

Senate Judiciary Committee
Hearing on "The Electronic Communications Privacy Act: Government
Perspectives on Protecting Privacy in the Digital Age"
April 6, 2011

Questions for the Record from U.S. Senator Al Franken
for Associate Attorney General James A. Baker

- 1. You stated in your testimony that section 2702(c)(6) of the Electronic Communications Protection Act, 18 U.S.C. 2702(c)(6), may be "insufficiently protective of consumer privacy," and suggested that "Congress could consider whether this rule strikes the appropriate balance between providers and customers."**
 - a. What, if any, role does section 2702(c)(6) play in the Department of Justice's law enforcement operations?**

Proposed DOJ response:

18 U.S.C. § 2702(c)(6) allows providers to disclose records and other information "to any person *other than a governmental entity*," without limitation. 18 U.S.C. § 2702(c)(6) (emphasis added). Accordingly, providers cannot rely on subsection 2702(c)(6) when they wish to report a crime to the Department, although they can rely on this provision to provide data to foreign governments, for example. Indeed, foreign governments sometimes use this provision to obtain voluntary disclosure of information directly from U.S. providers that may be used for their own criminal investigations, because § 2702(c)(6)'s exclusion of "governmental entities" applies only to departments and agencies of the United States or any State or political subdivisions thereof. *See* 18 U.S.C. § 2711(4) (defining "governmental entity"). Section 2702(c)(6) therefore can allow foreign governments to obtain subscriber or customer records or information (but not content of communications) without the assistance of the U.S. government, which may slightly reduce the number of assistance requests that the Department of Justice receives from foreign governments.

- b. Is section 2702(c)(6) necessary for the Department of Justice's law enforcement operations?**

Proposed DOJ response:

For the reasons discussed above, 18 U.S.C. § 2702(c)(6) is not necessary for the Department of Justice's law enforcement operations.

**Written Questions of Senator Patrick Leahy,
Chairman, Senate Committee On The Judiciary
to Associate Deputy Attorney General James Baker,
Hearing On "The Electronic Communications Privacy Act:
Government Perspectives on Privacy In The Digital Age"**

CYBERSECURITY

1. One of the greatest challenges facing the Nation today is the need to develop a comprehensive national strategy for cybersecurity. A key part of that strategy will be how Congress properly balances the need for more information sharing to combat cyber threats -- within the Government, between the Government and private sector, and among members of the private sector -- with the need to protect personal privacy.

- a. Section 2702 of ECPA provides guidelines for when private companies can voluntarily share electronic communications information with the Government. How does Section 2702 impact the way the Government currently combats cybersecurity threats?**

DOJ response:

At the outset, we agree that cybersecurity is a critical challenge. As reflected in the President's 60-Day Cyberspace Policy Review, the Administration recognizes the importance of cybersecurity and the challenges we face in protecting the Nation's private sector and Government networks from an array of threats and vulnerabilities. Information sharing is a vital component of a successful cybersecurity strategy. Without a steady flow of information about rapidly evolving cyber threats and vulnerabilities, both the private sector and the Government will be ill-prepared to prevent and respond to damaging cyber incidents.

We have received anecdotal accounts from Federal incident response entities and electronic communications and remote computing service providers suggesting that ECPA's restrictions on divulging the content of and records associated with stored communications discourage private companies from sharing information that would assist legitimate governmental and private sector cybersecurity efforts.

However, some of these sorts of disclosures reportedly are not occurring even when sharing is not barred by ECPA. For example, we have been told that providers are sometimes reluctant to share non-content records pertaining to cyber threats with other non-governmental providers, even though section 2702 does not prohibit private sector sharing of non-content

records at all. Thus, it is not altogether clear that ECPA is solely responsible for the private sector's reticence. Issues such as private sector competitiveness and aversion to assuming any legal risk—no matter how remote—may also play a role.

- b. Could this provision, or other parts of ECPA, be improved to better protect cyber security?**

DOJ response:

Amendments to existing law should be made to facilitate information sharing for information used to protect against cybersecurity threats. The Administration's cybersecurity legislative package includes a proposal intended to clarify the private sector's ability to voluntarily share cybersecurity threat information; however, the proposal would amend Title VI of the U.S. Code (Domestic Security) rather than Title 18. It would lift ECPA's restrictions on information sharing between the private sector and the Government for information used to protect computers from cybersecurity threats, subject to safeguards that would protect civil liberties.

- c. Should there be different standards under ECPA for when and how private companies can voluntarily share electronic communications information about cyber threats with the Government, verses when and how such information can be voluntarily shared among members of the private sector?**

DOJ response:

Both the private sector and the Government play critical roles in cybersecurity. The private sector owns and operates the vast majority of the information systems in the United States and, accordingly, has a primary stake in addressing cybersecurity threats; however, the Government has unique incident response capabilities that may be vital to effectively attributing and neutralizing such threats and to recovery and reconstitution efforts. Moreover, to the extent that privacy concerns may be cited as a reason to distinguish between private-to-private and private-to-government information sharing regimes, we note that privacy concerns are raised by both; nevertheless, when subject to appropriate safeguards, the Nation is better situated to address cyber threats when the private sector and the Government incident response efforts are at parity and informed by similar information. While we believe strongly that we should encourage voluntary sharing by the private sector with the Government, and recognize the importance of

private-to-private sharing, it is important to note that sharing among private sector entities can raise anti-competitiveness and antitrust concerns in certain circumstances.

LOCATION INFORMATION

- 2. In 1983, the Supreme Court¹ held that the police may track suspects by using an electronic beeper without first obtaining a search warrant. Do you believe that the privacy interests implicated by the Government's use of an electronic beeper to obtain location information are different than the interests implicated when the Government obtains GPS or cell site location information, and if so, why?**

Proposed DOJ response:

The Department believes different types of location information may implicate different privacy interests. As your question notes, the Supreme Court has held that the use of a tracking device to monitor the highway movements of a vehicle does not implicate the Fourth Amendment. Similarly, the majority of courts have held that cell-phone users have no reasonable expectation of privacy in providers' historical cell-site location records, both because that information is used to provide service and is retained by wireless carriers as routine business records and because of its relative lack of precision (see response to Question 4 below).

Conversely, the Department recommends that prosecutors obtain a warrant based on probable cause before requiring providers to disclose ongoing precise location data generated using GPS technology embedded in a particular cell phone.

- 3. During the hearing, you testified that not all location information is subject to the same legal standard under ECPA, in terms of when and how the Government can obtain such information. For example, you noted that the Department's policy is to seek a search warrant in order to obtain GPS location information. But, the Department's policy is to seek a court order to obtain cell site location information. While it is true that cell site location information is somewhat less precise than GPS location data, cell site location information does provide location information that is within a very limited area around a particular cellular tower. Given this, are the privacy and law enforcement interests in cell site location information significantly different from the privacy and law enforcement interests in GPS location information, and if so, why?**

¹ *U. S. v. Knotts*, 460 U.S. 276 (1983).

Proposed DOJ response:

See the response to Question 2 above.

4. You also testified that the legal standards for obtaining location information could vary, depending upon whether an electronic communications device is being used in a Fourth Amendment-protected area, or in an unprotected area. In the case of cell site location information:

- a. Should the legal standard for the Government to obtain this information vary depending upon whether a cell phone is being used in a private, rather than public area?**

Proposed DOJ response:

As stated above, cell-site location information is information that a phone provider uses to provide service and retains in its ordinary course of business about which of its cell towers, and usually which of three pie-slice “sectors” covered by that tower, provided service to a user’s phone when the user placed or received a call, text message, or data transfer. The legal standard that the Government may use to obtain such “communication-related” cell-site location information should not depend on whether a cell phone is being used in a private, rather than a public area. First, cell-phone providers collect communication-related cell-site location information in the ordinary course of their business and rely on this information to route their subscribers’ phone communications. Because the providers collect this information in order to provide service to their subscribers, individuals who choose to use cellular phones do not have a privacy interest in this information vis-à-vis their providers, even when they are using their phones in a private space. Accordingly, no heightened legal standard is required when the government obtains cell-site information from providers about cell phones that are located in private spaces. Indeed, this comports with the rules that have long applied to the use of phones in homes. In light of the Supreme Court’s decision in *Smith v. Maryland*, 442 U.S. 735 (1979) (Fourth Amendment does not apply to collection of numbers dialed and other activity indicating use of a phone within a home) and Congress’s passage of the Pen Register statute in 1986, the same standard applies whether the phone is located inside a home or on the public street.

Second, cell-site location information is not sufficiently precise to reveal a phone’s location within a particular private space. Accordingly, based on the Supreme Court’s reasoning in *United States v. Karo*, 468 U.S. 705 (1984), the government’s collection of cell-site location information would not invade a phone user’s privacy interests, even when the phone happens to

be located in a private space, because the cell-site location information would not allow the government to know it is in any private space, let alone a particular private space.

For both of these reasons, the Department of Justice believes that the legal standard for obtaining cell-site location information should not vary depending on whether a cell phone is being used in a private area, rather than a public one.

- b. Does your answer turn on whether the Government can use the location information to track an individual in real-time, as would be the case with a GPS tracking device?**

Proposed DOJ response:

We understand this question to be asking whether the legal standard for cell-site location information should be different where the government obtains cell-site information on an ongoing basis and can use this information to monitor an individual's general but non-specific whereabouts in a continuous manner. Cell-site location information rarely, if ever, provides the government with a continuous or near-continuous stream of information about an individual's location over an extended period of time because the information stream typically available for disclosure to the government includes only the cell-site information for a limited set of events—for example, when the phone user makes or receives a phone call or sends or receives a text message. In this sense, and in others, cell-site location information is unlike the information generated by a GPS tracking device. As set forth above, cell-site location information records are generated and used by the provider in the ordinary course of its business, and they do not provide a cell phone's precise location. Therefore, the legal standard for obtaining communication-related cell-site information should not be based on whether the Government obtains cell-site information in real time.

- c. Would it matter whether the cell site location information to be obtained was historical or prospective?**

Proposed DOJ response:

The Department believes that the Fourth Amendment does not require the government to obtain a warrant for call-related cell-site location information, regardless of whether that information is historical or prospective. This conclusion is particularly clear in the case of historical cell-site location information. When the government obtains historical cell-site location information from a phone provider, it is simply obtaining business records that the provider generated and kept in the ordinary course of business. Although these records may pertain to a particular phone subscriber, that subscriber will not have seen these records [and likely will not even know the specific information they contain, though it is reasonable to expect

that they recognize such information exists as a product of the mobile nature of the service provided]. Rather, these records are simply business records of the provider that contain technical information (such as the tower used to handle a call) that the provider generated and recorded in order to route communications to and from the subscriber. A phone subscriber cannot have a reasonable expectation of privacy in these provider business records, any more than the subscriber could assert a Fourth Amendment interest in other business records that the provider generates about the subscriber for its own business purposes, such as records about the subscriber's billing history or interactions with customer service personnel. (See also response to Question 4(a) above.)

5. Today, many personal electronic devices, such as smart phones, contain GPS location technology.

- a. Is it the Department's view that the Government must obtain a search warrant in order to access location information from a smart phone or other electronic communications device that contains GPS tracking capabilities?**

Proposed DOJ response:

When the government obtains physical possession of a smart phone or other electronic communications device, the government's search of that phone must comply with the requirements of the Fourth Amendment. Because numerous courts have concluded that cell phones are closed containers, the Department of Justice recommends that the government obtain a warrant before conducting this kind of search, unless an exception to the warrant requirement (such as consent or exigent circumstances) applies. In addition, see the response to Question 2 above.

- b. Does your answer change depending upon whether the electronic communications device is being used in a private or public area?**

Proposed DOJ response:

See above.