Written Testimony of Marc J. Zwillinger

Founder

ZwillGen PLLC

United States Senate Committee on the Judiciary

Hearing on

Strengthening Privacy Rights and National Security: Oversight of FISA Surveillance Programs

Washington, D.C.

July 31, 2013

Chairman Leahy, Ranking Member Grassley and Members of the Committee,

Thank you for asking me to submit written testimony about FISA oversight and specifically regarding my experience when confronted with government demands for user data under FISA and the FISA Amendments Act

By way of background, I worked as a Trial Attorney in the United States Department of Justice Computer Crime and Intellectual Property Section from 1997-2000, and for the last thirteen years I have had a private practice specializing in representing companies, including internet service providers, email providers, cloud services, social networking companies, and wireless carriers on issues related to government demands for user data under the Electronic Communications Privacy Act ("ECPA"), the Foreign Intelligence Surveillance Act ("FISA") and the FISA Amendments Act ("FAA").

I may also be the only private sector attorney to have ever appeared on behalf of a provider before the Foreign Intelligence Court of Review.[1] To be clear, I am submitting my written testimony today solely in my individual capacity, based on many experiences representing multiple clients from Apple to Yahoo!, and not on behalf of any one of them.

Although foreign intelligence surveillance is surely critical for national security, the FISA process has certain flaws which render it inconsistent with the core principles that are the foundation of this country's legal system. The most significant areas of concern are: (1) the lack of a true adversarial process with regard to the vast majority of legal issues that arise before the FISA court; and (2) the cloak of secrecy which covers not only the identity of targets, but also everything else surrounding the actual operation of the surveillance processes authorized by FISA and the FAA, including the existence of an individual piece of legal process, the numbers of affected accounts, the legal arguments that support the government's demands, and the FISA court's decisions. In this secret process, in many instances, the statute leaves the provider in the position of being the only bulwark against potential government overreaching, especially with regard to the Section 702 Directive process in which the FISA court's authority to supervise is minimal.[2] For the reasons described below, providers face significant pressure to comply with the government demands in some form. Though some aspects of any legal proceeding

[1] I was counsel to Yahoo! when it challenged the lawfulness of the directives served on it pursuant to the Protect America Act ("PAA"), the predecessor to the FAA, during 2007-2008. That challenge resulted in the partially released decision *In re Directives Pursuant to Section 105B of the Foreign Intelligence Surveillance Act*, 551 F.3d 1004 (Foreign Intl. Ct. of Rev. 2008), upholding the constitutionality of the PAA Directive process. It is possible that subsequent challenges by other providers may exist and remain under seal.

[2] In the criminal process, the legality of surveillance is usually tested when the evidence is sought to be introduced against the defendant. Because intelligence gathered for foreign intelligence purposes is rarely, if ever, used in criminal prosecutions, there will be no defendant to eventually challenge the surveillance.

related to intelligence gathering – like the target's identity – must always remain secret, the broader secrecy that engulfs the FISA process allows arguments to take root with the court and allows the government to isolate providers in a way that would likely not occur if the process were exposed to greater public scrutiny.

Accordingly, I believe the Senate should focus on adding stronger built-in safeguards to protect the rights of U.S. citizens and bringing greater transparency to the types of process used, the number of accounts affected, the legal arguments made, and the decisions that support surveillance orders. The current way the system operates -- which leaves only providers with the ability to the challenge the government -- but forces them to do so in complete secrecy, has a tendency to lead to legal interpretations that might not survive the light of public scrutiny. This system is insufficient for the reasons described below.

First, any FISA process a provider receives is under seal and classified. The company receiving an order (or directive) is restricted in their handling of the demand, which in turn, can adversely impacts the amount of review it may receive. For example, a provider with limited resources or one who is new to receiving classified orders, may have no cleared employees, or the cleared employees may not be members of the legal department or executive management authorized to employ the substantial legal resources required to raise such a challenge. This makes internal escalation of individual demands extremely difficult. In addition, issues related to the storage of classified information often restrict the provider's ability to keep and refer back to the legal process. Instead, the government holds the demand itself and shares it with the company only upon initial service and then on request. Thus, in practice, a provider in these circumstances can be influenced by the government's view of what is within the scope of the request. And where the provider does seek the advice of outside counsel to evaluate the demand -- while under intense time pressure to start the surveillance -- the number of lawyers qualified and cleared to provide advice on FISA issues is small.

Second, without published cases to examine, providers are left with an uncertain basis upon which to base a challenge to an order or a directive, especially since the provider knows that the court has already approved the issuance of process through some limited review, the scope of which is not readily apparent. Also, there is often no way for a provider to determine whether such process is routine, or has been complied with by other similarly situated providers. This problem is especially acute with directives issued under 702, which, are not required by statute to contain information on the specific targets at the time the directives are issued. Nothing in the statute prevents the government from identifying new specific targets after the directives have been issued. Yet it is the directives themselves, and not any subsequent orders identifying individual targets under the directives that the FAA specifically allows providers to challenge. Faced with limited information, no visibility into the basis for

the certification, no ability to disclose even the fact of the order or directive to anyone else (even other industry participants), providers are fairly isolated in determining the proper response. Indeed, one of the most valuable roles I can play as outside counsel is to help clients recognize the difference between a routine order and one based on a novel legal theory, which I am able to do this on occasion because I represent multiple companies who receive national security demands. A lawyer representing only one client on such matters would not have any basis, other than representations from the government or the FISA court itself, to identify novel orders and arguments.

Third, there are some institutional pressures and procedural disincentives against levying a challenge. As various transparency reports issued by certain providers make clear, large providers have to deal with representatives of the Department of Justice regarding thousands of annual criminal and intelligence demands for user data. As a result, providers who challenge governmental authority could face pressure from the government in other areas, including delays in responding to criminal legal process. Moreover, the government can show little to no flexibility in applying a fairly rigid process of handling classified information where access is needed even to review process, let alone bringing a challenge. This makes levying a challenge logistically difficult. Only cleared personnel and counsel can participate in such a challenge or discuss details of the Section 702 process and directives. With no public transparency, no ability to enlist amicus or industry participation,[3] and classifications that may limit the ability to brief internal and external corporate, legal, and business advisors, and limited counsel choices because many lawyers lack section 702 experience and clearances, only certain providers can contemplate challenging government orders or directives and only in fairly significant matters.

If a provider brings a challenge, the statutory process does not necessarily provide for complete transparency or a level playing field for the provider. As the published decision in *In re Directives* makes clear, a phalanx of 11 government lawyers, including the Acting Solicitor General of the United States, was involved in defending the statute.[4] And the decision also makes clear that the company had to overcome the hurdle of demonstrating that it had standing to appear to litigate these issues -- notwithstanding the clear legislative language that

[3] By contrast, when Yahoo! challenged what it believed to be an unconstitutional criminal order in the District of Colorado, many interest groups joined Yahoo! as amicus and the government ultimately withdrew its demand for additional documents.

[4] According to the opinion, the government was represented in the case by Gregory G. Garre, Acting Solicitor General, Mark Filip, Deputy Attorney General, J. Patrick Rowan, Acting Assistant Attorney General, John A. Eisenberg, Office of the Deputy Attorney General, John R. Phillips, Office of Legal Counsel, Sharon Swingle, Civil Division, and Matthew G. Olsen, John C. Demers, Jamil N. Jaffer, Andrew H. Tannenbaum, and Matthew A. Anzaldi, National Security Division, United States Department of Justice. This does not count the Attorney General, Michael B. Mukasey, who was listed on the brief but may not have contributed to the briefing. *In re Directives Pursuant to Section 105B of the Foreign Intelligence Surveillance Act*, 551 F.3d 1004 (Foreign Intl. Ct. of Rev. 2008).

authorizes a provider to file a challenge to the directives issued under the PAA.[5] The decision also shows that some of the documents relied upon in the decision of the Court of Review were classified procedures submitted as part of an ex parte appendix that remains sealed.[6]

My point is not that the Court of Review should have reached a different conclusion in 2008. When additional portions of the decision and the legal briefs are unsealed, lawyers, Fourth Amendment scholars and the public can reach their own conclusion on that score. My point is that the existing statute – which allows the court to do a fulsome review of a directive only when a provider levies a challenge – does not provide the type of safeguards that are typically built into our adversarial court system. In the history of the directive program under the PAA and the FAA, it may turn out that only one company has ever tried to challenge the lawfulness of the process. And that challenge included secret filings by the government, even though whatever was contained in those filings could presumably be changed by the Executive Branch. Moreover, the *ex parte* nature of those filings means the government did not disclose their substance even to cleared lawyers within the context of the sealed proceeding. Compare this to criminal process, which is much easier for providers to challenge, and is subject to a second set of challenges by criminal defendants, if the data is ever used in a proceeding. The FAA simply does not provide for the type of a true adversary process on which the American judicial system is based.

The current system of checks and balances under the FAA is simply not enough. It's not due to a lack of desire on the part of the providers to defend their users. Quite the opposite, the types of providers I represent do have strong business reasons to challenge what may be an overstepping of surveillance authority by the government or new legislation that may not provide adequate constitutional protections to their user's privacy. In many cases, if these companies do not rigorously enforce the limits imposed by law on law enforcement, law enforcement can and, unfortunately will, pressure the providers to do more. Such pressure is not only a burden for the companies, but raises serious concerns for the companies about losing the trust of their users. If users do not trust these companies, the users can and will take their business elsewhere.[7] But Internet companies run the gamut from large entities such as Yahoo!, which had the will and the wherewithal to fight the directive process, to startups and

---

[5] *See Id.* at 1008-09.

[6] "The [redacted text] procedures [redacted text] are delineated in an ex parte appendix filed by the government. They also are described, albeit with greater generality, in the government's brief. [redacted text) Although the PAA itself does not mandate a showing of particularity, *see* 50 U.S.C. § 1805b (b) , this pre-surveillance procedure strikes us as analogous to and in conformity with the particularity showing contemplated by Sealed Case. *See* 551 F.3d at 1013-14,

[7] For these precise reasons, several of my clients are members of the Due Process Coalition which is seeking amendments to the Electronic Communications Privacy Act to better protect user privacy in a manner more consistent with the Fourth Amendment in the context of government demands issued in criminal investigations and prosecutions.

smaller providers who may not have the money, knowledge, counsel or capability to fight government requests.

A built-in adversary, in the form of a Guardian *Ad Litem* for the American people would be a significant improvement addition to the existing statutory framework. Such an advocate could participate in all cases involving a new statute or authority or a new interpretation or application of an existing authority. The Guardian could either choose the cases in which to be involved, or the Guardian's participation can be requested by the court or a provider where an opposition would be useful to test and evaluate the legal arguments presented by the government. The Guardian's office could be established with proper security safeguards to draft, store, and access classified records more efficiently. It could also be required to report to the public and Congress the number of cases it has argued and how often it has limited or pared back the government's requests. The Guardian could also brief this committee, and provide a vital counterpoint for members to consider when exercising their oversight duties Appointing a Guardian *Ad Litem* for the public ensures that novel legal arguments in the FISA court would face a consistent, steady challenge no matter who the provider is. This would make the FISA process stronger by ensuring that results are consistently subject to checks and balances. And, as we have seen, the result of not having such a process allows the court and DOJ work through difficult legal issues with no balancing input. The Guardian would be especially useful in cases where the government demands access to communications in a way that may have a profound impact on people other than the target, such as where decryption made be involved or where a provider is asked to provide assistance in ways that are unlike traditional wiretaps.

The lack of an adversary process and the need for additional transparency into the directives process, the types of legal challenges, and the number of uses affected by it are not the only reforms I would suggest to the Section 702 Directive process, although they would be a good place to start. In that regard, I commend Senator Leahy and Senator Franken for proposing legislation that would improve the current situation and require more disclosure and mandatory public reporting to bring light to the government's practices. But I would also ask the Senate to consider further how to enhance the ability of providers to bring fair and meaningful challenges when they think it is necessary, and to build in a more systematic adversary, such as a Guardian Ad Litem, in appropriate cases.

While most of my written testimony has focused on the procedural deficiencies involved in the FISA and FAA challenge process, the basic idea that a court order is never needed where just one side of a communication is foreign should also be reconsidered. The types of communications that can be demanded under 702 directives are not just phone calls, but can also include emails, instant messages, photos, videos, and stored cloud documents. Yet the framework of 702 is that whenever one party to the communication is reasonably believed to

be outside the United States, any content sent to or from that party can be obtained. This paradigm may make sense if surveillance is analogized only to a traditional phone call, where a single foreign side means that conversation is at least 50% foreign. But this is not the case with in an internet communication – like a cloud document – which can have many "sides."

For example, if a document stored on a collaborative sharing platform was accessed by 10 people, 9 of whom are in the United States but one of whom is outside the United States and deemed to be a proper surveillance target, the document may be eligible for disclosure under the statute. Yet that document may have been created by a U.S. person, is usually accessed by U.S. persons, and the document is stored in the United States. When such significant U.S. person involvement is present, any government request for surveillance should involve more traditional court involvement – not the minimal review of the 702 process. And, if such collection were to occur, the collection of U.S. communications traffic in such circumstances should not be deemed "incidental," when it is the predominant activity being captured. Equally problematic is the theoretical issue of documents created in the U.S. and stored in the U.S. that a user then accesses from abroad. Under current law, the Government could argue that simple access from a hotel room in London would open the door to the collection of documents previously protected by the FISA warrant process without a court order simply because a foreign user boarded a plane. Allowing warrantless surveillance of these types of U.S.–centric communications and documents is not consistent with the Fourth Amendment which doesn't cease to apply just because one participant in the communication, no matter how minor their role, may be foreign. Accordingly, the framework of Section 702 is inadequate to protect the interests of U.S. persons, and this should not be deemed cured merely because the Executive Branch takes measures to institute its own secret checks and balances.

Thank you for the opportunity to testify today. I would be pleased to work with the Committee on an ongoing basis as the process to reform FISA moves forward.