Testimony of Orin S. Kerr
Professor, George Washington University Law School
United States House of Representatives
Committee on the Judiciary
Subcommittee on the Constitution, Civil Rights, and Civil Liberties
Hearing on Electronic Communications Privacy Act Reform

May 5, 2010

Chairman Nadler, Ranking Member Sensenbrenner, and Members of the Subcommittee:

My name is Orin Kerr, and I am a Professor at George Washington University Law School. I wish to thank the Members of the Committee for their willingness to delve into the complicated and yet extremely important privacy laws that Congress has created to protect Internet and telephone communications. I teach these statutes to my students as part of my law school course on Computer Crime Law, and my students are routinely surprised that the law here is so out-of-date.

Reforms here are surely needed. The question is, what reforms are best? I have set out many of my own views in a law review article, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, published by the George Washington Law Review in 2004. But today's hearing has been prompted by a specific set of proposals offered by the Digital Due Process coalition. Given that, I thought it would be most help to list the proposals offered by the Digital Due Process coalition and then respond to them.

Before I begin, I want to stress two points. First, I think it's helpful to approach reforming these statutes with a simple goal in mind: In my view, the goal of the Electronic Communications Privacy Act should be to try to match privacy rights in online and telephone- based investigations to the kinds of privacy rights we are familiar with in traditional physical investigations. Most of us have watched the TV show *Law & Order*, and we're familiar with both the powers that the government has to solve crimes as well as the limitations placed on those powers needed to protect and preserve our individual rights. Those powers and their limitations reflect a constitutional balance: It is the balance that the Supreme Court tries to make in interpreting the Fourth Amendment's prohibition on unreasonable searches and seizures. The Electronic Communications

Privacy Act is a statutory version of the Fourth Amendment for a new technological age: It tries to impose the same sort of balanced approach to the new investigations involving new network technologies that the Fourth Amendment strikes in the physical world. As a result, the goal of reforming the statute should be to maintain that balance as technology continues to change.

Second, it would be extremely helpful for Congress to precede any amendments to these statutes with extensive hearings on the latest technologies and the latest government practices. The best way for Congress to update these statutes is to hold open hearings in which government officials can explain how they are using these new technologies and representatives from Internet service providers and phone companies can explain how their technologies work and how they cooperate with law enforcement. Without such hearings, we can only guess at the specifics of how different rules will actually impact real-world investigations. Informed rulemaking requires a thorough understanding of investigative practices and new technologies, and the best way to determine that would be through open Congressional hearings.

With those general points made, let me now turn to the four specific proposals made by the Digital Due Process coalition:

Proposal 1

> *"A governmental entity may require an entity covered by ECPA (a provider of wire or electronic communication service or a provider of remote computing service) to disclose communications that are not readily accessible to the public only with a search warrant issued based on a showing of probable cause, regardless of the age of the communications, the means or status of their storage or the provider's access to or use of the communications in its normal business operations."*

My reaction: Generally favorable, but with two reservations.

Explanation: I agree that the distinctions found in the current statute make no sense. Further, it is my view that the Fourth Amendment requires a warrant to be obtained in this setting, as I explained in a recent article. *See* Orin Kerr, *Applying the Fourth Amendment to the Internet: A General Approach*, 62 Stan. L. Rev. 1005 (2010).

As a result, any statutory rule that allows the government to obtain contents with less process than a warrant will be unconstitutional in many settings.

I have two reservations. First, such a rule may not work when the government obtains records from corporations that are suspected of engaging in criminal activity. In the corporate crime setting, the government generally obtains records using subpoenas rather than warrants. The government compels the corporation to disclose its records under the power of the subpoena without first obtaining probable cause. Because the Electronic Communications Privacy Act applies to all providers of electronic communication service, however, a warrant requirement for all contents stored by entities covered by the statute might inadvertently block investigations into such corporate crimes.

Consider how a warrant requirement might work in that setting. If a warrant is required for every compelled access to every e-mail account, the corporation under investigation will plausibly insist that each e-mail account of each corporate employee must be justified by its own search warrant and its own finding of probable cause. Corporations engaged in criminal activity could use this rule by keeping all their records stored in the form of e-mails: They could store the evidence of fraud in documents stored as attachments, using the protections of the Electronic Communications Privacy to hide evidence of fraud from investigators. The result would block many if not most investigations into corporate criminal activity. For example, my understanding is that the Securities and Exchange Commission (SEC) does not have criminal enforcement power and could not obtain a warrant to investigate securities violations under an all-warrant rule. The SEC relies on subpoenas, which would not be usable so long as the corporation under investigation provided e-mail to its employees.

To avoid this, Congress should consider a rule that permits the government to use its subpoena authority in the case of investigations into corporate crimes when obtaining records from a designated representative of the corporation. A similar rule may also be useful in the case of investigations into misconduct by government employees. The government employees may have no Fourth Amendment rights in their government-provided accounts, but investigators will nonetheless wish to compel the contents of a government employee's accounts from the agency that provides the service. If there are

no Fourth Amendment protections in that setting, a warrant should not be necessary and a subpoena should suffice.

Proposal 2

> *"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."*

My reaction: I disagree in part.

Explanation: I have two concerns about this proposal. First, it is vague. Second, it does not distinguish among different types of location information.

My first difficulty with this proposal is that it is vague. The proposal would require probable cause, but probable cause *of what*? Is that probable cause to believe the person tracked is guilty of a crime? Or is it probable cause to believe the evidence of location information obtained would *itself* be evidence of crime?

The difference is important. In the case of a search warrant, "probable cause" generally refers to probable cause to believe that the information to be obtained is itself evidence of a crime. But cell phone location information will itself be evidence of crime only in specific kinds of cases. For example, such information normally will not be evidence of a crime if investigators want to obtain the present location of someone who committed a past crime.

To see this, imagine the police have probable cause to arrest a criminal for a crime committed last week. The police want to locate the suspect in order to arrest him. In that case, the police will not have probable cause to believe that the location of the criminal's cell phone is itself evidence of a crime. The suspect's location a week after the crime occurred does not give the police any information indicating that the suspect did or did not commit the crime. But if the police have probable cause to arrest someone, and they know his cell-phone number, I would think the law should allow the government some way of locating the suspect pursuant to an appropriate court order. A requirement that

location information be obtainable only based on probable cause to believe that the location information is itself evidence of a crime would not seem to allow that.

My second concern with the proposal is that not all location information is created equal. The level of cause that should be required may depend on the resolution of that identity information. Location information that tells investigators only that a suspect is somewhere in Manhattan is quite different from location information that tells investigators that a suspect is in the far left corner of his bedroom. Before legislating in this area, I think the committee should hold a hearing focused on the technology. Just how much resolution does location information from cell phones actually reveal? How is technology likely to change?

Such distinctions are important because mobile phone location can be determined in different ways. When investigators seek historical location data – that is, location data indicating where a phone was located at some point in the past when a crime occurred – the available information is likely to give only a very rough indication of location. In that case, the available information normally will consist only of indicating what cell towers were used to transmit calls to and from a phone in the past. So-called "cell site" information is generated because cell phones must communicate with local cell towers to transmit and receive calls: The information as to what cell towers a particular phone is communicating with gives the cellular phone provider a rough idea of the location of the phone.

Other techniques can be used to obtain more exact location information in "real time," that is, as a crime is actually occurring in the present. For example, GPS-enabled cell phones calculate location information by receiving signals transmitted from satellites in orbit. Cellular provide providers can then obtain the information received from those signals, and that information generally is much more precise than historical cell-site data. Similarly, cell phone providers normally can obtain precise information on the physical location of a cell phone in real time using methods that measure the strength and timing of communications between a particular cell phone and multiple towers. My understanding is that different telephone providers have different abilities to perform this sort of precise location determination in real time.

Given the range of different techniques that could be used to determine the location of a mobile phone, and the different resolution of the different techniques, it would be very helpful to have a hearing on the latest types of technologies and government practices. Representatives of cell phone providers can give you the most accurate sense of how their networks work and what information they can provide. Government officials can testify as to exactly how they use cellular phone location information. What are the cases? Is such information used to monitor ongoing crimes, such as monitoring a known criminal as he commits an offense? Is it used to find individuals known to have committed past crimes? Is it used to try to prove that a suspect was in a location in which a crime occurred, to rule out a potential alibi? It is hard to know the right level of protection without knowing the kinds of cases to which the new rule will be applied.

Proposal 3

> *"A governmental entity may access, or may require a covered entity to provide, prospectively or in real time, dialed number information, email to and from information or other data currently covered by the authority for pen registers and trap and trace devices only after judicial review and a court finding that the governmental entity has made a showing at least as strong as the showing under 2703(d)."*

My reaction: I agree.

Explanation: I agree that the standard for obtaining information under the pen register statute should require judicial review and should be raised to the specific and articulable facts standard used in 18 U.S.C. § 2703(d). However, I think the standard should not be higher than that. In particular, Congress should not require a warrant given that the kind of information here is non-content data rather than content data.

Proposal 4

> *"Where the Stored Communications Act authorizes a subpoena to acquire information, a governmental entity may use such subpoenas only for information related to a specified account(s) or individual(s). All non-particularized requests must be subject to judicial approval."*

My reaction: I'm certainly open to it, but it's very vague.

Explanation: I have no objections to the idea of requiring judicial review for bulk requests, but I'm not entirely sure what line the Digital Due Process coalition intends to draw with this proposal. What is the line between a "particularized" request and a "bulk" request?

For example, imagine the government seeks records of the Internet accounts assigned to a specific Internet Protocol address during a one-week period. Is that a "particularized" request or a "bulk" request? On one hand, it doesn't seem to specify the account or individual, but on the other hand it will often be the case that only one account was associated with that IP address during a one-week period. Similarly, imagine the government submits 1,000 account names and obtains a single subpoena to gather the basic subscriber information for all 1,000 accounts. On one hand, that seems to be a bulk request. On the other hand, it specifies which individual accounts will be obtained.

Greater clarity would be helpful to understand what the Digital Due Process coalition has in mind with this proposal. Further, additional hearings into the details of the investigations that prompted this proposal would be helpful. As I explained in the beginning of my testimony, Congress needs to be informed about what is actually happening "on the ground" before it can make sensible rules to govern those practices. Open hearings on the use of bulk requests to obtain identify information would give Congress a better sense of what is actually happening. This could then be used to craft the appropriate response to best balance government needs and individual privacy interests.