ZwillGen PLLC

1705 N Street, NW • Washington, D.C. 20036

Marc J. Zwillinger
(202) 706-5202 (phone)
(202) 706-5298 (fax)
marc@zwillgen.com

September 12, 2012

Via Email

The Honorable Patrick J. Leahy
Chairman
United States Senate
Committee on the Judiciary
224 Dirksen Senate Office Building
Washington, DC 20510

The Honorable Charles E. Grassley
Ranking Member
United States Senate
Committee on the Judiciary
224 Dirksen Senate Office Building
Washington, DC 20510

Dear Chairman Leahy and Senator Grassley:

I am writing to assure you that Chairman Leahy's amendment to the Electronic Communications Privacy Act of 1986 ("ECPA") will preserve law enforcement's ability to obtain and use electronic evidence when conducting criminal investigations while also providing needed certainty to service providers and users about the legal standards under which that electronic evidence is obtained. I am quite familiar with these matters because I spent three years prosecuting cyber crime cases as an attorney in the Computer Crime and Intellectual Property Section of the Department of Justice's Criminal Division, where I taught other prosecutors and law enforcement agents how to search and seize electronic evidence. Moreover, for the past twelve years, I have counseled corporate clients, including internet service providers, on issues relating to compliance with the Stored Communications Act, the Wiretap Act, and FISA. I have also testified before the Senate and House Judiciary Committees on three separate occasions on issues related to ECPA reform.

The Leahy Amendment would amend ECPA to require law enforcement officials to obtain a search warrant in order to access the content of third-party communications held by a communications service provider who provides service to the public. The current version of 18 U.S.C. § 2703 already imposes a warrant requirement for email and other electronic communications in electronic storage for 180 days or less by an electronic communications service provider. The Leahy amendment would extend this warrant requirement to the entire period of storage, and would extend it also to the contents of

communications stored by remote computing services, without changing the way the government can gain access to emails within corporations and other legal entities.

No Effect on Company Email Systems

I am aware that certain entities and individuals have suggested that requiring law enforcement to obtain a warrant to access communications content from a provider of electronic communication services or remote computing services would stymie FTC, SEC and other administrative investigations of corporate wrongdoing because these agencies lack the authority to obtain search warrants and typically conduct their initial investigations with administrative subpoenas. It is true that the FTC and SEC may not be able to seek search warrants to get emails from third-party providers on their own, but they have the ability to work with the Department of Justice in criminal cases to obtain such warrants. More importantly, these agencies regularly operate by sending investigative demands and/or subpoenas to the target companies themselves seeking the production of records, and not to a company's service provider. The Leahy amendment would not interfere with the ability of these agencies to subpoena evidence of corporate wrongdoing **directly from the entity being investigated**.

To explain further, ECPA's prohibitions on disclosure of contents of communications currently apply, and would continue to apply, **only to remote computing services (defined as entities who provide computer storage or processing services to the public), and providers of electronic communications services to the public.** *See* 18 U.S.C. § 2702. Where such a disclosure prohibition applies, the covered entity may only make the specific types of disclosures that are authorized by the exceptions in 18 U.S.C. § 2702(b), which includes an exception that allows disclosure to the government when the government uses the proper form of compulsory legal process specified in 18 U.S.C. § 2703. *See* 18 U.S.C. §2703(b)(1) (authorizing disclosures consistent with § 2703). After the Leahy Amendment, the process required for the government to compel an otherwise prohibited disclosure of stored content would be a search warrant.

But unlike third-party service providers who service the public, corporations who operate their own private networks are **not covered by any of the current disclosure restrictions in 18 USC § 2702(a)**, because they do not offer services to the public. *See Anderson Consulting LLP v. UOP*, 991 F. Supp. 1041 (N.D. IL 1998) (finding that there is no ECPA restriction on disclosure of contents of emails carried on company's own computer network). The absence of a prohibition on disclosure in 18 U.S.C. § 2702(a) means that any FTC or SEC subpoena for a company's own internal emails will not be barred by the disclosure prohibitions of ECPA.[1] Thus, although a company could object to

[1] Although 18 U.S.C. § 2702(a) is titled "Voluntary Disclosures," it is the section of the ECPA that provides an absolute restriction on disclosures of stored content by public ECS and RCS providers, whether truly voluntary or based on some form of compulsion, unless the type of disclosure is specifically authorized elsewhere in the statute.

a subpoena for internal emails on the same variety of grounds that it could object to a subpoena for printed documents (relevance, burdensomness, privilege, etc), ECPA could not form a basis for a legal objection.

Indeed, if it were otherwise, even without the Leahy Amendment, all companies would currently have an existing ECPA defense to civil subpoenas directed at internal emails, because there is no compulsory process for obtaining such evidence under ECPA and no exceptions for civil discovery. *See Crispin v. Christian Audigier, Inc.*, 717 F. Supp. 2d. 965 (C.D.Cal. 2010); *Flagg v. City of Detroit*, 252 F.R.D. 346 (E.D. Mich. 2008); *Viacom Int'l v. YouTube*, 253 F.R.D. 256 (S.D.N.Y. 2008; *In re Subpoena Duces Tecum to AOL, LLC*, 550 F. Supp. 2d 606 (E.D. Va. 2008). Yet, to my knowledge, no court has ever held that a private company that provides email service to its own employees can resist civil discovery under ECPA. This is because private companies have no disclosure restrictions with regard to their own private email system under 18 U.S.C. § 2702.

If the entity whose records are sought also happens to be an internet service provider to the public, there is still no bar to production. First, as described, the prohibitions in ECPA would not apply unless the company is acting as the third-party provider for the messages that are being sought by the subpoena, rather than as an administrator of the corporate network. And even if it were acting as a third party provider, the exceptions in 18 U.S.C. § 2703(b) would still allow for the production of all messages where the company itself was the addressee, originator, or intended recipient of the messages, or where the company itself was the owner of the account where the information was posted. Thus, when compelled to produce the information by a subpoena, the company could not likely use ECPA as a defense for communications it has access to in the ordinary course of business.

Accordingly, changing the standards for law enforcement to obtain contents of communications for third-party data stored online should have no effect on the government's ability to obtain electronic evidence directly from the party that sent and received an email, or uploaded or downloaded a document for its own use. Indeed, such individuals or entities have always been directly subject to subpoena power (consistent with the Fifth Amendment) for their own records, whether stored in file cabinets or online. The Leahy Amendment would not change that practice.

General Benefits

Importantly, the Leahy Amendment would leave in place lower legal standards for the building blocks of law enforcement investigations. Subscriber identifying information (such as name, address, email address, and temporarily assigned IP addresses) would still be available with a subpoena, and transactional data revealing with whom a person had communicated, when, and for how long, would still be available with a court order issued on a lesser standard than probable cause. This is the type of information that prosecutors use to build probable cause that enables them to seek court-ordered access

to more sensitive information, such as communications content.

Equally important, the amendment would also leave in place the exceptions to the warrant requirement that appear in current law. Thus, if there is an emergency involving child abduction or an imminent terrorist attack, and there is no time to seek a warrant, law enforcement officers can access the communications immediately and prove probable cause to a court later. There is no need to create further exceptions from the warrant requirement cases in which quick action is required.

It is my view that, on the whole, a warrant-for-content requirement would benefit criminal investigations by clarifying the law about the proper legal standard for law enforcement to follow. It would also help clarify the law for service providers and Internet users. The Court of Appeals for the Sixth Circuit has already ruled that the Fourth Amendment protects email regardless of its age. *United States v. Warshak,* 631 F.3d 266 (6th. Cir. 2010). The *Warshak* decision has created uncertainty for providers who operate in multiple jurisdictions without knowledge of the precise location of their subscribers, and who cannot reasonably apply different legal standards in different jurisdictions based on the location of the user. It is also unclear whether the reasoning of that decision extends to other forms of stored content. Such uncertainty has increased the friction between such providers and law enforcement, causing delays in criminal cases. Rather than delaying the collection of communications content, a warrant requirement would speed such collection in many circumstances by reducing this friction. Moreover, from the law enforcement perspective, an unconstitutional statutory provision is at the center of many criminal investigations, potentially putting prosecutions at risk. Today, if law enforcement officers were to obtain stored communications content without a warrant, that evidence could be suppressed at the end of the prosecution.

As a former computer crimes prosecutor, I believe that the Leahy Amendment would provide needed clarity and certainty to facilitate the work of law enforcement, reduce the friction between internet service providers and law enforcement, and ensure the proper degree of protection for the private communications of Internet users.

Sincerely,

Marc J. Zwillinger
ZwillGen PLLC

cc: Members of the Senate Judiciary Committee