

SENATE COMMITTEE ON THE JUDICIARY

Hearing on

"Strengthening FISA: Does the Protect America Act Protect Americans' Civil Liberties and Enhance Security?"

Tuesday, September 25, 2007

**Testimony of Michael A. Sussmann
Partner, Perkins Coie LLP:**

Perspective of Communications Providers on the Protect America Act of 2007

Chairman Leahy, Ranking Member Specter, and Members of the Committee, thank you for this opportunity to provide testimony concerning providers' perspectives on FISA modernization, the Protect America Act of 2007 (the "Act"), and upcoming efforts to renew and amend national security legislation.

I am a partner in the Washington, DC office of Perkins Coie LLP. We represent a large number of fixed-line (telephone), wireless, and Internet service providers in responding to government demands for customer information and electronic surveillance. I have a current national security clearance and I counsel providers on compliance with the Foreign Intelligence Surveillance Act (FISA) and orders issued from the Foreign Intelligence Surveillance Court, national security letters, and other issues relating to national security. Prior to joining Perkins Coie, I was at the Department of Justice for 12 years, handling national security issues for the Assistant Attorney General for the Criminal Division and then, for eight years, as a senior counsel in the Computer Crime and Intellectual Property Section. My testimony today is based on my own views and experience and does not represent the views of any particular communications provider.

The Role of Communications Providers Under FISA

Communications providers have a critical role to play in the implementation of FISA and other foreign intelligence surveillance legislation. Providers receive classified orders from the FISA Court; review the orders and consider their legality and practicality from a technical standpoint; and decide whether to comply with an order or seek modification or clarification from the FISA Court or the government. Notwithstanding the valuable perspective of the privacy community and others in academia, outside the federal government no one other than the providers see or will see FISA orders or directives under the Protect America Act. Indeed, section 105B(h) of the Act provides specific authorization for *providers* alone to challenge before the FISA Court the legality of a directive issued under the Act. It is therefore important that providers' perspectives be considered when FISA is amended or when new legislation in this area is considered. Clarity is essential and will reduce the likelihood of disputes, delay in responding to directives or orders, and filing of petitions.

Providers' Perspective on FISA and FISA Modernization

When passed in 1978, the Foreign Intelligence Surveillance Act was critical in overlaying federal court supervision and specific procedures onto the government's ability to conduct national security investigations that involved U.S. persons. The protections contained in FISA not only provide the supervision of a neutral and independent Article III judge, they provide legal standards and regularized procedures that allow providers to know they are keeping within the law and hewing to the intent of Congress.

Providers therefore must rely on the President and Congress to forge the necessary legal tools for national security investigations and to balance those needs with the protections guaranteed by the Constitution and by statute, and with general notions of privacy and individual liberty. With clear guidance in the form of legislation, providers have for almost 30 years complied with the signed orders from federal judges appointed to the FISA Court. The clarity in FISA and in the instructions from the FISA Court has allowed providers to offer lawful assistance in national security investigations that required access to electronic communications.

While providers understand the needs that the Protect America Act is intended to address, a number of provisions contained therein are either ambiguous or are subject to differing interpretations. Since the Act sunsets six months after its enactment, and leaders in Congress and executive branch have discussed the issue of its renewal or amendment, I would like to summarize for the Committee eight issues from the Protect America Act that would benefit from clarification in any future legislation that would seek to renew or amend the Act.

Eight Issues From the Protect America Act That Would Benefit From Clarification

1. Does the Protect America Act authorize through the use of directives the production of *stored* communications (e.g., email mailboxes) from providers, as opposed to just the real-time interception of communications?

Notably, the Act uses the terms "acquisition" and "acquisition of foreign intelligence information" throughout, including for each of the five criteria for a certification in section 105B(a), and in the description of a directive in Section 105B(e). By way of analogy, in the criminal context, the term "acquisition" is used in the federal Wiretap Act, 18 U.S.C. § 2510, but not the Stored Communications Act, 18 U.S.C. § 2701. The term "intercept" is defined in the Wiretap Act as "the aural or other *acquisition* of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device." 18 U.S.C. § 2510(4) (emphasis added). The same usage can be found elsewhere in the statute (*see* 18 U.S.C. § 2511(2)(f): "Nothing contained in [the Wiretap Act] or . . . the Communications Act of 1934, shall be deemed to affect the *acquisition* by the United States Government of foreign intelligence information from international or foreign communications" (emphasis added)). However, the Stored Communications Act, which deals exclusively with the disclosure (to the government or third parties) of stored communications, does not use the term "acquisition," instead using

such terms as “divulge” or “disclose” “the contents of a communication *while in electronic storage.*”

Notwithstanding the plain language in the law, case law does exist that interprets the term “acquisition” to include stored communications. Since disclosure under the Protect America Act of stored communications could involve access to entire email mailboxes or other account content, as opposed to just individual email messages or documents, the question of applicability of the Act to stored communications and content certainly is one that should be answered in clear and unambiguous terms, especially if the account creation and use predates the time when the government reasonably believed that the surveilled person was located outside the United States.

2. Does the Protect America Act authorize through the use of directives physical searches and “section 215 orders” for production of business records, since physical searches and section 215 orders are not considered "electronic surveillance" under FISA as it existed before passage of the Protect American Act?

Section 105B(a)(2) of the Act requires certifications to the FISA Court concerning directives to contain determinations by the Director of National Intelligence (“DNI”) and the Attorney General that “the acquisition does not constitute electronic surveillance.” Neither physical searches authorized under FISA at 50 U.S.C. §1822 nor the compelled disclosure of business records authorized at 50 U.S.C. § 1861 (often referred to as “section 215 orders” because of the section of the USA Patriot Act that created this power) fall under FISA’s definition of electronic surveillance at 50 U.S.C. § 1801(f). Therefore, if the DNI and Attorney General make the *other* determinations required by sections 105B(a)(2)-(5), directives arguably could include demands for physical searches and for business records.

I note that in testimony last week before the House Judiciary Committee, Ken Wainstein, Assistant Attorney General for the National Security Division of the Justice Department, took the position that the Act does not authorize physical searches of the homes, businesses or effects of persons located in the United States. He further stated that the Administration would not take advantage of any authorization under the Act to demand business records.

Notwithstanding the positions offered by Mr. Wainstein, I believe the Act as written could allow for such searches and demands for records which, in turn, could be a basis for the compelled disclosure by providers of stored communications. For this reason, it would be preferable for any new legislation in this area to address the availability of physical searches and demands for business records under the Act.

3. Whose "reasonable belief" concerning the location of parties to a communication is contemplated in section 105B(a)(1) of the Protect America Act – only that of the U.S. intelligence community or that of providers, as well?

If a directive were to require surveillance on 20 target accounts, and a provider were able to ascertain that five of those accounts contained and involved only domestic communications, surveillance of those five accounts would constitute “electronic surveillance” and would not be authorized under the Protect America Act. It would be instructive to providers to know whether they can “look behind” a directive and comply with regard to only those accounts (in this case 15 of 20) for which a reasonable belief as to an international connection exists. In some cases it may be obvious to a service provider, such as when a target call is registered on a cell site within the United States; and in other cases, it may be clear from network information that the target was accessing a system from within the United States if such information was analyzed. Service providers do not want technical mandates, but they also do not want to be liable if the “reasonable belief” turns out to be incorrect. A clearer articulation of this standard would benefit all stakeholders.

4. Does the requirement that a certification be based on a determination that “a significant purpose of the acquisition is to obtain foreign intelligence information” provide any *real* limitation in the breadth of surveillance?

If technically feasible, a directive requiring surveillance of all communications to or from a particular foreign country would appear to be lawful if the U.S. government was looking for the communications of just one terrorist, as it could be said that a *significant purpose* of that acquisition would be to obtain foreign intelligence information. For this reason, a limitation for overbreadth may be advisable. To achieve this goal, Congress may want to consider amending section 105B(a)(4) to say that “a significant purpose of the acquisition is to obtain FII *and the collection is not overly broad.*”

To be clear, providers are not in a position to assess the purpose of an acquisition, nor should they be. But overbreadth is a significant concern for service providers as it creates technical burdens, which I discuss below. Further, since minimization under FISA is *post hoc*, meaning that everything is collected and only relevant communications are reviewed, the practical consequences of overbroad surveillance include the collection and retention of large quantities of “innocent” communications.

5. Does a provider get notice of the government’s motion to compel compliance with a directive under section 105B(g) of the Protect America Act, and thereby a chance to respond to such motion, or can the government’s motion be filed with the FISA Court on an *ex parte* basis with a provider only learning of the government motion upon issuance of an order by the FISA Court?

While traditional government practice before the FISA Court has been limited to *ex parte* filings and appearances, the Protect America Act authorizes (a) providers to challenge before the FISA Court the legality of a directive, and (b) the government to seek assistance from the FISA Court in compelling compliance on the part of a provider. However, the Act only provides procedures in the former case. Where providers are unable to comply with the requirements under a

directive, it is important that they have the ability to present their positions to the FISA Court, should the issue of provider compliance be presented to the FISA Court by the government.

6. In *non-emergency* cases, can directives be issued to communications providers orally, and what information should be required to be in any written directives?

Section 105B(e)(1) of the Protect America Act authorizes the DNI and Attorney General to “direct a person to immediately provide the Government with all information, facilities, and assistance necessary to accomplish the acquisition.” However, there is no mention in the Act as to whether this direction should come in the form of a specific writing, or whether communications that are solely oral would be acceptable.

Providers would like any directives issued under the statute to be presented to providers in the form of a writing. Oral directives do not provide a clear record of a government request, and for obvious reasons they can lend themselves to misunderstandings.

Moreover, as both the federal Wiretap Act and the Pen Register and Trap and Trace statute provide instruction as to what details must be included in any order presented to a provider, Congress may want to consider whether it should include in any future amendments to FISA requirements for certain information to be included in a directive. For example, information such as the statutory authorization, reference to a certification by the FISA Court, a declaration that all assistance requested does not constitute electronic surveillance, and the maximum number of simultaneous surveillance contemplated by the directive may be helpful. Such specificity might enhance accountability and set clearer limits on the surveillance authorized under a directive.

7. What are the limits to the burdens placed on providers by directives, and can a directive require changes to service and/or architecture to accomplish surveillance, so long as costs are paid?

Section 105B(f) of the Protect America Act provides that the “Government shall compensate, at the prevailing rate” a provider for compliance with a directive. Providers are nonetheless concerned about their ability to comply with a directive which is overly burdensome or which requires interference with or changes to its network infrastructure or provision of service.

A provider compliance center that can support 20 simultaneous interceptions in the criminal context will not necessarily be able to support a request in a directive to run 100 – both from the standpoint of personnel and equipment. Likewise, a provider’s network simply may not be built to intercept certain communications, such as peer-to-peer text messaging. While many courts have addressed issues of undue burden in government requests, the Protect America Act is silent on this point. A notion of fairness could be added in section 105B(h)(1)(A) by inserting a reference to burden such as the following: “A person receiving a directive issued pursuant to subsection (e) may challenge the legality *or undue burden* of that directive by filing a petition”

8. Finally, since the immunity provision in the Protect America Act is not severable from the remainder of the statute, would immunity survive a FISA Court finding that the Act is unconstitutional?

Section 105B(1) states that “notwithstanding any other law, no cause of action shall lie in any court against any person for providing any information, facilities, or assistance in accordance with a directive under this section.” Because of the public interest in and controversy surrounding FISA and warrantless surveillance, it is not unlikely that a plaintiff will challenge the constitutionality of the Protect America Act or any successor legislation. Providers who, in good faith, comply with a directive would nonetheless lose the protection of section 105B(1) immunity if they are later sued and the statute were previously found to be unconstitutional.

Courts might be inclined to extend this immunity, and indeed good public policy requires such protection, for it is in the interest of all three branches of our government for citizens to accept the legality and force of any law properly enacted; second-guessing the *future* effect of a law in fact undermines the rule of law. A provision in an amended Protect America Act that makes the immunity provision severable in the event of a finding of unconstitutionality benefits the executive branch in removing hesitancy in compliance with directives, Congress by giving more certainty to the effect of its laws, and the courts in reducing unnecessary litigation over the existence of immunity.

Conclusion

As I discussed earlier, communications providers have a critical role in facilitating lawful access to electronic communications in national security investigations. As intermediaries between government authorities and subjects of surveillance, they ensure that surveillance laws are followed.

I am grateful to have had this opportunity to provide a perspective from industry on FISA and FISA modernization, and to highlight certain ambiguities in the Protect America Act that Congress may want to consider when crafting any future legislation. It is imperative that these laws are as clear and unambiguous as possible. The views I expressed today are of course my own, and I cannot claim to represent all or even a majority of industry views. Nonetheless, my hope is that the deliberations of this Committee will be aided by inclusion of industry’s perspectives along with other viewpoints on this topic.

###