



U.S. Department of Justice

Office of Legislative Affairs

Office of the Assistant Attorney General

Washington, DC 20530

April 5, 2011

The Honorable Patrick Leahy
Chairman
Committee on the Judiciary
United States Senate
Washington, DC 20510

Dear Mr. Chairman:

Enclosed please find responses to questions for the record arising from the appearance of Associate Deputy Attorney General James A. Baker at a hearing before the Committee on September 22, 2010, entitled "The Electronic Communications Privacy Act: Promoting Security and Protecting Privacy in the Digital Age."

We apologize for the delay and hope that this information is of assistance to the Committee. Please do not hesitate to contact this office if we may provide additional assistance regarding this, or any other matter. The Office of Management and Budget has advised us that from the perspective of the Administration's program there is no objection to submission of this letter.

Sincerely,

A handwritten signature in black ink, appearing to read "Ronald Weich".

Ronald Weich
Assistant Attorney General

Enclosure

cc: The Honorable Charles Grassley
Ranking Minority Member

**Written Questions of Chairman Patrick Leahy
to Associate Deputy Attorney General James A. Baker,
Hearing On “*The Electronic Communications Privacy Act:
Promoting Security And Protecting Privacy In The Digital Age*”
Senate Judiciary Committee
September 22, 2010**

Cell Phone Location Information

1. In September, the Court of Appeals for the Third Circuit held that the Government could be required to obtain a search warrant before it could access stored cell site location information. The court found that ECPA gives magistrate judges discretion to require a warrant issued on a showing of probable cause, or to require a lesser showing of “specific and articulable facts” that the information sought is relevant and material to an investigation. The court also noted that there is uncertainty in the law about the level of privacy protections for cell site data.
 - (a) **What is the Department’s view about the legal standards that should apply in order for the Government to access (i) stored cell site location data, (ii) GPS location data, and (iii) other mobile location information?**

Response: The Department has taken the position in federal courts that a court order under 18 U.S.C. § 2703(d), based on a showing of “specific and articulable facts,” is the appropriate means of obtaining historical cell-site location records in a criminal investigation. As for the prospective acquisition of GPS (or other similarly precise) location data concerning a wireless phone, the Department has long recommended that federal prosecutors obtain a warrant based upon probable cause. By contrast, the Department has taken the position in court that prospective acquisition of cell-site location information – which is significantly less precise than GPS data, and which does not implicate a Fourth Amendment interest – may be authorized under the authority of the pen register and trap and trace statute in tandem with 18 U.S.C. § 2703(d).

- (b) **Should Congress clarify these standards under ECPA, and if so, how?**

Response: The Administration has not come to any conclusions about particular amendments to ECPA. However, the Department believes that clarifying amendments could be beneficial, provided that they do not imperil public safety or otherwise impair the current ability of prosecutors and agents to obtain such non-content information, including at the preliminary stages of an investigation.

Email Storage

2. ECPA extends greater privacy protections to emails that are stored for less than 180 days, than for emails that are stored for a longer period. When Congress enacted this provision, most experts believed that an email, once sent, would be deleted. But, today, storing email for extended periods of time is very common

and there are even new technologies, like cloud computing, that allow users to store mails remotely for years.

(a) How does the distinction regarding the age of stored email impact the Department's ability to acquire evidence in criminal matters?

Response: Under 18 U.S.C. § 2703(a), the government can compel disclosure from a provider of an electronic communication service of electronic communications (such as email) in electronic storage for less than 181 days only pursuant to a warrant. The government can compel disclosure of other communications using a warrant, 2703(d) order, or subpoena. If the government uses a 2703(d) order or subpoena, it must give prior notice to the customer or subscriber. Such notice may be delayed under 18 U.S.C. § 2705 if there is reason to believe that prior notification would cause intimidation of witnesses, destruction of evidence, or other similar harm to an investigation.

The standard for obtaining email is significant because in many cases, investigators may have strong evidence that a target is engaged in serious criminal activity, and they may know that the target uses a particular email account, but they may lack evidence tying the email account to the criminal activity. For example, investigators might know that an individual who engaged in fraud schemes through two Hotmail email accounts also used a third Hotmail account, but they may lack sufficient information linking the third account to the known fraud schemes to obtain a warrant. Or investigators might know that an individual produced child pornography on his home computer and downloaded child pornography from the Internet, but they might still lack sufficient information linking this conduct to the individual's Yahoo! email account to obtain a warrant. In such circumstances, investigators may be able to use a subpoena or 2703(d) order to acquire certain stored email.

(b) Does this distinction make sense and should Congress consider changing, or eliminating this distinction?

Response: The Administration has not come to any conclusions about particular amendments to ECPA. However, any alteration to the current legal framework should take into account the variety of communication and storage services used today, from webmail to corporate mail, from private bulletin boards to social networking sites to public blogs. Access to information from these services is critical to the success of criminal cases. Thus, before requiring a warrant for any particular class of electronic evidence, it is important to consider how such a requirement might play out in practice.

For example, law enforcement needs tools to investigate and build cases in early stages in order to develop probable cause. Allowing the acquisition of certain types of content -- with process short of a warrant but with appropriate additional safeguards -- can fill this role. In addition, imposing a warrant requirement on compelled production of the contents of communications would cause significant problems in the corporate email context. Currently, if a corporation is suspected of involvement in illegal activities (for example, fraud, antitrust violations, or environmental crimes), the government may subpoena relevant documents from the corporation.

If a warrant requirement were imposed on compelled production of email, the corporation could shelter incriminating documents from subpoena merely by storing them as email or attachments to email. Furthermore, a warrant requirement would also substantially burden investigative agencies, such as the FTC and SEC, that lack authority to obtain search warrants.

Section 2709

3. The Department of Justice recently proposed that Congress amend Section 2709 of ECPA to make it easier for the FBI to obtain Americans' electronic communications transactional records. **How does the Department's proposal address and protect Americans' privacy rights and civil liberties?**

Response: The proposal does not change the way the FBI obtains electronic communication transactional records of Americans. The proposed amendment to 18 U.S.C. § 2709(b)(1) to include the phrase "electronic communications transactional records" is intended by the Department as a technical fix to ensure consistency between the types of records National Security Letter (NSL) recipients are required to provide to the FBI under 18 U.S.C. § 2709(a) and the types of records that are subject to the procedural protection of an FBI certification of relevance pursuant to 18 U.S.C. § 2709(b)(1). Without the proposed fix, the statute is ambiguous. The Department is prepared to discuss other language to remove that ambiguity, so long as it preserves the FBI's ability, consistent with constitutional and statutory rights, to obtain permitted electronic communications transactional records.

The Department and the FBI take seriously the privacy rights and civil liberties of Americans. We have robust policies, procedures and oversight in place to ensure that protection of privacy rights and civil liberties is carefully balanced with the FBI's need to obtain information in support of our predicated national security investigations to protect Americans from terrorist attacks and other threats to the national security.

ECPA Reform

4. During the hearing, you testified that while the Department is currently reviewing ECPA, it is not yet prepared to provide any recommendations to Congress on updating this important law. I advised that the Committee will be moving forward with its work to update this law and urged the Department to promptly get its recommendations to the Committee. **When will the Department provide its recommendations to the Committee on reforms to ECPA?**

Response: The Department and the Administration are working expeditiously on formulating recommendations for ECPA reform, but at this point we cannot provide a certain date for when we will submit these recommendations.

Questions submitted by U.S. Senator Arlen Specter
to Associate Deputy Attorney General James A. Baker

5. Mr. Baker, in April I introduced the Surreptitious Video Surveillance Act of 2010 (S. 3214) to require any governmental entity conducting video or still surveillance *within a residence* to seek a warrant. Title III of the Omnibus Crime Control and Safe Streets Act, known as the federal Wiretap Act, does not forbid video surveillance or require a warrant. Do you support the legislation's effort to codify a warrant requirement for in-home surveillance? Will you undertake to expeditiously provide comments on the legislation?

Response: The Department appreciates the important privacy concerns S.3214 seeks to address, and we will be happy to provide formal comments on the legislation. As a practical matter, it is noted that extensive federal court precedent already imposes stringent controls on law enforcement use of surreptitious video surveillance to monitor activity in private areas. In addition, video surveillance does not squarely fit within the framework of the Wiretap Act, which regulates the "interception" of "communications" between and among "parties," because video surveillance does not involve communications between parties. Thus, it is unclear how the provisions of Title III would apply to video surveillance, or why including such surveillance within the Wiretap Act is practically necessary.

6. Mr. Baker, you testified that the Electronic Communications Privacy Act (ECPA) is a vital tool for the law enforcement community. How does ECPA assist investigations?

Response: Law enforcement officials rely on ECPA to further important investigations, solve crimes, and apprehend criminals. Criminals involved in terrorism, drug trafficking, violent crime, kidnappings, computer hacking, sexual exploitation of children, organized crime, gangs, and white collar offenses use email, cell phones, and the Internet in furtherance of their offenses, and network service providers retain information critical to solving these crimes. ECPA process is used regularly by the Department of Justice in investigations of all of these types of crime.

Investigators use ECPA to obtain both content and non-content information from service providers. The content of a communication, such as a voice mail or the subject line and body of an email, is often direct evidence of crime. Non-content information associated with a communication can show investigators with whom a subject communicates, at what time, for how long, and it can provide information about the location of a criminal. Such non-content

information - generally available with a lower evidentiary threshold - is a critical building block in investigations and can lead to the development of probable cause to arrest a criminal and search for evidence.

**Questions Submitted by U.S. Senator Russell D. Feingold
to Associate Deputy Attorney General James A. Baker**

7. At a May 5, 2010, hearing of the House Judiciary Subcommittee on the Constitution, Civil Rights, and Civil Liberties, service provider attorney Albert Gidari submitted written testimony that stated the following with regard to government requests for information in criminal investigations:

The following issues are faced by service providers every day in response to government demands for acquisition and use of location information:

d. Target v. Associates (hub and spokes). Regardless of the legal standard applicable to the target phone, what standard applies to obtain the location information for all those with whom the target communicates? It is common in hybrid orders for the government to seek the location of the community of interest - that is, the location of persons with whom the target communicates.

- a. Do federal prosecutors obtain location information about groups of individuals that include individuals that are not suspected of any crime, such as all individuals who communicate with a particular suspect?
- b. If so, what legal theory does it rely on? How frequently is this technique employed?

Response: Federal prosecutors may on occasion have a need to obtain information about wireless telephones carried by individuals not suspected of crimes, where that information may nevertheless be relevant in a criminal investigation. For instance, a fugitive may be known to be

traveling with a family member or other companion carrying a known wireless phone; in such circumstances, determining the location of the companion's phone would be an appropriate means of locating the fugitive.

Regarding "community of interest" location information – as described above, the location of all phones in contact with an identified target phone – we do not believe federal prosecutors seek such prospective "hub and spoke" information with any degree of regularity. For the government to obtain this information, it would have to meet the statutory threshold ("specific and articulable facts" for cell-site information and probable cause for GPS information) for each device it was seeking information about. Meeting this burden would be difficult in practice.

However, there may be some circumstances in which such orders are appropriate. Consider, for example, an investigation in which law enforcement knows that members of a narcotics ring use prepaid cell phones to communicate exclusively with other members of the ring regarding their narcotics enterprise. Under such circumstances, once law enforcement becomes aware of the phone number for a cell phone in current use by the ring, it is appropriate to seek an order to obtain location information for all cell phones in contact with the known phone. If the ring members replace their prepaid phones frequently (as is often the case), requiring law enforcement to obtain an initial order and then subsequent follow-up orders could substantially impede the investigation.

8. **As I understand it from the hearing testimony, the Justice Department believes that in a criminal investigation to obtain retrospective cell-site location information, it should seek a court order under 18 U.S.C. 2703(d); to obtain prospective cell-site location information, it should seek a 'hybrid' court order under 18 U.S.C. § 2703(d) and the pen register/trap and trace statute; and to obtain prospective GPS-based location information, it should seek a probable cause search warrant.**

a. Is this accurate?

Response: Yes.

b. Do all U.S. Attorney's offices follow these standards?

Response: As a result of local rulings, in a number of districts federal prosecutors obtain prospective cell-site information only pursuant to a search warrant. In addition, United States Attorneys' Offices follow local court guidelines to obtain prospective GPS data from service providers.

c. With respect to investigations conducted under the Foreign Intelligence Surveillance Act, what type(s) of legal process does the Justice Department seek to obtain these types of location information?

Response: CLASSIFIED (being transmitted separately)

9. Please specify how many federal courts of appeals have issued rulings on government access to the types of location information described in Question 2 and what legal process they have held the government must obtain.

Response: To date, only one federal court of appeals has addressed the issue of cell site location information. In a recent decision, the Third Circuit Court of Appeals held that retrospective cell-site location information "is obtainable under a [Title 18, United States Code] § 2703(d) order and that such an order does not require the traditional probable cause determination." *In re Application Of The United States Of America For An Order Directing A Provider Of Electronic Communication Service To Disclose Records To The Government*, No. 08-4227 (3d Cir. Sept. 7, 2010). At the same time, however, the court also held that the statute "gives the [magistrate judge] the option to require a warrant showing probable cause ... although it is an option to be used sparingly" Pineda-Moreno, Maynard, and similar decisions relate strictly to the use of GPS tracking devices installed by the government. Because the question in context calls for information about court decisions involving wireless location data obtained from service providers (and because ECPA, the subject of the hearing, does not impose restrictions on the use of such devices), the omission is intentional and appropriate.

10. Please specify how many federal district courts have issued rulings on government access to the types of location information described in Question 2 and what legal process they have held the government must obtain. If judges within a particular district court have come to different conclusions with regard to the same type of location information, please so indicate.

Response: The number of district courts (including both district judges and magistrate judges) issuing written opinions on the procedures for obtaining cell phone location information are listed below. With respect to all three categories of information described below, we note that these figures present a skewed picture of the practice in most federal districts, as many judges regularly grant the Department's applications -- and thus implicitly endorse our legal positions -- without issuing written opinions.

Retrospective cell-site location information

Judges and magistrate judges in five different federal districts have issued written opinions expressly upholding the use of a court order under 18 U.S.C. § 2703(d) to obtain historical cell-site location records. (This includes two cases in which district court judges reversed magistrate judges on appeal.) Judges in two additional districts have endorsed this approach in dicta. In two other districts, courts have rejected the government's approach and demanded a warrant; one of these decisions, however, was vacated by the recent Third Circuit decision discussed in the response to Question 3 *supra*.

Courts in three additional districts have reached internally conflicting decisions. In the Northern District of Indiana, one court has without analysis denied a government application under 18 U.S.C. § 2703(d) and demanded a warrant; more recently, a different judge in the same district denied a defendant's motion to suppress historical cell-site location records, holding that such records are not protected by the Fourth Amendment. In the Southern District of Texas, a district court judge has approved the use of a court order under 18 U.S.C. § 2703(d) to obtain historical cell-site location records; however, a magistrate judge recently denied such an application and demanded a warrant, reversing his previous policy of approving section 2703(d) orders for these types of records. Finally, a magistrate judge in the Eastern District of New York has held that 18 U.S.C. § 2703(d) on its face allows the government to obtain such records, but that the Fourth Amendment nevertheless requires a warrant.

Prospective cell-site location information

Judges and magistrate judges in five different federal districts have issued written opinions expressly upholding the use of a court order under the pen register and trap and trace statute, in tandem with 18 U.S.C. § 2703(d), to obtain prospective cell-site location information. (This includes two district court judges who reversed magistrate judges on appeal.) In twelve other

districts, courts have rejected this so-called “hybrid” approach and demanded a warrant. We note that in several of these cases, the courts reaching this conclusion have conflated cell-site location information with more precise GPS (or similar) location information.

Courts in two districts have reached internally conflicting decisions. In the Southern District of New York, two judges have endorsed the “hybrid” theory, and two others have rejected it. Similarly, in the Eastern District of New York two district court judges have upheld the Department’s approach – in each case reversing a magistrate judge – while one district court judge has rejected it, as one magistrate judge continues to do despite his reversal by the district court.

Prospective geolocation information (GPS or other method)

Courts in two different districts have issued written opinions expressly upholding the use of a search warrant based on probable cause to obtain prospective geolocation information (such as GPS or similarly precise information) concerning a criminal suspect’s wireless phone. In a third district, one district court judge has adopted this view, while a magistrate judge has held that in the special case of fugitives the proper authority is an order under the All Writs Act in aid of a pre-existing arrest warrant. Despite reversal of that decision by the District Court, this Magistrate Judge has reasserted the same view in a subsequent opinion.

11. As was discussed at the hearing, the statutory protection afforded to the contents of an electronic communication depends (among other things) on whether it is stored or in transit, whether it is more than 180 days old, and whether the recipient has opened it.

- a. In 2007, 2008 and 2009, how many times did the Department of Justice and/or Federal Bureau of Investigation obtain a court order issued pursuant to 18 USC § 2703(d) for the contents of electronic communications?**

Response: The Department of Justice does not keep records regarding how frequently legal process under 18 U.S.C. § 2703 is used.

- b. In 2007, 2008 and 2009, how many times did the Department of Justice and/or Federal Bureau of Investigation issue a subpoena for the contents of electronic communications? In these cases, how many times was notice delayed pursuant to 18 U.S.C. § 2705?**

Response: The Department of Justice does not keep records regarding how frequently legal process under 18 U.S.C. § 2703 is used.

12. What statutory authority does the Justice Department use to obtain content from a website that allows users to store and share photographs?

Response: If the government sought to compel disclosure of photographs from a website that allows users to store and share photographs, such activity would be covered by 18 U.S.C. § 2703(a) and (b). Under § 2703(a), the government may compel disclosure of the content of communications in electronic storage in an electronic communications service for 180 days or less only pursuant to a search warrant. Under § 2703(b), the government may compel disclosure of other communications stored by a remote computing service using a warrant, a 2703(d) order, or a subpoena. When the government uses a subpoena or 2703(d) order, it must provide prior notice to the subscriber or customer. That notice may be delayed if authorized under 18 U.S.C. § 2705 if there is reason to believe that prior notification would cause intimidation of witnesses, destruction of evidence, or other similar harm to an investigation.

A website that allows users to store and share photographs may voluntarily disclose content to the government under the circumstances set forth in 18 U.S.C. § 2702(b). For example, a voluntary disclosure is permissible in “an emergency involving danger of death or serious physical injury to any person” that “requires disclosure without delay of communications relating to the emergency.” 18 U.S.C. § 2702(b)(8)

13. When Justice Department lawyers apply for a court order to install or use a pen register and/or trap and trace device pursuant to 18 U.S.C. § 3121 *et seq.*, do they commonly include in the application a statement of facts explaining why the information likely to be obtained is relevant to an ongoing criminal investigation?

Response: Practice in this area varies according to local custom. In some districts, prosecutors do include a factual statement; in other districts, prosecutors provide the certification required by the statute, without additional factual recitation.

14. What specific types of information does the Federal Bureau of Investigation seek and obtain today with a national security letter issued pursuant to 18 U.S.C. § 2709 for “electronic communications transactional records”?

Response: Generally, the types of electronic communications transactional records (ECTRs) sought and obtained from electronic communications service providers (ECSPs) are: the name, physical address, e-mail address, account number, or other identifying information for a person or entity involved in an electronic communication; the Internet Protocol (IP) address or other network address, including any temporarily assigned IP or network address, for a computer involved in an electronic communication; the period of usage, session time, and the communication routing or transmission information for an electronic communication; the length of the service (including the start date) and types of service utilized by a person or entity involved in an electronic communication; the methods and sources of payment for such service (including any credit card or bank account number); and the means used to access an electronic communication service or account. In late 2009, however, one ECSP stopped providing ECTRs in response to National Security Letters (NSL) issued by the FBI pursuant to 18 U.S.C. § 2709. In late 2010, two other ECSPs also stopped providing ECTRs in response to NSLs issued by the FBI pursuant to 18 U.S.C. § 2709.

15. What specific types of information did the Federal Bureau of Investigation seek and obtain prior to November 5, 2008, with a national security letter issued pursuant to 18 U.S.C. § 2709 for “electronic communications transactional records”?

Response: The types of ECTRs sought by the FBI with NSLs today are the same as were sought and obtained prior to November 5, 2008, namely: the name, physical address, e-mail address, account number, or other identifying information for a person or entity involved in an electronic communication; the Internet Protocol (IP) address or other network address, including any temporarily assigned IP or network address, for a computer involved in an electronic communication; the period of usage, session time, and the communication routing or transmission information for an electronic communication; the length of the service (including the start date) and types of service utilized by a person or entity involved in an electronic communication; the methods and sources of payment for such service (including any credit card or bank account number); and the means used to access an electronic communication service or account.