Testimony of Professor Peter P. Swire
Professor of Law
Moritz College of Law
The Ohio State University

before the

Subcommittee on Crime, Terrorism, and Homeland Security

of the

Judiciary Committee of the U.S. House of Representatives

on

Oversight Hearing on the Implementation of the USA PATRIOT Act: Sections of the Act that Address - Crime, Terrorism, and the Age of Technology

To Examine *Section 209*: Seizure of Voice-Mail Messages Pursuant to Warrants; *Section 217*: Interception of Computer Trespasser Communications; and *Section 220*: Out-of-District Service of Search Warrants for Electronic Evidence

April 20, 2005

Mr. Chairman, Mr. Ranking Member, I thank the Committee very much for the opportunity to testify before you today on Sections 209, 217, and 220 of the Patriot Act. This testimony gives my relevant background. It supports renewal of Section 220, the nationwide service of search warrants for electronic evidence. For Section 217, the computer trespasser exception, I believe that the exception should only be renewed if Congress takes a simple step to assure that it will be used only as intended. I therefore believe that any renewal of that provision should depend on also enacting a suppression remedy for electronic communications that are seized and go beyond the limited scope permitted by the provision. For Section 209, which is entitled "seizure of voice mail messages pursuant to warrants," this testimony suggests that the provision affects a much greater portion of telephone communications than has been previously understood. I therefore devote the bulk of my testimony to that issue.

Background

I am now Professor of Law and John Glenn Scholar of Public Policy Research at the Moritz College of Law of the Ohio State University. I am Director of that school's Washington summer internship program, and live in the Washington, D.C. area.

From 1999 until early 2001 I served as the Chief Counselor for Privacy in the U.S. Office of Management and Budget. In that role, I participated in numerous privacy, computer security, computer crime, and related issues. Of most relevance to today's hearing, early in 2000 I was asked by John Podesta, the President's Chief of Staff, to chair a 15-agency White House Working Group on how to update electronic surveillance law for the Internet Age. The Working Group met intensively over a period of several months.

The Administration's draft legislation was announced in June, 2000 and introduced as S. 3083. Roughly speaking, the Administration bill contained a third or a half of the increased surveillance powers that were later included in Title II of the Patriot Act. The Clinton Administration bill also contained important privacy protections. These privacy protections included treating "electronic" communications, such as e-mails and web surfing, with the same protective standards that apply to phone calls and other "wire" and "oral" communications. Our proposal at that time also included raising the standard somewhat for pen register and trap and trace orders.

After hearings, this Committee considered the issues in the fall of 2000. Interestingly, the Committee at that time criticized the Administration plan for being out-of-balance and not protective enough of citizen privacy. The Committee voted out H.R. 5018 overwhelmingly, with only one dissenting vote. The Committee bill notably included the same suppression remedy for "electronic" evidence that exists for "oral" and "wire" communications. The Committee also raised the standard for pen register and trap and trace orders, making clear that the judge should exercise discretion in granting such orders and stating that orders should be issued only where there are "specific and

articulable facts" to support the order. Despite the nearly unanimous Committee support, the bill ran out of time in the 106th Congress. As the House Judiciary Committee considers electronic surveillance issues this year, I believe that members and staff may find it informative to revisit the debates from the fall of 2000, in order to see how these precise issues were addressed during the extended deliberations that occurred at that time.

I left the government and returned to law teaching in January, 2001. After the attacks of September 11, I participated in the public debates surrounding the Patriot Act. Many of the issues in today's hearing were addressed in a paper I wrote at that time for the Brookings Institution, entitled "Administration Wiretap Proposal Hits the Right Issues But Goes Too Far," available at http://www.brookings.edu/dybdocroot/views/articles/fellows/2001_swire.htm. That paper discussed the computer trespasser exception in Section 217 and nationwide trap-and-trace orders in Section 220. The paper especially stressed the importance of including a sunset provision in the Patriot Act. The hearings this year, I believe, show the wisdom of Congress in doing that. If sunset provisions are not included in surveillance law, then the Department of Justice has little or no incentive to come to the Congress, explain clearly the current state of the law, and set priorities among its proposals for expanded surveillance authority. Including some sunset in this year's reform bill would give this Committee, the Congress, and the American people a better opportunity to set good policy and have informed debate on these issues again in the future.

Since passage of the Patriot Act, a large portion of my academic research has been on the new surveillance provisions. With Charles Kennedy, I wrote "State Wiretaps and Electronic Surveillance After September 11," 54 Hastings L.J. 971 (2003), available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=416586. My longest article in this area is "The System of Foreign Intelligence Surveillance Law," 72 Geo. Wash. L. Rev. 1306 (2004), available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=586616. This article presents the most detailed history and explanation to date of the Foreign Intelligence Surveillance Act, including over a dozen reform proposals that affect Sections 215, 218, 505 and other portions of the Patriot Act. As discussed below in this testimony, I wrote "*Katz* is Dead, Long Live *Katz*," 102 Mich. L. Rev. 904 (2004), available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=490623. This article draws attention to the dramatic reduction in privacy for our phone calls that is resulting from changing technology. In addition, I have written on Sections 214 and 215 for the www.patriotdebates.com sponsored by the American Bar Association. Requests for printed copies of these writings can be sent to Ms. Carol Peirano, Moritz College of Law, 55 West 12th Ave., Columbus OH 43210. I hope that this writing, and other materials at www.peterswire.net, will be of use to the Committee and other interested persons as these important issues are considered.

Section 209, Incorrectly Titled "Seizure of Voice Mail Messages Pursuant to Warrants

It is especially important that the Committee direct its attention to the incorrect title of Section 209. In the Patriot Act, this section is called "Seizure of Voice Mail Messages Pursuant to Warrants." The Computer Crimes and Intellectual Property Section of the Department of Justice, in its Field Guidance on the Patriot Act, gives a more accurate title: "Obtaining Voice-mail and Other Stored Voice Communications." http://www.usdoj.gov/criminal/cybercrime/PatriotAct.htm. The fact that Section 209 applies to all stored voice communications makes it much more far-reaching than the misleading current title of Section 209 indicates.

Some brief history helps explain what is at stake. The 1928 case of *Olmstead v. United States*, 277 U.S. 438 (1928), held that wiretaps were not a "search" under the Fourth Amendment where they were conducted outside of the home. *Olmstead* was overruled in the famous cases of *Katz v. United States*, 389 U.S. 347 (1967), and *Berger v. New York*, 388 U.S. 41 (1967), which established that the Fourth Amendment does apply to telephone wiretaps and other communications where there is a "reasonable expectation of privacy." In 1968, Congress passed a federal wiretap statute in Title III of that year's crime bill. Title III set strict national rules for wiretaps of "wire" communications (such as phone calls) and "oral" communications (such as ordinary conversations that are bugged).

In 1986, Congress passed the Electronic Communications Privacy Act. ECPA extended many of Title III's protections to "electronic" communications, which include e-mail and web surfing. Notably, a strict Title III order is required before law enforcement can intercept electronic communications. Although most of the phone wiretap protections apply, three do not: (1) interceptions are permitted for any crime, rather than the list of serious felonies in 18 U.S.C. § 2516; (2) the high-level approval within the Justice Department required under 18 U.S.C. § 2518 is not required for "electronic" interceptions; and, most importantly, (3) the statutory suppression remedy under 18 U.S.C. § 2515 does not apply to "electronic" interceptions. The Clinton Administration proposal in 2000 would have changed these three provisions, providing the same privacy protections against wiretaps of e-mails as exists for phone calls. This Committee almost unanimously voted for those changes in 2000.

ECPA also created for the first time a federal regime that governs access to stored electronic communications. Congress correctly recognized that computers and other new information technology make it much more common for ordinary persons to have their communications stored in electronic form, often in the hands of an Internet Service Provider or some other third party. After lengthy debate, Congress decided in the Stored Communications Act to give these stored records less protection than applies to contemporaneous communications such as a phone call or an e-mail as it travels from sender to recipient.

The rules for government access to the contents of stored electronic communications are much less strict than for wiretaps of phone calls or bugging of oral communications. Instead of the special Title III wiretap requirements, an ordinary probable cause search warrant is sufficient to see e-mail and other stored electronic communications. In many instances, the contents of stored communications can be accessed by a grand jury subpoena or an order under 18 U.S.C. § 2703(d), which permits access to stored communications where there are "specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation." For further discussion of the rules on stored communications, see Susan Freiwald, "Online Surveillance: Remembering the Lessons of the Wiretap Act," 56 Alabama L. Rev. 9 (2004) (emphasizing privacy perspective); Orin Kerr, "A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It," 72 Geo. Wash. L. Rev. 1208 (2004) (emphasizing law enforcement perspective).

It was against this backdrop that Congress enacted Section 209 of the Patriot Act. That provision makes a seemingly simple change to the law of stored communications. Previously, the contents of only stored *"electronic"* communications were available under the looser rules of the Stored Communications Act. Section 209 applies the looser rules to all stored "*wire or electronic"* communications. Even though the Patriot Act calls this provision "Seizure of Voice Mail Messages Pursuant to Search Warrant," there is no mention of "voice mail" in the statutory text, and many messages may be obtained with much less than a search warrant.

This precise change in the law was debated within the Clinton Administration in 2000 as we put together our legislative proposal. At that time, advocates for the change argued that the new power would be useful for investigating stored, unopened voice mails. They also argued that people have a lower expectation of privacy in a voice-mail than in a phone call, because people understand the possibility that someone else might hear the voice mail. On the other hand, opponents of the change argued that people expect privacy in a voice mail much as they do in a phone conversation – both are generally private communications and deserve the full protections that apply where there is a "reasonable expectation of privacy." Eventually, the change was not included in the legislative proposal.

Based on my continued research, I have come to believe that Section 209 sweeps far more broadly than has been publicly discussed. What if the contents of ordinary telephone calls become stored as a matter of routine? This storage is likely to become far more common with the imminent growth of Voice over Internet Protocol ("VoIP") telephone calls. VoIP uses the packet-switching network of the Internet to connect telephone calls rather than the traditional circuit-switching used by established phone systems. The Wall Street Journal has reported estimates that about 20% of new phones shipped to U.S. businesses now use VoIP technology, with that number exceeding 50% by 2007. Wall St. Journal, Jan. 12, 2004, at R7. Residential use will follow quickly, spurred by the expected low cost of international and other long-distance calls.

Use of VoIP is likely to result in a drastic increase in storage of the content of telephone calls for at least two reasons. First, the use of computers for making telephone calls makes it trivially easy for one party to store the contents of the conversation. This ease of storage comes at a time of plummeting cost of computer storage, as shown in the enormously greater size of today's typical hard drives. Ordinary users may store phone calls in the future the way they store e-mails and photos today or log their instant message sessions.

A second technological change with VoIP is the likelihood that there will be systematic "caching," or storage, of telephone communications at the network level. One existing product, for instance, is called "CacheEnforcer." CacheEnforcer stores communications for a group of users, such as for a company or a network operated by a university. Network managers, not individual users, determine the caching procedures. The caching can help the network in various ways including improving average network speed and assisting in network security. The product website says: "Because the CacheEnforcer sits in front of your WAN [wide area network] or Internet link, all outbound traffic passes through it. By setting appropriate policies on the CacheEnforcer, network managers, not individual users, determine the appropriate caching policies for the entire network." www.allot.com/html/products_cacheenforcer.shtm. Once "all outbound traffic" can be stored, then many, many telephone calls will be subject to the lower protections for stored records.

In a recent article in the Michigan Law Review, I discussed how these trends undermine the constitutional protections for the privacy of telephone conversations. "*Katz* is Dead, Long Live *Katz*," 102 Mich. L. Rev. 904 (2004), available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=490623. Because the Supreme Court has found that people lack a "reasonable expectation of privacy" in some stored records, e.g., Smith v. Maryland, 442 U.S. 735 (1979) (stored lists of phone numbers dialed), there is a serious risk that the stored phone calls of our near future will no longer be protected by the Fourth Amendment. If that is the case – and current doctrine suggests it is – then it is entirely up to Congress to define the standards for accessing these phone calls. *See* Patricia L. Bellia, "Surveillance Law Through Cyberlaw's Lens," 72 Geo. Wash. L. Rev. 1375 (2004) (analyzing *Miller* and related doctrine).

If Section 209 is retained in its current form, then the stored phone calls of our near future will be available to law enforcement with less than a probable cause warrant. Now we see how misleading it is to describe Section 209 as "seizure of voice mail messages pursuant to warrants." Section 209 applies to *all* stored "wire" communications (that is, to all stored telephone communications), and not just to voice mail. In addition, Section 209 would often allow law enforcement access to these conversations with less than a warrant, such as through a 2703(d) order.

What is to be done with Section 209? To avoid deception, the first step is to rename it to match the statutory text: "Seizure of stored telephone communications with less than a wiretap order." Next, this Committee should place questions to the

Department of Justice to confirm its understanding of the issues discussed here. At the end of my testimony I have proposed a set of questions to help uncover the actual effect of Section 209 on telephone communications. Asking these questions will go a long way toward creating a shared understanding of what is and is not implicated by a renewal of Section 209. That shared understanding, in turn, is essential to any informed consideration of what legislative steps to take.

In terms of possible actions, one option of course would be to let the provision sunset. The argument in favor of this option is that Section 209 is a wide-ranging authorization for the government to listen to phone conversations with less than a wiretap order. In light of that large effect on listener privacy, the relatively small gains to law enforcement due to access to voice mails quite possibly are not worth it.

A second option would be actually to amend the statute to match its current name – voice mails placed by one person could be governed by Section 2703, but communications among two or more parties would be governed by the wiretap laws. To address one practical issue raised by the Department of Justice in its Field Guidance on Section 209, it may be possible for law enforcement in good faith to open files where it does not reasonably believe that the files contain stored wire communications, but then apply the statutory suppression remedy of Section 2515 to prevent use of the inadvertently-opened files in subsequent investigations and proceedings.

Based on responses by the Department of Justice, it may be possible to develop other options that meet priority law enforcement needs without opening a large fraction of telephone calls to surveillance with less than a wiretap order.

Section 217, The Computer Trespasser Exception

I am sympathetic to having some form of the computer trespasser exception in Section 217, but the current version lacks logical safeguards against abuse. The discussion here gives the rationale for the provision, and then explains the needed safeguards, which should include written authorization, reporting requirements, and a statutory suppression remedy.

The problems that led to creation of Section 217 are discussed in my 2001 article "Administration Wiretap Proposal Hits the Right Issues But Goes Too Far," available at http://www.brookings.edu/dybdocroot/views/articles/fellows/2001_swire.htm, and in Orin S. Kerr, "Internet Surveillance Law After the USA PATRIOT Act: The Big Brother That Isn't," 97 Nw. U. L. Rev. 607 (2003). In brief, problems arose in how law enforcement could work with the owners of computer systems that are under attack. The pre-2001 law generally allowed a system owner to monitor the system to prevent and respond to attacks. It also allowed a system owner to turn over to police evidence of criminal attacks that had already occurred. What the pre-2001 law did not allow, however, was for law enforcement to "look over the shoulder" or "surf behind" the owner of the computer system. The policy concern about "looking over the shoulder" is that it can lead to too much surveillance. Law enforcement and system owners could agree that

the law enforcement officials would be permanently stationed in communication companies, monitoring anything suspicious. A particular concern is that system owners might feel pressured to allow law enforcement officials on the premises, leading to virtually unlimited wiretapping.

The pre-2001 rules were frustrating for system owners who wanted to ask the police for help with computer attacks. If intruders are coming into a system regularly, for instance, the owner might want the police to lie in wait for the attack and then use a trap and trace order to follow the intruder back to the source. Before 2001, however, the police could not take up residence and wait for a future attack. The problem was especially acute for the Department of Defense, which is subject to an enormous number of hacking attacks and which could not coordinate easily with law enforcement under the pre-2001 rules. The pre-2001 law also posed problems for smaller enterprises, which often lack the technical expertise to defend their own systems against attack and thus wish to have police help.

The idea of the computer trespasser exception first surfaced within the Department of Justice in 1999. We discussed it within the Administration during 2000, but it was not a subject of Congressional hearings and we did not include it in our 2000 proposal. The idea was included in the Bush Administration's proposal and was enacted in the Patriot Act. Because the idea was so new, it was properly made subject to the sunset provision, so that this Committee and the entire Congress can consider how to proceed.

In considering Section 217, I believe the Committee should have two simple goals in mind: (1) Section 217 should enable system owners and law enforcement to coordinate effectively in facing hacker attacks; and (2) Section 217 should not become a license for widespread wiretapping by law enforcement. My view is that the current language does an effective job of meeting the first goal. The current language, however, lacks the logical safeguards that are needed to achieve the second goal, and I therefore propose three modifications.

First, the authorization from the owner or operator of the system should be in writing. Currently, one of the requirements to use the computer trespasser exception is that "the owner or operator of the protected computer authorizes the interception." My proposed change is to insert "in writing" after "interception." This simple step will be eminently routine in ordinary investigations. It will provide the name of the person inside the organization who takes responsibility for inviting law enforcement to review the e-mails and other computer traffic at the organization. If there is any dispute after the fact about what happened, law enforcement will have the benefit of being able to show the authorization. The system owner or operator will have the benefit of knowing that an employee has taken a proven, written step to authorize law enforcement to enter. That will reduce the risk that any law enforcement officers will talk their way into a computer system without true consent by the system owner. In addition, customers and users of the system will have the benefit of knowing that the system owner actually did consent to having communications monitored. Overall, a simple writing requirement reduces the

risk of irregularity before the monitoring of communications occurs.

Second, Section 217 should have reporting requirements to Congress and the public. So far as I know, there is currently no public information about how often and in what contexts Section 217 has been used. This sort of public reporting would reduce the risk that Section 217 will be used in a widespread way to wiretap communications.

Third, and most importantly, there should be a statutory suppression remedy for exceeding the scope of permitted wiretapping. I will briefly explain the reasons to have a suppression remedy generally for "electronic" communications, and then show why the need is especially compelling with respect to Section 217.

Since 1968, Title III has had the suppression remedy of 18 U.S.C. § 2515 for all "wire" and "oral" communications. This rule was initially introduced in the wake of extensive evidence of persistent and illegal wiretaps under previous law, such as the abundant documentation in the American Bar Association study led by Samuel Dash. In the ECPA compromise in 1986, interception of e-mails and other "electronic" communications were made subject to the strict Title III standards, except the suppression remedy was not included. The Clinton Administration recommended the suppression remedy to Congress in 2000, and this Committee approved it with only one dissenting vote. Then, unfortunately, the provision was not included in the Bush Administration proposal in 2001 and it is not current law.

The lack of a suppression remedy means that law enforcement can violate the wiretap laws with respect to e-mail and web surfing with essentially no legal repercussion. The likelihood of criminal prosecution against a law enforcement official for wiretapping is remote or non-existent – the first such prosecution has not yet been brought. Any suppression remedy under the Fourth Amendment is highly speculative at this time, when it is not even clear that the courts would find a constitutional "reasonable expectation of privacy" in e-mails. This lack of a statutory suppression remedy obviously creates a risk to due process and privacy, because the fruit of illegal access to e-mail can be used in investigations and introduced in court. Importantly, as Professor Orin Kerr has persuasively argued, the lack of a suppression remedy also impedes law enforcement. The reason is that there is a great lack of clarity of how the law applies to new technology. Having a suppression remedy, in the eyes of former DOJ prosecutor Kerr, would assist investigations because the lines of permitted and prohibited behavior would be clarified. Kerr also points out that current interpretation of the surveillance law for "electronic" communications largely occurs in civil cases, and having a suppression remedy would allow the Department of Justice a much greater and more effective role in shaping that law over time. Orin S. Kerr, "Lifting the 'Fog' of Internet Surveillance: How a Suppression Remedy Would Change Computer Crime Law," 54 Hastings L.J. 805 (2003).

The compelling case for a statutory suppression remedy is even stronger with respect to Section 217. The current version of Section 217 essentially assumes that law enforcement will always follow its conditions. Section 217 requires: (1) authorization by

the owner or operator; (2) a lawful investigation; (3) reasonable grounds to believe the intercepted communications will be relevant to an investigation; and (4) such interception does not acquire other communications. What happens if law enforcement violates one or more of those requirements? Nothing. To take a glaring example, suppose that law enforcement arm-twists a major ISP to let law enforcement camp at the ISP and look at all the e-mails. Under current Section 217, all of the e-mails of all of the users could become grist for future investigations. All of them could be used in subsequent trials, against ordinary e-mail users who had no connection at all to computer hacking.

The members of this Committee and I share the hope and belief that this sort of violation of wiretapping laws is not occurring today. But this Committee has the responsibility to craft the legal rules to prevent that abuse in the future. The current Section 217 has no safeguards against widespread "electronic" wiretapping. Section 217 permits owners of computer systems to invite law enforcement in to help with proper investigations. Those goals of Section 217 can be achieved while also assuring that Section 217 does not become an excuse for law enforcement to enter computer systems and look at so many other personal communications.

Section 220, Nationwide Service of Search Warrants for Electronic Evidence

The Committee has also asked me to comment on Section 220, which allows nationwide service of search warrants for electronic evidence. I will briefly explain my understanding of the rationale for the provision, which I support.

In 1986, when ECPA was passed, the local telephone company could generally fulfill a trap and trace order - the call came from a readily-identified phone number in a unified phone network. By 2001, the network had become far more complicated. To trace the source of an e-mail, law enforcement first had to serve a trap and trace order on the local Internet service provider. That provider then might tell police that the e-mail came from a backbone provider, who got it from another backbone provider, who got it from another service provider elsewhere, who might finally be able to identify the sender of the e-mail.

Before 2001, law enforcement had to get one court order from a judge at the first stage, and a separate court order from another judge at each stage later on. This was time-consuming, expensive, and largely redundant because the first federal judge had already approved the order. The Clinton Administration in 2000 and the Bush Administration in 2001 thus both proposed to allow one order to be effective nationwide, back to the source of the particular communication.

One criticism I have heard of this change is that prosecutors might shop around for a judge who will approve an order based on slender evidence. I have heard no evidence to support that this is happening. Oversight questions to the Department of Justice are appropriate to learn whether the Department has concentrated its requests for nationwide orders in front of certain judges. If such a pattern does exist, the Department

should be requested to explain the reasons for it and what measures it has taken to prevent forum-shopping abuse.

Conclusion

I thank the Committee for inviting me to testify today, and commend the detailed examination of the Patriot Act that is occurring this year. If I can be of any further assistance to the Committee as it proceeds, I would be honored to do so.

Contact information:
Professor Peter P. Swire
phone: (240) 994-4142
e-mail: peter@peterswire.net
web: www.peterswire.net

Proposed Questions for the Department of Justice about Section 209 of the Patriot Act

1. Assume that a stored recording of a telephone conversation is made by a network administrator without notice to the two parties. Do the two parties to the telephone conversation retain the same "reasonable expectation of privacy" in the stored conversation that they would have if the conversation was not stored? If so, would the Fourth Amendment protections be lower in any respect than those set forth in *Berger v. New York*?

2. Does your answer to Question 1 differ if the network administrator has provided general notice, such as through the terms of use, that caching and other storage of telephone conversations may occur for network security and other reasons?

3. Assume that one party to a telephone conversation, which is conducted by VoIP on a computer, keeps a stored record of the conversation on that computer. Assume that the other party does not know the conversation is being recorded. Does either party to the conversation have a "reasonable expectation of privacy" in the contents of that conversation, so that Fourth Amendment protections apply?

4. Does your answer to Question 3 differ if both parties know the conversation is being recorded? Has the party who is not doing the recording thereby consented to waiving Fourth Amendment protections?

5. Does Section 209 as it currently exists allow law enforcement seizure of stored wire communications other than voice mails?

6. Does Section 209 as it currently exists apply to the fact setting of Question 1?

7. Does Section 209 as it currently exists apply to the fact setting of Question 2?

8. Does Section 209 as it currently exists apply to the fact setting of Question 3?

9. Does Section 209 as it currently exists apply to the fact setting of Question 4?

10. Assume that VoIP telephone transmissions are done through a "store and forward" system in which there is transient storage of phone conversations as packets move from one part of the Internet to the next. Would this form of storage be enough to permit seizure of the stored recordings of telephone conversations under Section 209? Would it be enough under the panel decision in U.S. v. Councilman? Would it be enough under the Department of Justice position as set forth in the briefs in U.S. v. Councilman for the en banc First Circuit?

11. Under Section 209 as it currently exists, are there any circumstances in which law enforcement can seize stored voice mail or a stored telephone conversation recording by use of a 2703(d) order or any other procedure that is less strict than a search warrant issued by a neutral magistrate?

12. Please provide the Committee with information on the extent to which the new authority in Section 209 has been used in anti-terrorism cases. Has the new authority been used in any anti-terrorism investigations or prosecutions? Approximately what proportion of uses of the new authority has been for use in anti-terrorism cases?