KEEPING THE INTERNET
OPEN • INNOVATIVE • FREE

www.cdt.org

CENTER FOR DEMOCRACY
& TECHNOLOGY

1634 I Street, NW
Suite 1100
Washington, DC 20006

P +1-202-637-9800
F +1-202-637-0968
E info@cdt.org

ANALYSIS OF DEPARTMENT OF JUSTICE MARCH 19, 2013 ECPA TESTIMONY

April 8, 2013

In recent testimony, the Justice Department came close to endorsing an important reform of the Electronic Communications Privacy Act. However, the DOJ also suggested other changes that would go in the opposite direction, expanding the power of federal regulatory agencies and weakening privacy protections that have been on the books for two decades.

In testimony before the House Judiciary Crime Subcommittee on March 19, the Justice Department acknowledged that it is time for Congress to update the rules under which government agencies compel service providers to disclose email and other private documents stored online on behalf of their customers.[1] DOJ came very close to endorsing a reform that is widely supported, which is to uniformly apply the Constitution's warrant standard to all private electronic communications and other documents stored online for third parties. We applaud the Department for this important step.[2] However, the Department also raised three troubling proposals that would weaken current privacy protections:

- Expanding the power of regulatory agencies;
- Lowering the standard for government access to data about Internet communications;
- Limiting the role of the courts in issuing "2703(d) orders."

I. A major step forward: Extending the warrant requirement to all content stored online

DOJ cited a provision of the Electronic Communications Privacy Act of 1986 (ECPA) that allows the use of a subpoena, issued without the approval of a judge, to compel service providers to disclose email stored for their customers that is older than 180 days even though the statute requires a warrant to compel service providers to disclose email that is less than 181 days old. In its testimony, the DOJ said for the first time that there is "no principled basis to treat

[1] http://judiciary.house.gov/hearings/113th/03192013_2/Tyrangiel%2003192013.pdf.

[2] The warrant standard is supported by a wide coalition of leading Internet and communications companies, advocacy groups across the political spectrum, think tanks, and academics. See http://www.digitaldueprocess.org and http://digital4th.org.

email less than 180 days old differently than email more than 180 days old."[3] Likewise, referring to the theory that email loses the protection of the warrant as soon as it is opened, the Department said, "Similarly, it makes sense that the statute not accord lesser protection to opened emails than it gives to emails that are unopened." The DOJ went on to essentially endorse the warrant standard:

> "Some have suggested that the best way to enhance privacy would be to require law enforcement to obtain **a warrant based on probable cause** to compel disclosure of stored email and similar stored content information from a service provider. **We appreciate the appeal of this approach and believe that it has considerable merit**, provided that Congress consider contingencies for certain, limited functions for which this may pose a problem." (Emphasis added.)

We welcome the DOJ's statements acknowledging that a warrant should be required for government investigators to compel disclosure by service providers of email and other content stored online, regardless of how old it is (subject, of course, to emergency and consent exceptions already in the statute). Such a reform of ECPA would support ongoing innovation, cure the Constitutional defect identified by the Sixth Circuit, give certainty and clarity to federal, state, and local law enforcement agencies, and clear up some of the ambiguity in the statute that courts have long complained of. [4]

We want to especially note that, when the DOJ referred to "similar stored content information from a service provider," its statement should be read, in our view, as referring to all content stored by a service provider on behalf of third party users, including text messages, other instant messages, voicemails, private tweets, and private messages on social networking sites, as well as documents and other content stored on a cloud server.

However, despite its recognition that ECPA needs to be updated to protect privacy, the DOJ went on to discuss possible statutory changes that would take the law in the opposite direction, expanding the power of regulatory agencies and providing less protection for certain data than under ECPA's current rules.

---

[3] DOJ did not say so explicitly in its testimony, but the logic of its statement also applies regardless of whether a private document is stored by a third party provider acting as an "electronic communication service provider" or as a "provider of remote computing service." Under current law, for example, a link in an email to a document stored online is protected if the email is less than 181 days old, but DOJ argues that, under ECPA, the document itself when held by a third party provider of remote computing service can be obtained without a warrant the instant it is created in the cloud. These distinctions no longer make sense.

[4] In 2010, the Sixth Circuit held that the Constitution requires a warrant for government access to email, regardless of whether it is more than 180 days old or less, and that ECPA is unconstitutional to the extent that it authorizes the government to demand access from service providers with less than a warrant. *United States v. Warshak*, 631 F.3d 266 (6th Cir. 2010). Leading Internet companies, including Google, Facebook, Microsoft, Twitter and Yahoo!, have all announced that they follow the *Warshak* rule nationwide and require warrants for content, and it is our understanding that federal prosecutors and probably many local prosecutors already get warrants for content.

II. A major step backwards: Expanding the power of regulatory agencies?

We turn now to the areas of concern in DOJ's testimony. In what would be a sweeping proposal, the DOJ seemed to suggest expanding the authority of regulatory agencies to obtain email and other private documents with subpoenas served on an entity providing communications services or data storage services to third parties. The DOJ's testimony on this point was very ambiguous, but we want to alert policymakers and stakeholders to the potential implications of the DOJ's testimony.

DOJ devoted a large part of its testimony to describing the work of regulatory agencies and the importance of electronic evidence to their investigations. However, DOJ never acknowledged that, under current law, regulatory agencies cannot require service providers to disclose the contents of email less than 181 days old. Instead, ECPA already requires that regulatory agencies, to obtain fresh evidence in civil matters, must serve subpoenas directly on the target of their investigation (or on other persons or entities that sent or received the messages rather than the third party operator of the email or cloud storage service). By citing successful regulatory investigations under the current rule, the DOJ indirectly admitted that agencies function very effectively by serving subpoenas directly on the targets of their investigations (or other "first" parties), as they always have, dating back before the Internet.

Consistent ECPA reform would make it clear that all subpoenas for material covered by ECPA should be served on the parties that created or received the communications, not on the third parties that provide transit or storage services. However, instead of acknowledging that the current rule for how administrative agencies access newer email should also apply to how they access other private or proprietary documents stored online, the DOJ raised some concerns about the current rule and about the implications of a uniform rule for warrants and subpoenas. As we explain below, many of the DOJ's specific concerns can already be addressed under current law or are addressed in the leading ECPA reform proposal in the Senate. However, at times, the DOJ seemed to be suggesting that the "unprincipled" distinctions in current law (allowing subpoenas for some but not other content) should be retained as they relate to administrative agencies. At other times, DOJ seemed to go even further to imply a very far-reaching change in law: that Congress should *lower* the standard in current law, allowing regulatory agencies to by-pass the targets of their investigations and use subpoenas to require service providers to disclose confidential documents stored on behalf of their customers.

Whether the DOJ was proposing only to preserve the 180-day rule for regulatory agencies or going further to suggest lowering the standard for accessing more recent material, its position would be untenable. Administrative agencies, which can conduct wide-ranging investigations without specific suspicion of wrongdoing,[5] should not have *more* power than law enforcement agencies, which are at least subject to limits on their ability to open investigations and on the scope of their investigations.

[5] The regulatory "power of inquisition," the Supreme Court has said, "is not derived from the judicial function. It is more analogous to the Grand Jury, which does not depend on a case or controversy for power to get evidence, but can investigate merely on suspicion that the law is being violated, or even just because it wants assurance that it is not. When investigative and accusatory duties are delegated by statute to an administrative body, it, too, may take steps to inform itself as to whether there is probable violation of the law." *U.S. v. Morton Salt*, 338 U.S. 632, 642-43 (1950).

Within the federal government alone, there are hundreds of agencies that have subpoena power.[6] An even larger number of state and local regulatory agencies have subpoena power.[7] Allowing regulatory agencies to serve subpoenas on service providers for the content created by third parties would diminish privacy, threaten proprietary information, and impose an immense burden on those service providers.

The most obvious problem with allowing agencies to serve civil subpoenas on service providers is that it would eviscerate the warrant protection on the criminal side, because existing rules allow information to be shared readily from civil investigators to their criminal counterparts.[8] For example, Form 1662 of the Securities and Exchange Commission, http://www.sec.gov/about/forms/sec1662.pdf, which is designed to be used with all SEC civil subpoenas, expressly states:

> "The Commission often makes its files available to other governmental agencies, particularly United States Attorneys and state prosecutors. There is a likelihood that information supplied by you will be made available to such agencies where appropriate. Whether or not the Commission makes its files available to other governmental agencies is, in general, a confidential matter between the Commission and such other governmental agencies."

A second and related major problem is that serving administrative subpoenas on service providers instead of on the individuals or entities that actually created or were the recipients of the content will result in inefficiencies and overproduction of private and proprietary data not relevant to the governmental investigation. When a subpoena is served directly on the target of investigation or on an entity that created any relevant material, the target or other first party is responsible for identifying documents relevant to the inquiry wherever they may be stored and in whatever format, assembling them, segregating those that are privileged, and disclosing to the government those that are relevant. It is most efficient for the target to identify and compile responsive documents whether they are stored in file cabinets on site, in off-site storage, on the company's local network, or on the network of its cloud provider.

On the other hand, if subpoenas were instead served on service providers, all of this careful vetting and compiling of data would go out the window. Service providers could not know what is relevant to an investigation and what is not, and what is privileged and what is not, and they

---

[6] A wide range of federal agencies have the power to issue subpoenas without approval of a judge. See U.S. Department of Justice, "Report to Congress on the Use of Administrative Subpoena Authorities by Executive Branch Agencies and Entities," http://www.justice.gov/archive/olp/rpt_to_congress.pdf (identifying approximately 335 subpoena authorities held by various executive branch entities under current law).

[7] See, for example National District Attorneys Association, "Administrative Subpoena Authority" (September 20111) http://www.ndaa.org/pdf/Administrative%20Subpoena%20Compilation.pdf (compiling state subpoena authorities in welfare cases).

[8] The Supreme Court held in *United States v. Kordel*, 397 U.S. 1 (1970), that evidence gathered by the government in a civil case may be used also in a criminal proceeding, provided that the government does not act in bad faith. In *United States v. Stringer*, 521 F.3d 1189 (9th Cir. 2008), the Ninth Circuit held that information subpoenaed by the Securities and Exchange Commission (SEC) in a civil proceeding could be used in criminal proceedings brought by either the SEC or another government agency. The court noted that Congress has expressly authorized the SEC to take information it obtained with a subpoena and share it with the Department of Justice to facilitate the investigation and prosecution of crimes. See 15 U.S.C. §§ 77t(b), 78u(d).

should not be put in the position of having to decide. Instead, because there is no practical alternative, service providers would be forced to overproduce, turning over to the government all of the target's documents whether or not they are relevant. This might include personal emails an employee may have exchanged with his spouse, trade secrets, and correspondence with company lawyers. Especially in the age of cloud storage, this could result in huge amounts of irrelevant but sensitive data being disclosed to the government.

Recognizing these risks and inefficiencies, in civil proceedings the courts have consistently ruled that civil subpoenas for email and other content stored in the cloud should be served directly on the party that sent or received the email or created the content.[9] The ECPA reforms in the leading Senate bill, S. 607, would preserve that approach. ECPA reform under S. 607 would also preserve current rules allowing administrative agencies to use subpoenas to compel service providers to disclose subscriber identifying information. This allows for a logical use of the building blocks of civil investigations: subpoenas served on service providers to disclose any identifying information about their subscribers and users and then subpoenas served on those subscribers and users to actually obtain the content.

As we suggested above, some of the concerns DOJ raised in connection with regulatory investigations are already resolved in current law or would be addressed in pending ECPA reform legislation:

- **DOJ raised the concern that "many individuals who violate the law may be tempted to destroy their communications rather than turn them over."**

  This concern is already addressed and solved in ECPA. Section 2703(f) authorizes any governmental entity, including a regulatory agency with only civil enforcement powers, to require any service provider, upon mere request of the government agency, to preserve any records or other evidence in its possession pending the issuance of a court order or other process. With this authority, a regulatory agency or any other governmental entity can ensure that records are not destroyed by the subject of an investigation while subpoenas are being issued to the subject of the investigation and enforced.

  If subpoenaed materials are destroyed (in what is traditionally called "spoliation"), the courts and regulatory agencies can apply age-old sanctions, including inferring that the

[9] *Flagg v. City of Detroit,* 252 F.R.D. 346 (E.D. Mich. 2008) (finding that a Rule 34 request for production of documents served on a party for any materials in is custody *or control* was the "more straightforward path" to discovery of messages stored by a service provider). See also *O'Grady v. Superior Court,* 139 Cal. App. 4th 1423 (2006) http://www.internetlibrary.com/pdf/OGrady-Apple-Cal-Crt-App.pdf:

> "Congress could reasonably conclude that to permit civil discovery of stored messages from service providers without the consent of subscribers would provide an informational windfall to civil litigants at too great a cost to digital media and their users. Prohibiting such discovery imposes no new burden on litigants, but shields these modes of communication from encroachments that threaten to impair their utility and discourage their development. … In other words, Congress could quite reasonably decide that an email service provider is a kind of data bailee to whom email is entrusted for delivery and secure storage, and who should be legally disabled from disclosing such data in response to a civil subpoena without the subscriber's consent. This does not render the data wholly unavailable; it only means that the discovery must be directed to the owner of the data, not the bailee to whom it was entrusted."

information was harmful to the party that caused it to be destroyed. "Potential sanctions for spoliation include: dismissal of a claim or granting judgment in favor of a prejudiced party; suppression of evidence; an adverse inference, referred to as the spoliation inference; fines; and attorneys' fees and costs."[10]

- **DOJ said in its testimony that reform efforts "must account for existing practices as to entities, such as corporations, that provide email to their employees."**

  This concern is addressed and solved in the Leahy-Lee bill, S. 607, which was introduced after the DOJ testimony was submitted. The Leahy-Lee bill makes it clear that nothing in ECPA limits the authority of a government agency to use a subpoena to demand records from a corporation that provides email to its employees.

- **DOJ expressed concern about cases in which "the subscriber no longer exists – as in the case of a bankrupt corporation."**

  Again, the problem is already addressed under current law. In Chapter 7 and Chapter 11 bankruptcies, the bankruptcy trustee acquires control over all the assets of the bankrupt entity and has full power to access the email accounts of the bankrupt corporation and to comply with any subpoenas for email or documents stored electronically by the bankrupt entity.[11]

- **DOJ said in its testimony that Congress should consider ensuring that "courts treat civil discovery subpoenas just like they already treat grand jury subpoenas, trial subpoenas, and administrative subpoenas."**

  This concern is addressed and solved in the Leahy-Lee bill, which adds civil discovery subpoenas to the list of subpoenas that can be used to compel disclosure of subscriber identifying information, placing all subpoenas on the same footing and likewise placing governmental and non-governmental parties on the same footing.

Bottom line: Under the ECPA reform proposed in S. 607, government agencies could still serve a subpoena on the creator (or recipient) of the email or other content it seeks. Paper documents and electronic documents whether stored remotely or locally would all be treated the same.

---

[10] *Gatto v. United Airlines et al*, Civil Action No. 10-cv-1090-ES-SCM, 2013 U.S. Dist. LEXIS 41909 (D.N.J, March 25, 2013) (after plaintiff was ordered by the court to grant defendants access to his Facebook account, he deleted the account; court approved an instruction to the jury that it could draw an adverse inference from the plaintiff's actions).

[11] As the Supreme Court said in *Commodity Futures Trading Comm. v. Weintraub,* 471 U.S. 343, 352-53 (1985), "The powers and duties of a bankruptcy trustee are extensive. Upon the commencement of a case in bankruptcy, all corporate property passes to an estate represented by the trustee. … Moreover, in reorganization, the trustee has the power to 'operate the debtor's business' unless the court orders otherwise. … Even in liquidation, the court 'may authorize the trustee to operate the business' for a limited period of time. … [I]t is clear that the trustee plays the role most closely analogous to that of a solvent corporation's management." In Weintraub, the Court held that the bankruptcy trustee has the power to waive the attorney-client privilege of the corporation. Surely, the trustee also has the power to turn over corporate email in response to a subpoena (and to waive or assert any privileges in those records on behalf of the corporation).

III. Lowering the standard for government access to data about Internet communications

The Justice Department would like to roll back the standard established in 1994 for government access to Internet transactional data.

Under current law, the government can use a subpoena to require a service provider to disclose certain basic information:

- the name and address of a subscriber or customer of a communications service;
- the types of service used and the start and end dates showing when the services were subscribed to or used;
- specific session times and duration, such as when the person logged in and for how long;
- other identifying information, such as the IP address assigned to a user at a specific time;
- billing information, including any credit card number used to pay for the service.

These items of information are considered to be less sensitive than the contents of communications, but they can be of great help to law enforcement in the early phases of an investigation. For example, they allow the government to identify persons in communication with a suspected criminal whose communications are being monitored, and they can help identify the sender of a particular piece of content the government has obtained. ECPA reform based on the principles recommended by Digital Due Process (www.digitaldueprocess.org) and supported by Digital 4th (www.digital4th.org) would not change the rule requiring disclosure of this information with a subpoena. Likewise, the current rule would be unaffected by the Leahy-Lee bill, S. 607, or the Lofgren-Poe-DelBene bill, H.R. 983.

Traditionally, government agents have also been able to use subpoenas to compel telephone companies to disclose call detail records – records collected by phone companies for billing or other purposes showing who called whom and when. This information is clearly more sensitive than the other subscriber data available with a subpoena,[12] and the government must obtain a court order in order to intercept such information in realtime. ECPA reform based on the principles recommended by Digital Due Process and supported by Digital 4th would not change the rule allowing access to stored telephone dialing records with a subpoena. Nor would the Leahy-Lee bill, S. 607, or the Lofgren-Poe-DelBene bill, H.R. 983.

However, it has long been recognized that "the acquisition of source and destination information concerning electronic communication reveals more about the contents of the communications than a phone number reveals about the contents of a telephone call."[13] Some have argued that

[12] Calling patterns can reflect a person's associations and interests, implicating not only privacy but also First Amendment rights. See Susan Freiwald, "Uncertain Privacy: Communications Attributes after the Digital Telephony Act," 69 S. Calif. L. Rev. 949 (1996)(as a result of changing technology, "disclosure of communication attributes presents an extremely intrusive view into people's private lives").

[13] Patricia Bellia, "Surveillance Law through Cyberlaw's Lens," George Washington Law Review, Vol. 72 (2004), at 55.

the content/non-content distinction is so inapplicable to Internet communications that Internet transactional data should be available to the government only with a warrant.[14]

In 1994, when Congress was considering CALEA, concerns were raised about the richness of the transactional data associated with Internet communications.[15] Congress responded by adopting the standard currently in 2703(d). The House Judiciary Committee said this about the provision in its report:

> "Recognizing that transactional records from on-line communication systems reveal more than telephone toll records or mail covers, subsection (a) eliminates the use of a subpoena by law enforcement to obtain from a provider of electronic communication services the addresses on electronic messages. In order for law enforcement to obtain such information, a court order is required.
>
> "This section imposes an intermediate standard to protect on-line transactional records. It is a standard higher than a subpoena, but not a probable cause warrant. The intent of raising the standard for access to transactional data is to guard against "fishing expeditions" by law enforcement. Under the intermediate standard, the court must find, based on law enforcement's showing of facts, that there are specific and articulable grounds to believe that the records are relevant and material to an ongoing criminal investigation.
>
> "Law enforcement could still use a subpoena to obtain the name, address, telephone toll billing records, and length of service of a subscriber to or customer of such service and the types of services the subscriber or customer utilized."[16]

This change was hailed by FBI Director Louis Freeh when he testified that the CALEA bill "reflects reasonableness in every provision:"

> "Enhanced privacy protection regarding governmental access to stored transactional records is included which, again, by my own admission, is a vast improvement from the initial draft which the Government proposed."[17]

---

[14] Susan Freiwald and Patricia L. Bellia, "Fourth Amendment Protection for Stored E-Mail," University of Chicago Legal Forum (2008), 121, 159-79.

[15] E.g., Digital Telephony and Law Enforcement Access to Advanced Telecommunications Technologies and Services: Joint Hearings on H.R. 4922 and S. 2375 Before the Subcomm. on Tech. and the Law of the S. Comm. on the Judiciary and the Subcomm. on Civil and Constitutional Rights of the H. Comm. on the Judiciary, 103rd Cong. 6, 158, 160–61, 166–78 (1994), available at http://ia700400.us.archive.org/23/items/digitaltelephony00wash/digitaltelephony00wash.pdf (statement of Jerry Berman, including memorandum of the Electronic Frontier Foundation).

[16] Telecommunications Carrier Assistance to the Government, Report to Accompany H.R. 4922, Committee on the Judiciary, 103rd Cong. 2d Sess. Rpt. 103-827 (Oct. 4, 1994).

[17] Testimony of FBI Director Louis Freeh, Aug. 11, 1994, "Digital telephony and law enforcement access to advanced telecommunications technologies and services: Joint Hearings before the Subcommittee on Technology and the Law of the Senate Committee on the Judiciary, and the Subcommittee on Civil and Constitutional Rights of the House Committee on the Judiciary, 103rd Congress, 2d Session, on H.R. 4922 and S. 2375," at pp. 114, 115.

The enhanced standard of 2703(d) was, indeed, one of the few privacy enhancements made to ECPA since its adoption in 1986 – and arguably the most significant.

Now, the Justice Department would like to repeal that improvement and roll back the standard for government access to Internet transactional data to what it was before 1994.

The Justice Department justifies such a change only on the ground that it would make the law technology neutral, but DOJ does not explain, and there is no principled reason why, technology neutrality should demand a lowering of the standard. If pure neutrality is the goal, then the standard for access to stored telephone dialing information should be raised, because it is the standard for stored dialing information that is the outlier. Under current law, access to telephone dialing information in real time requires a court order, access to Internet addressing information in real time requires a court order, and access to Internet addressing information in storage requires a court order (albeit under somewhat different standards). Only telephone dialing information in storage is available with a mere subpoena.

The change proposed by the Justice Department would exacerbate the inconsistencies in current law, setting different standards for access to the same data depending on whether it is acquired in realtime or from a log.

Congress was correct in 1994 when it required a court order to compel disclosure of Internet addressing data. Nothing in the intervening 19 years would justify rolling back that standard. If anything, data generated in the course of using the Internet is even more extensive and revealing today than it was in 1994.

IV. Limiting the role of the courts ("clarifying the standard") for issuing 2703(d) orders

In its testimony, the DOJ raised again a proposal it first offered in April 2011, concerning court orders issued under 18 USC § 2703(d). However, the DOJ's proposal has been effectively proven wrong by the intervening decision of the Supreme Court in US v. Jones, the GPS tracking case. Here's why:

ECPA covers all information pertaining to electronic communications, both content and non-content. Given the comprehensive coverage of the statute, Congress appropriately created a sliding scale of authorities, with essentially three tiers, permitting the government to obtain some basic data with a subpoena and other more sensitive data with a court order issued under an intermediate standard specified in 18 U.S.C. § 2703(d), while requiring a warrant for the most sensitive data, including the content of communications and any data protected by the Fourth Amendment.

As the DOJ notes, the government can use a court order under the intermediary standard of § 2703(d) to compel the production of a potentially wide range of data, ranging from subscriber identifying information to email addresses or IP addresses to full logs of email to and from addresses and Internet surfing data. (Section 2703(d) also states that a court may issue a (d) order for the disclosure of content, but that would be unconstitutional under *Warshak* as well as under the DOJ's new view of the treatment that should be accorded to content.)

Most critically, the DOJ also argues that § 2703(d) can be used to compel disclosure of location tracking information, monitoring a person's movements minute by minute over a long period of time. The DOJ argues that location tracking data is a "record pertaining to a subscriber" and thus encompassed by § 2703(d). However, reading the concurrences in *Jones*, it appears that location tracking over time may be a search under the Fourth Amendment requiring a warrant. Clearly, the tracking of persons, even on the public streets, poses constitutional questions that need to be considered.

When Congress drafted § 2703(d), it recognized that technology and the way people use it would change over time, and Congress was not entirely sure where the courts might draw the line as to what electronic data was be protected by the Constitution.

Accordingly, in § 2703 Congress gave the courts some discretion to recognize that certain data including content and non-content might be properly available to the government only with a warrant. Section 2703(d) provides that "[a] court order for disclosure… *may* be issued by any court that is a court of competent jurisdiction and shall issue *only if* the governmental entity offers specific and articulable facts showing that there are reasonable grounds to believe that … the records or other information sought, are relevant and material to an ongoing criminal investigation." 18 U.S.C. § 2703(d) (emphasis added).

In 2010, the Third Circuit held that the plain language of § 2703(d) gives judges discretion to deny (d) orders for compulsory disclosure of location tracking data if the courts believed that the information might require a Fourth Amendment warrant. See In re Application of the United States, 620 F.3d 304 (3d Cir. 2010). The court noted that the Constitution might require a warrant for access to location tracking information. In holding that judges have discretion under § 2703(d), the Third Circuit was able to avoid having to draw a precise line about location tracking data on constitutional grounds, allowing judges to make that judgment based on the facts of a specific case. Moreover, the Appeals Court was able to avoid having to hold § 2703(d) unconstitutional, which it would have had to conclude if it had found that the issuance of orders was mandatory and that the tracking data at issue was in fact constitutionally protected.

The Supreme Court decision in *Jones* effectively confirmed the wisdom of the Third Circuit's decision, since a constructive majority of Justices concluded that location tracking over a prolonged period of time can be a Fourth Amendment search, which normally requires a warrant.

The DOJ wants to reverse the Third Circuit opinion and amend § 2703(d) to require judges to issue (d) orders for all categories of information that DOJ argues are covered by (d). (Except the DOJ presumably does not want to mandate the issuance of (d) orders for content, even though (d) currently covers content, since a mandatory (d) order for content would make 2703(d) unconstitutional under the Justice Department's new view of the protected status of content.) Making (d) orders mandatory for all non-content information would jeopardize the constitutionality of ECPA, by forcing courts to issue orders under the intermediary standard of § 2703(d) even if the courts conclude that the information at issue is constitutionally protected.

Until Congress draws the precise lines regarding location data, and makes it clear what requires a warrant and what doesn't, it should leave § 2703(d) as is, thereby providing a safety valve allowing courts to require a warrant for data that might be constitutionally protected. If courts had to grant a § 2703(d) order whenever the "specific and articulable facts" relevance standard

were met, courts would be forced to confront a range of constitutional questions that otherwise need not be resolved and they might find ECPA unconstitutional (as the Sixth Circuit already has) for allowing access to constitutionally protected information without a warrant. That should be the *last* thing the DOJ wants.

For more information, contact Greg Nojeim, Center for Democracy & Technology, (202) 407-8815 or gnojeim@cdt.org.