but the government should not have unchecked discretion to electronically track anyone, anywhere, at any time without cause.

Expectation of Privacy in a Public Place

Legal doctrine has long recognized that the privacy of the home is the core privacy right protected by the Fourth Amendment. Thus, "[w]ith few exceptions, the question whether a warrantless search of a home is reasonable and hence constitutional must be answered no." *Kyllo v. United States*, 533 U.S. 27, 31 (2001); *see also United States v. Karo*, 468 U.S. 705, 714 (1984). As noted above, the Court has not extended this level of privacy protection for activities conducted in public places. *See e.g., Knotts,* 460 U.S. 276.

However, rapid changes in technology have been eroding the distinction between private and public spaces. Our Liberty and Security Committee addressed this dynamic several years ago in the context of public video surveillance systems.[2] Like the use of cameras, tracking technologies may threaten actual privacy expectations in public in two ways. First, even in public places, individuals will often check to see whether there are people nearby who can observe their actions and will alter their behavior accordingly. Unseen cameras or tracking devices alter this equation by removing an individual's ability to determine whether he or she is actually being "watched." In addition to stealth, such technologies facilitate lengthy and continuous monitoring. Thus, the technology enables tracking in ways that are basically physically impossible for human law enforcement officers – or private individuals – to match. For many Americans, such pervasive surveillance and tracking conjures up Orwellian images that "Big Brother is watching you," and an instinctive reaction that privacy is being invaded, even in a public place.

Second, when camera systems and tracking technologies are able to create digital databases from which a digital dossier of an individual's daily movements can be compiled, this will not simply increase the *amount* of information being observed and collected. Such surveillance also provides the capability to compile and analyze vast quantities of data well

[2] *See* The Constitution Project's Liberty and Security Committee, *Guidelines for Public Video Surveillance: A guide to Protecting Communities and Preserving Civil Liberties* 8 (2006), available at: http://www.constitutionproject.org/pdf/54.pdf .

beyond what could be accomplished by human law enforcement officers on their own. In the words of the D.C. Circuit in *Maynard*, moving from basic monitoring to a digital database with such complete pattern analysis is "the distinction between a day in the life and a way of life." We believe that when powerful tracking technologies to conduct pervasive surveillance are paired with this analytic capability and a digital database, such monitoring can violate an individual's reasonable expectation of privacy even in a public place.

Use of GPS Tracking Violates Reasonable Expectations of Privacy

Global Positioning System (GPS) technology is a satellite-based navigation system that can provide extremely accurate location information. Commercially available GPS devices for use by ordinary consumers can pinpoint an individual's location accurately to within fifteen meters.[3] Moreover, GPS devices send a constant signal that may be received from a remote location, and as noted above, these data may be stored in a digital database and then searched for patterns. As described in a recent article:

> Once a GPS receiver is outfitted with a transmitter or recording device, third parties interested in determining the whereabouts of the GPS device may remotely and unblinkingly surveil its location continually virtually anywhere on the globe. Quantitatively and qualitatively, then, GPS-enabled surveillance is far cheaper and vastly superior to visual surveillance, as no one human or organization of human observers is currently capable of such comprehensive, continuous, and accurate information regarding location and movement monitoring.[4]

As noted above, the Supreme Court has established that protection for the home is at the core of the Fourth Amendment, and thus a warrant will be required for any search that covers the inside of a home. *See Kyllo,* 533 U.S. at 31; *Karo*, 468 U.S. at 714. In recognition of the precision of GPS tracking, the federal government, by policy, has required that when there is a strong potential that the GPS device they would like to track may be carried inside a home – such as a GPS enabled phone – law enforcement agents must obtain a warrant before obtaining GPS tracking data. Thus, U.S. Department of Justice policy states that in order to seek GPS tracking information generated by GPS enabled phones, agents must first obtain a warrant based on probable cause.[5]

Federal government agents and police in various jurisdictions have not applied this same policy for the use of GPS devices to track the movement of vehicles. Various law enforcement agencies, including the FBI, have sought to install GPS devices on vehicles to track suspects without first obtaining a warrant based upon probable cause. Relying upon a 1983 U.S. Supreme Court case involving earlier technology and surveillance over the course of a single trip, law enforcement has argued that tracking travel over the public roads does not violate anyone's reasonable expectation of privacy. However, we believe that the 1983 decision, *United States v. Knotts,* 460 U.S. 276 (1983), does not contemplate or cover the extended use

---

[3] *See* Garmin, What is GPS? http://www8.garmin.com/aboutGPS/ .

[4] Lenese Herbert, "Challenging the (Un)Constitutionality of Governmental GPS Surveillance," 26 CRIMINAL JUSTICE 34, 35 (Summer 2011).

[5] Statement of James A. Baker, Associate Deputy Attorney General, Before the Committee on Judiciary, U.S. Senate, April 6, 2011, available at: http://judiciary.senate.gov/pdf/11-4-6%20Baker%20Testimony.pdf .

of GPS tracking. Instead we agree with the analysis of the U.S. Court of Appeals for the District of Columbia Circuit in *United States v. Maynard,* 615 F.3d 544 (D.C. Cir. 2010), *cert. granted sub nom. United States v. Jones,* 131 S. Ct. 671 (2011), which explains how the nature and extent of GPS surveillance changes the analysis of what constitutes a reasonable expectation of privacy. Thus, we believe that the Fourth Amendment's warrant requirement applies in this context.

In *Knotts*, 460 U.S. at 283, the Supreme Court held that no warrant was required when police tracked a suspect using a radio beeper as he travelled by vehicle on public roads for a single trip. This earlier technology required the police to follow the vehicle in order to track the signal. In addition, as noted above, the Court explicitly left open the question of "twenty-four hour surveillance" and "dragnet-type law enforcement practices." As the D.C. Circuit explained in *United States v. Maynard*:

> *Knotts* held only that "[a] person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another," [460 U.S.] at 281, not that such a person has no reasonable expectation of privacy in his movements whatsoever, world without end.

Maynard, 615 F.3d at 557. The D.C. Circuit examined in depth the difference between surveillance over the course of a single car trip, and 24/7 electronic monitoring over the course of a month, with automatic recording of every location visited over the course of that time period. Thus the court noted:

> The difference is not one of degree but of kind, for no single journey reveals the habits and patterns that mark the distinction between a day in the life and a way of life, nor the departure from a routine. . . . These types of information can each reveal more about a person than does any individual trip viewed in isolation. Repeated visits to a church, a gym, a bar, or a bookie tell a story not told by any single visit, as does one's not visiting any of these places over the course of a month. The sequence of a person's movements can reveal still more.

Maynard, 615 F.3d at 562.

We agree. GPS technology has made pervasive and continuous location tracking possible in a way that was never before feasible relying solely on human law enforcement officers. As the article cited above concluded, "no one human or organization of human observers is currently capable of such comprehensive, continuous, and accurate information regarding location and movement monitoring" that GPS can provide.[6] Moreover, when such tracking is conducted, vast quantities of data are collected, automatically stored in a searchable digital database, and analyzed for patterns of behavior that can reveal a great amount of very personal and private information. These technologies convert traditional "tailing" of a suspect into a new and different type of surveillance, paired with new and powerful digital analytic tools, that alters our analysis of expectations of privacy in a public place. Such tools may be a valuable aid to law enforcement when following a particular suspect. But their use is also a search that should require a warrant based upon a showing of probable cause.

[6] Herbert, *supra* note 4 at 35.

We do not suggest that the Supreme Court must overrule the *Knotts* decision to recognize the need for a warrant in GPS tracking cases. Rather, based upon "the distinction between a day in the life and a way of life" as framed by the D.C. Circuit, we believe the line can be drawn at 24-hours. If law enforcement seeks to use GPS or other electronic tracking for more than a 24-hour period – from the time the tracking first begins until the time it ends, regardless of whether the device is continuously operated – it must seek a warrant, even if the locations tracked are public places.[7] We recognize that this 24-hour limit may be considered a somewhat arbitrary line, but the Supreme Court has recognized that in some circumstances the Court must "articulate more clearly the boundaries of what is permissible under the Fourth Amendment," and although the Court may "hesitate to announce that the Constitution compels a specific time limit, it is important to provide some degree of certainty," to enable law enforcement to establish procedures that will "fall within constitutional bounds." *See County of Riverside v. McLaughlin*, 500 U.S. 44, 56 (1991) (setting a 48-hour post-arrest time limit for holding a hearing to establish probable cause). Moreover, even if the Court chooses not to recognize a warrant requirement for GPS tracking covering a period of more than 24-hours, Congress can and should enact legislation to impose such a warrant requirement for GPS and other electronic tracking.

Our analysis applies equally whether law enforcement is seeking to collect the tracking information from its own device that it has installed, or from a third-party such as a service provider. We recognize that under the "third party" doctrine a person is considered not to have a reasonable expectation of privacy in information that he or she voluntarily discloses to a third party. *See United States v. Miller*, 429 U.S. 435, 443 (1976). However, the third party doctrine has been widely criticized as outdated in the Digital Age,[8] including by our Liberty and Security Committee. As we noted in our report on government data mining programs, "in many instances, individuals have no choice but to disclose information to a third party in order to be able to participate in basic aspects of modern society,"[9] and the Supreme Court has indicated a willingness to narrow this doctrine in at least some cases.[10] Ultimately, we do not believe the government should be able to conduct an end run around Fourth Amendment requirements by relying on third parties to collect the GPS data for them.

In short, when powerful electronic surveillance such as GPS tracking is conducted to cover a period of longer than 24-hours, we consider this to be a search under the Fourth Amendment for which a warrant based upon probable cause is required. Therefore, except in cases where the subject turns over the information to law enforcement voluntarily, a warrant based on probable cause should be required before law enforcement may seek GPS or other

---

[7] Some committee members believe that the warrant requirement should apply for all such electronic location tracking, even that lasting less than 24-hours. However, all undersigned members agree that for tracking that extends beyond a 24-hour period, a warrant must be required.

[8] *See e.g.,* Daniel J. Solove, *Fourth Amendment Codification and Professor Kerr's Misguided Call for Judicial Deference,* 74 Fordham L. Rev. 747, 753 (2005); Herbert, *supra* note 4 at 37.

[9] The Constitution Project's Liberty and Security Committee, *Principles for Government Data Mining: Preserving Civil Liberties in the Information Age* at 13 (2010), available at http://www.constitutionproject.org/pdf/DataMiningPublication.pdf .

[10] Our data mining report points out that in *Ferguson v. City of Charleston,* 532 U.S. 67, 83-84 (2001), the Court recognized a reasonable expectation of privacy in the results of diagnostic tests performed by a hospital.

electronic location tracking information for a period extending beyond 24 hours. That limit would be reached at the 24th hour, even if law enforcement turned the device off for part of that time period. Law enforcement should be permitted to use these powerful tracking tools, but only where they can demonstrate probable cause and obtain a warrant. If such tracking is not considered to be a search covered by the Fourth Amendment's warrant requirement, then law enforcement would be permitted to conduct unlimited GPS tracking on anyone, anywhere and could do so for illegitimate reasons or for no reason at all. Thus, as noted above, if the Supreme Court fails to recognize that a warrant should be required for GPS tracking of longer than 24-hours, then Congress should enact such a requirement.

Those opposing the view that GPS tracking violates a reasonable expectation of privacy have argued that there can never be a reasonable expectation of privacy in a public place, and they disagree that pervasive surveillance creates a meaningful difference in the privacy intrusion. *See United States v. Jones,* 625 F.3d 766 (D.C. Cir. 2010) (Sentelle, J., dissenting from denial of rehearing en banc). Under this view, even continuous 24/7 monitoring for a month, that automatically sends data to a digital searchable database, does not intrude on a "reasonable expectation of privacy" because "[t]he sum of an infinite number of zero-value parts is also zero." *Id.* at 769.[11] In our assessment, this viewpoint fails to appreciate the transformative nature of current and developing tracking technologies. We are not simply facing a greater number of data points, but a qualitative change that can alter the very nature of public places.

We note that the U.S. Courts of Appeals that have upheld the ability of law enforcement to use GPS tracking without a warrant have explicitly cautioned that there are likely limits to the extent of warrantless tracking that would be constitutionally permissible. In *United States v. Garcia*, 474 F.3d 994 (7th Cir. 2007), *cert denied* 552 U.S. 883 (2007), Judge Posner, writing for the court, explained:

> The new technologies enable, as the old (because of expense) do not, wholesale surveillance. One can imagine the police affixing GPS tracking devices to thousands of cars at random, recovering the devices, and using digital search techniques to identify suspicious driving patterns. . . . It would be premature to rule that such a program of mass surveillance could not possibly raise a question under the *Fourth Amendment.* . . . Technological progress poses a threat to privacy by enabling an extent of surveillance that in earlier times would have been prohibitively expensive. Whether and what kind of restrictions should, in the name of the Constitution, be placed on such surveillance when used in routine criminal enforcement are momentous issues that fortunately we need not try to resolve in this case."

Garcia, 474 F.3d at 998. Both the Eighth Circuit and the Ninth Circuit have cited this cautionary language with approval. *See United States v. Marquez,* 605 F.3d 604, 610 (8th Cir. 2010); *United States v. Pineda-Moreno*, 591 F.3d 1212, 1217 n.2 (9th Cir. 2010). And the two U.S. Courts of Appeals that have considered GPS tracking after the D.C. Circuit's August 2010

[11] Some courts have also rejected such challenges on the grounds that the defendant did not have standing to contest the tracking because he was only a passenger in the GPS-tracked vehicle. *See, e.g. United States v. Marquez,* 605 F.3d 604, 609 (8th Cir. 2010). The question of standing would remain under our approach, but this would simply mean that in particular cases, certain individuals cannot complain that *their* Fourth Amendment rights were violated.

decision in *Maynard*, both distinguished the cases before them on the grounds that each only involved short-term GPS surveillance. *See United States v. Cuevas-Perez,* 640 F.3d 272 (7th Cir. 2011); *United States v. Hernandez*, 647 F.3d 216 (5th Cir. 2011). Similarly, in *Kyllo*, the Supreme Court cautioned against policies that would "permit police technology to erode the privacy guaranteed by the *Fourth Amendment*." *Kyllo,* 533 U.S. at 34.

Installation of a GPS Device is a Seizure for Purposes of the Fourth Amendment

In addition, where the use of GPS tracking requires installation of a device on an individual's vehicle or other property, a warrant would also be required based upon the government's intrusion into personal property. Where the government must come into physical contact with an individual's property to install the device, this triggers Fourth Amendment protection. *Cf. United States v. Jones,* 625 F.3d 766 (D.C. Cir. 2010) (Kavanaugh, J., dissenting from denial of rehearing en banc).

The majority of the federal Courts of Appeals which have addressed the actual installation of GPS tracking devices have analyzed the privacy, and not the property interests, at stake. Thus, for example, in *United States v. Pineda-Moreno*, 591 F.3d 1212 (9th Cir. 2010), the Ninth Circuit rejected the argument that the installation of a GPS device on the defendant's car without a warrant violated the Fourth Amendment, on the ground that he had no reasonable expectation of privacy in his car parked in his driveway because a driveway is "only a semi-private area" and he took no steps, such as a fence or gate, to exclude passersby from it.

However, in addition to the Fourth Amendment privacy concerns raised by the use of GPS tracking devices, the Fourth Amendment right to be free from unreasonable seizures is raised by the actual installation of the device itself. The Supreme Court has stated that the Fourth Amendment "protects two types of expectations, one involving 'searches,' the other 'seizures.' A 'search' occurs when an expectation of privacy that society is prepared to consider reasonable is infringed. A 'seizure' of property occurs where there is some meaningful interference with an individual's possessory interests in that property." *Soldal v. Cook County., Ill.*, 506 U.S. 56, 62 (1992) (quoting *United States v. Jacobsen*, 466 U. S. 109, 113 (1984)).

The question, then, is whether the installation of a tracking device interferes with the vehicle owner's possessory interest in the vehicle. Although two Circuits have found that the tracking devices did not interfere with the owner's ability to otherwise use or operate the vehicle and did not damage the vehicle, so no seizure had occurred, *see United States v. Garcia*, 474 F.3d 994 (7th Cir. 2007); *United States v. McIver*, 186 F.3d 1119 (9th Cir. 1999), other cases have recognized that a warrant is required before law enforcement may come into physical contact with an owner's property. As Justice Stevens explained in his dissent in *United States v. Karo*, the owner of property has a right to exclude it from "all the world" and the police use infringes on that right, notwithstanding the fact that the vehicle in question may still otherwise be usable and/or operable. *Karo,* 468 U.S. 705, 729 (Stevens, J. concurring in part and dissenting in part).

Similarly, although the property interest issue was not raised in *Knotts* (because in that case the defendant did not own the property in which the beeper was placed and thus did not have standing to raise the issue), in his concurrence, Justice Brennan wrote, "when the

Government does engage in physical intrusion of a constitutionally protected area in order to obtain information, that intrusion may constitute a violation of the Fourth Amendment even if the same information could have been obtained by other means." *Knotts,* 460 U.S. at 286. In this same vein, in *Silverman v. United States*, the Supreme Court held that installation of a listening device on the defendants' property through a heating duct in a shared wall was an "unauthorized physical encroachment within a constitutionally protected area," even though the device in question penetrated the defendants' property by less than an inch. *Silverman,* 365 U.S. 505, 512.

This line of reasoning has led at least one circuit judge to conclude that the Fourth Amendment does apply to installation of a GPS device, *see United States v. McIver*, 186 F.3d 1119, 1135 (9th Cir. 1999) (Kleinfeld, J., concurring), and another to urge that this theory deserves serious consideration. *See United States v. Jones,* 625 F.3d 766 (D.C. Cir. 2010) (Kavanaugh, J., dissenting from denial of rehearing en banc).[12] In *McIver,* Judge Kleinfeld wrote:

> [T]he owner of a vehicle has a possessory interest that is meaningfully interfered with if a transmitter is installed, even where the installation does not interfere with a reasonable expectation of privacy. That is to say, installing a beeper is a seizure. Many seizures by law enforcement officers are permissible under the Fourth Amendment....But it is one thing to justify a seizure, and quite another not to treat substantial interference with possessory interests as a seizure.
> *****
> In the absence of a warrant issued by a neutral magistrate, or applicability of an exception to the Fourth Amendment warrant requirement, people are entitled to keep police officers' hands and tools off their vehicles.

McIver, 186 F.3d at 1135.

We agree with this analysis, and thus, we believe that where the use of GPS tracking requires installation of a device on an individual's vehicle or other property, a warrant would also be required based upon the government's intrusion into personal property. Where the government must come into physical contact with an individual's property to install the device, this triggers Fourth Amendment protection. *See United States v. Jones,* 625 F.3d 766 (D.C. Cir. 2010) (Kavanaugh, J., dissenting from denial of rehearing en banc).

Probable Cause Should Also be Required for Cell Phone Location Tracking

In many cases, cell phone tracking information is not as precise as GPS tracking, because the phones are simply tracked to the nearest cell tower. However, especially with the advent of "microcells" which may only cover a single shopping mall or hotel, in some cases, cell

[12] *See also Commonwealth v. Connolly*, 2009 Mass. LEXIS 642 (Sept. 17, 2009) (Placement of tracking device on a vehicle was a "seizure" under Massachusetts constitutional analog to the Fourth Amendment. "When an electronic surveillance device is installed in a motor vehicle, be it a beeper, radio transmitter, or GPS device, the government's control and use of the defendant's vehicle to track its movements interferes with the defendant's interest in the vehicle notwithstanding that he maintains possession of it.").

phone tracking information may more easily pinpoint a user's location than GPS data. Similarly, cell phones may be able to transmit in certain locations where GPS devices do not work – such as subways – thereby providing more accurate location information.

Moreover, the Supreme Court has recently recognized that individuals may have a legitimate expectation of privacy in the use of their cell phones. Although the Court did not ultimately decide the privacy issue, it examined privacy interests in the use of cell phones in *City of Ontario v. Quon*, 130 S.Ct. 2619 (2010). The Court noted that:

> Cell phone and text message communications are so pervasive that some persons may consider them to be essential means or necessary instruments for self-expression, even self-identification. That might strengthen the case for an expectation of privacy.

Id. at 2630.

In short, monitoring of cell tower information on a continuous basis raises the same issues as does the use of extended GPS tracking. We therefore similarly conclude that any location tracking technologies, if applied continuously and if capable of generating searchable and extensive digital databases, raise the same privacy concerns. Thus, a warrant based upon probable cause should be required for the use of any such location tracking technologies. Typically, law enforcement would need to obtain cell phone tracking data from a third party service provider, but as discussed above, we have concluded that a warrant should be required even where data are sought from third parties.

In recognition of these concerns for privacy in the Digital Age, The Constitution Project's Liberty and Security Committee agreed in 2010 that The Constitution Project should join the Digital Due Process Coalition (DDP). DDP is a coalition of more than thirty of the nation's leading communications, equipment, and online services companies and non-governmental privacy advocates, which have come together to seek reform of the Electronic Communications Privacy Act of 1986 (ECPA). Among the four DDP reform principles is one regarding cell phone tracking information. Specifically, we have agreed with the DDP coalition that government entities should be able to obtain "location information regarding a mobile communications device only with a warrant issued based on a showing of probable cause."[13] We join in the call for Congress to amend ECPA to impose this warrant requirement.

Recommendations:

For these reasons, we recommend that:

1. Except in cases where the subject turns over the information voluntarily to law enforcement, a warrant based upon probable cause should be required before law enforcement may seek GPS or other electronic location tracking information for a period of more than 24-hours (measured from the time tracking begins until it ends, even if the

[13] *See* The Digital Due Process Coalition Principles available at: www.digitaldueprocess.org. The Constitution Project has joined the DDP Coalition, and thus also supports all three of the other DDP principles. These principles seek to clarify ECPA and to incorporate stronger privacy safeguards for individuals when government seeks access to electronic communications.

device is turned off for some portion of that time period). The warrant requirement should apply for electronic tracking to be conducted by law enforcement itself as well as to requests by the government to obtain such information from a third party. If the Supreme Court does not adopt such a rule, Congress should enact legislation establishing this warrant requirement.

2. A warrant based upon probable cause should be required before law enforcement may install a GPS or other tracking device on an individual's property. As with Recommendation #1 above, if the Supreme Court does not adopt such a rule, Congress should enact legislation establishing this warrant requirement.

3. Congress should amend the Electronic Communications Privacy Act (ECPA) to require that a governmental entity may access, or may require a covered entity to provide, prospectively or retrospectively, location information regarding a mobile communications device only with a warrant issued based on a showing of probable cause.

MEMBERS OF THE CONSTITUTION PROJECT'S LIBERTY AND SECURITY COMMITTEE
Endorsing the *Statement on Location Tracking*[*]

CO-CHAIRS:

David Cole, Professor of Law, Georgetown University Law Center

David Keene, Former Chairman, American Conservative Union

MEMBERS:

Bob Barr, former Member of Congress (R-GA); CEO, Liberty Strategies, LLC; the 21st Century Liberties Chair for Freedom and Privacy, the American Conservative Union; Chairman, Patriots to Restore Checks and Balances; Practicing Attorney in Atlanta, GA

David E. Birenbaum, Of Counsel, Fried, Frank, Harris, Shriver & Jacobson LLP; Senior Scholar, Woodrow Wilson International Center for Scholars; US Ambassador to the UN for UN Management and Reform, 1994-96

Phillip J. Cooper, Professor, Mark O. Hatfield School of Government, Portland State University

Mickey Edwards, Vice President, Aspen Institute; former Member of Congress (R-OK) and chairman of the House Republican Policy Committee

Thomas B. Evans, Jr., Chairman, The Evans Group, Ltd.; Founder Florida Coalition for Preservation; Member of Congress (R-DE), 1977-1983

John W. Dean, Counsel to President Richard Nixon

Eugene R. Fidell, Senior Research Scholar in Law and Florence Rogatz Visiting Lecturer in Law, Yale Law School

Philip Giraldi, Contributing Editor for *The American Conservative Magazine*, antiwar.com, and *Campaign for Liberty*; Executive Director, Council for the National Interest; former operations officer specializing in counter-terrorism, Central Intelligence Agency, 1975-1992; United States Army Intelligence

Asa Hutchinson, Senior Partner, Asa Hutchinson Law Group; Undersecretary, Department of Homeland Security, 2003-2005; Administrator, Drug Enforcement Administration, 2001-2003; Member of Congress (R-AR), 1997-2001; United States Attorney, Western District of Arkansas, 1982-1985

David Lawrence, Jr., President, Early Childhood Initiative Foundation; Publisher (Ret.), *Miami Herald* and *Detroit Free Press*

Kate Martin, Director, Center for National Security Studies

Mary O. McCarthy, Consultant, Freedom of Information and Privacy Act; Associate Deputy Inspector General, Investigations, Central Intelligence Agency, 2005-2006; Visiting Fellow, Center for Strategic and International Studies, 2002 to 2004; Senior Policy Planner, Directorate of Science and Technology, Central Intelligence Agency, 2001-2002; Senior Director, Special Assistant to the President, National Security Council, 1998-2001; Director for Intelligence Programs, National Security Council, 1996-1998; National Intelligence Officer for Warning, (Deputy 1991-1994) 1991-1996.

Paul R. Pillar, Visiting Professor and Director of Studies, Security Studies Program, Georgetown University; Intelligence officer (positions included Deputy Chief of DCI Counterterrorist Center, National Intelligence Officer for the Near East and South Asia, and Executive Assistant to the Director of Central Intelligence), Central Intelligence Agency and National Intelligence Council, 1977-2005

James Robertson, Neutral Arbitrator and Mediator, JAMS; U.S. District Judge for the District of Columbia, 1994-2010

William S. Sessions, Partner, Holland and Knight LLP; Director, Federal Bureau of Investigation, 1987-1993; Judge, United States District Court for the Western District of Texas, 1974-1987, Chief Judge, 1980-1987; United States Attorney, Western District of Texas, 1971-1974

Earl Silbert, Partner, DLA Piper; United States Attorney, District of Columbia (1974-1979); former Watergate Prosecutor

Neal R. Sonnett, Member, American Bar Association Board of Governors; Past Chair, American Bar Association Task Force on ABA Task Force on Treatment of Enemy Combatants and Task Force on Domestic Surveillance in the Fight Against Terrorism

William H. Taft, IV, Of Counsel, Fried, Frank, Harris, Shriver & Jacobson; Legal Advisor, Department of State, George W. Bush administration; Deputy Secretary of Defense, Reagan administration

Colby Vokey, LtCol USMC (Ret.); Attorney, Fitzpatrick Hagood Smith & Uhl LLP; U.S. Marine Corps, 1987-2008, Lieutenant Colonel; Lead Counsel for Guantanamo detainee Omar Khadar at Military Commissions, 2005-2007

Patricia McGowan Wald, former Judge, International Criminal Tribunal for the former Yugoslavia; former Chief Judge, United States Court of Appeals for the D.C. Circuit

John W. Whitehead, President, The Rutherford Institute

Lawrence B. Wilkerson, Colonel, US Army (Ret.); Adjunct Professor of Government and Public Policy at the College of William and Mary; Chief of Staff to Secretary of State Colin L. Powell, 2002-2005

THE CONSTITUTION PROJECT STAFF:

Sharon Bradford Franklin, Senior Counsel, Rule of Law Program

[*] Affiliations listed for identification purposes only.