Testimony of Orin S. Kerr
Associate Professor, George Washington University Law School
United States Senate, Select Committee on Intelligence,
Hearing on The USA Patriot Act
February 19, 2005

Mr Chairman, Members of the Committee:

My name is Orin Kerr, and I am an Associate Professor at George Washington University Law School. It is my pleasure to submit this written testimony concerning the USA Patriot Act. My testimony will contain three parts: first, a brief explanation of my view that the public debate over the Patriot Act largely has misunderstood the Act; second, an overview of the legal issues raised by foreign intelligence surveillance; and third, an analysis of the constitutional issues raised by orders to compel information such as library records, bookstore records, and Internet communications.

I. The Debate Over the USA Patriot Act

The public debate over the USA Patriot Act has been based on a number of major misunderstandings about the scope and effect of the law. Millions of Americans believe that the Patriot Act profoundly reshaped the balance between privacy and security in a post-9/11 world. That is simply wrong. The truth is that the law is much more modest: Most of the Patriot Act consists of

minor adjustments to a set of preexisting laws, such as the Foreign Intelligence Surveillance Act and the Electronic Communications Privacy Act. The Patriot Act left the basic framework of preexisting law intact, offering mostly minor changes to the set of statutory privacy laws Congress first enacted in the 1970s and 1980s. I explained this in greater depth in a law review article published in January 2003, and stand by that view today. *See* Orin S. Kerr, *Internet Surveillance Law After the USA Patriot Act: The Big Brother That Isn't*, 97 Northwestern University Law Review 607 (2003), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=317501.

Fortunately, the gap between the perception and the reality of the Patriot Act is beginning to narrow. In recent months, critics of the Patriot Act have come to acknowledge that most of the Act is consensus legislation that does not raise civil liberties concerns. For example, in an April 5, 2005 press release the American Civil Liberties Union acknowledged that:

> most of the voluminous Patriot Act is actually unobjectionable from a civil liberties point of view and . . . the law makes important changes that give law enforcement agents the tools they need to protect against terrorist attacks. A few provisions . . . must be revised. . . . .
>
> I.

See *Bipartisan Legislation Would Fix Worst Parts of Patriot Act While Maintaining Key Law Enforcement Powers*, available at http://www.aclu.org/SafeandFree/SafeandFree.cfm?ID=17935&c=206.

Although it is unfortunate that this acknowledgment appeared as late as it did, the ACLU's recognition that the Patriot Act debate is actually quite narrow is an important step to understanding Patriot Act reform. It reveals that the differences among pre-Patriot Act law, the law under the Patriot Act, and proposals to reform the Patriot Act tend to be relatively small. Of course, any legislative proposals that impact government power to conduct criminal or intelligence surveillance

must be treated with the greatest consideration and care. Finding the right balance that both gives the government the power it needs to investigate terrorist threats and preserves our precious civil liberties is a very difficult task. At the same time, the effect of the Patriot Act and the scope of proposed amendments to it are much narrower than press accounts would lead one to believe.

II. Overview of the Issues Raised By The USA Patriot Act and Foreign Intelligence Surveillance

I will now turn to an overview of the issues raised by the law of intelligence surveillance to help put the debate in better perspective. At the most basic level, any modern legal regime that allows the government to investigate crime or terrorism must address a number of basic methods for acquiring information. In particular, the law must cover three basic types of authorities:

1) *Authority to conduct physical searches to retrieve physical evidence or collect information*.

2) *Authority to compel third parties to produce physical evidence or disclose information.*

3) *Authority to conduct real-time monitoring over communications networks.*

In the case of criminal investigations, the legal regime that covers these authorities is well-established. The first authority is governed by the traditional Fourth Amendment warrant requirement. The police must have a search warrant based on probable cause to enter a home or business unless a person with apparent or actual authority over the place consents, exigent

circumstances exist, or another exception to the warrant requirement applies. The second authority is governed by the Fourth Amendment rules governing subpoenas. Although many different types of subpoenas exist, and the rules can vary slightly depending on the type of subpoena, the general rule is that the police can compel third parties to disclose information in their possession using a subpoena. A subpoena can be issued under a wide range of circumstances: the information need only be relevant to the government's investigation, and compliance with the subpoena cannot be overly burdensome to the subpoena recipient. Finally, the third authority is regulated primarily by statutory law. Two different laws apply: the interception of contents such as phone calls and e-mails is regulated by the Wiretap Act, 18 U.S.C. §§ 2510-22, and the collection of non-content information such as phone numbers dialed and e-mail addresses is governed by the Pen Register statute, 18 U.S.C. §§ 3121-27. The former requires the law enforcement to obtain a "super warrant" based on probable cause unless an exception applies, while the latter permits law enforcement monitoring of non-content information under a relevance court order something like a subpoena.

The law governing monitoring for intelligence purposes is somewhat different than the law governing evidence collection for criminal cases. The Fourth Amendment's requirements are much less clear – and generally less strong – than in the routine criminal context. As a general matter, the few courts that have confronted how the Fourth Amendment applies to intelligence collection have held that the rules are somewhat similar to the rules for criminal investigations but also more flexible. When the Fourth Amendment applies, information and evidence collection must be reasonable in light of the countervailing demands and interest of intelligence collection. *See* United States v. United States District Court, 407 U.S. 297, 323-24 (1972); In re Sealed Case, 310 F.3d 717, 745-46 (Foreign Int. Surv. Ct. Rev. 2002). This legal framework appears to place Congress in the

primary role of generating the law governing intelligence collection, with the Fourth Amendment serving as a backstop that reviews Congress's approach to ensure that it is constitutionally reasonable.

Congress has responded to the challenge by passing the Foreign Intelligence Surveillance Act, also known as "FISA." FISA attempts to create a statutory regime for intelligence monitoring that largely parallels analogous rules for gathering evidence in criminal cases. FISA covers the three basic authorities as follows: First, 18 U.S.C. §§ 1821-29 covers the authority to conduct physical searches, a parallel to the provision of the Federal Rules of Criminal Procedure that allows investigators to obtain a search warrant in criminal cases. Second, 18 U.S.C. §§ 1861-62 and 18 U.S.C. § 2709 covers authority to compel third-parties to disclose records and physical evidence, a parallel to the provision of the Federal Rules of Criminal Procedure that allows the issuance of subpoenas in criminal investigations. Third, 18 U.S.C. §§ 1801-22 and 18 U.S.C. §§ 1841-45 cover the authority to conduct real-time monitoring over communications networks. Specifically, sections 1801-22 cover the authority to obtain the contents of communications, a parallel to the Wiretap Act used in criminal cases, and sections 1841-45 cover the authority to obtain non-content information, a parallel to the Pen Register Statute used in crime investigations.

The debates over the FISA-related provisions of the Patriot Act focus primarily on the second type of authority: powers to compel third parties to produce physical evidence or disclose information. Specifically, critics object to the weak privacy regulations found in provisions such as Section 215 of the Patriot Act that address the government's power to compel third parties to produce physical evidence or disclose information in intelligence cases. For the most part, these weak privacy regulations match the standards applied in the analogous criminal context. For

example, the Supreme Court has held that a grand jury subpoena can be issued if the order to compel seeks information that may be relevant to a criminal investigation. *See* United States v. R. Enterprises, Inc., 498 U.S. 292 (1991). This authority "paints with a broad brush" by design, permitting subpoenas to be issued ordering third parties to disclose physical evidence and information "merely on suspicion that the law is being violated, or even just because . . . assurance [is sought] that it is not." *Id.* at 297 (quoting United States v. Morton Salt Co., 338 U.S. 632, 642 -643 (1950)). The Supreme Court has justified this low standard on the ground that orders to compel evidence from third parties are preliminary investigative tools designed to determine if more invasive forms of surveillance are necessary. "[T]he Government cannot be required to justify the issuance of a grand jury subpoena by presenting evidence sufficient to establish probable cause because the very purpose of requesting the information is to ascertain whether probable cause exists." *See R. Enterprises, Inc.*, 498 U.S. at 297.

The key question that the Committee must consider is whether a higher standard is appropriate for orders to compel in the context of intelligence investigations. The environment of intelligence investigations is somewhat different than the environment of criminal investigations. For example, subpoenas can be easily challenged and can be complied with under few time pressures, both of which are important explanations for the light legal regulations of subpoenas. *See* United States v. Dionisio, 410 U.S. 1, 10 (1973). At the same time, the harm that intelligence investigations seek to avoid is on average greater than the harm a typical criminal investigation seeks to deter. In addition, it is worth noting that Congress has opted to provide special privacy protections to protect some types of Internet communications and stored e-mails, raising the privacy protection beyond that provided by subpoenas. *See* 18 U.S.C. § 2703. Perhaps Congress should

consider a similar approach in the intelligence context, permitting subpoena-equivalents to be used in some contexts but higher-threshold court orders to be used in other contexts that raise more substantial privacy concerns.

III. Constitutionality of Orders to Compel Library Records and Internet Communications

The statutory regulation of orders to compel evidence from third parties is particularly important because the Fourth Amendment offers little in the way of regulation of such orders. In this final section, I wish to explain the constitutionality of orders to compel, specifically in the context of library records and Internet communications obtained from third party providers. My conclusion is that orders to compel the disclosure of evidence from third parties ordinarily do not require probable cause. Under current law, for example, probable cause is not required to compel libraries to compel library records.

The constitutionality of orders to compel evidence without probable cause can be justified on two alternative grounds. The first is that the disclosure of information to third parties has been held to eliminate Fourth Amendment protection in that information. As the Supreme Court stated in *United States v. Miller*, 425 U.S. 435, 443 (1976):

> This Court has held repeatedly that the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed.

Under the disclosure rationale of *Miller*, third parties normally can be ordered to disclose records

held by them without implicating the Fourth Amendment on the theory that the information was disclosed to them in the course of their coming into possession of the information.

Applying this rationale, courts have uniformly held that an individual does not retain Fourth Amendment rights in non-content records that reveal how that individual used an account or service provided by a third party. A person may reasonably believe that the third party will not disclose the information to the police, but this alone does not create a Fourth Amendment "legitimate" or "reasonable" expectation of privacy in the information. For example, a person does not retain a reasonable expectation of privacy in the information the telephone company retains about how a particular telephone account was used. *See* United States v. Fregoso, 60 F.3d 1314, 1321 (8th Cir. 1995). Similarly, a customer does not retain a reasonable expectation of privacy in the information that Western Union retains about how a particular Western Union account was used. *See* In re Grand Jury Proceedings, 827 F.2d 301, 302-03 (8th Cir. 1987).

The rationale also applies to library records. For example, in *Brown v. Johnston*, 328 N.W.2d 510 (Iowa 1983), a library challenged a subpoena obtained by a state investigator who wanted to gather library circulation records to see if anyone had checked out books relating to cattle mutilation. The Iowa Supreme Court rejected the argument that an ordinary subpoena could not be used to collect library records:

> It is true the State's investigation was only preliminary; and as Brown and the library board argue, no suspects were identified nor was the search for information limited to any named library patrons. This does not diminish the need for the information, however, as we assume the whole purpose in examining the record was to gain enough information so that the investigation could be narrowed.
>
> The State's interest in well-founded criminal charges and the fair administration of criminal justice must be held to override the claim of privilege here. Brown and the library board have cited no cases to us which have reached a contrary conclusion under similar facts, and we have found none. *Id.* at 513.

Although I have been unable to find any cases applying the Fourth Amendment to bookstore records, the same analysis would seem to apply to sales records kept by bookstores. To be sure, some state courts have interpreted their own state constitutional provisions to create greater privacy protections to regulate state police officers in the context of bookstores. *See, e.g.*, Tattered Cover, Inc. v. City of Thornton, 44 P.3d 1044 (Colo. 2002). But as far as I am aware, no court has held that a person retains a reasonable expectation of privacy in their bookstore customer records under the Fourth Amendment. As a general matter, the Fourth Amendment rules that apply to bookstores are the same as the Fourth Amendment rules that apply to other spaces. *See, e.g.,* Maryland v. Macon, 472 U.S. 463 (1985).

Finally, the same rationale applies to non-content Internet account records. Non-content Internet account records are disclosed to the ISP, and are not protected under the Fourth Amendment. *See* United States v. Hambrick, 55 F. Supp. 2d 504, 508 (W.D. Va. 1999), *aff'd*, 225 F.3d 656 (4th Cir. 2000) (unpublished opinion); United States v. Kennedy, 81 F. Supp. 2d 1103, 1110) (D. Kan. 2000) (same).

This does not mean an individual can never have a reasonable expectation of privacy in information held by third parties. Existing caselaw focuses on whether the information transferred to the third-party is disclosed to the third party or is sealed away from them. If a person gives third party a sealed container to hold on their behalf, then that person retains a reasonable expectation of privacy in the unexposed contents of that sealed container. *See, e.g.,* United States v. Most, 876 F.2d 191, 197-98 (D.C. Cir. 1989); United States v. Barry, 853 F.2d 1479, 1481-83 (8th Cir. 1988). For that reason, a person retains a reasonable expectation of privacy in the contents of sealed postal

letters or packages sent via UPS or FedEx until the point that the letters and packages arrive at their destination. *See* Ex Parte Jackson, 96 U.S. (6 Otto) 727, 733 (1877); Walter v. United States, 447 U.S. 649, 651 (1980).

It is unclear under current law how the sealed/unsealed distinction applies to disclosed information such as Internet communications, particularly in the context of the contents of Internet communications. Courts may conclude that by sending an e-mail, the user discloses that e-mail to an ISP under *Miller*. On the other hand, courts may conclude that the contents of e-mail can be analogized to the contents of a sealed letter, and thus retain Fourth Amendment protection. At the current time, all we know is that the Fourth Amendment does not protect non-content information held by ISPs, and may or may not protect content information held by ISPs. Notably, this uncertainty is part of what led Congress to impose greater statutory protections in the case of e-mail contents sought in criminal investigations under 18 U.S.C. § 2703(a).

Finally, existing cases suggest that a subpoena or equivalent order to compel without probable cause may be constitutionally sufficient even if a suspect retains a reasonable expectation of privacy in the information. The case here are sparse, as the courts have decided few cases in which the government ordered a third party to disclose sealed packages. But the few cases on this question suggest that the government can subpoena information even if that information is protected by a reasonable expectation of privacy; no probable cause warrant is required. *See* United States v. Barr, 605 F. Supp. 114, 119 (S.D.N.Y. 1985) (permitting subpoena served on third-party mail service for undelivered mail); United States v. Schwimmer, 232 F.2d 855, 861-63 (8th Cir. 1956) (permitting subpoena served on third-party storage facility for private papers in facility's possession); Newfield v. Ryan, 91 F.2d 700, 702-05 (5th Cir. 1937) (permitting subpoena served on telegraph

company for copies of defendants' telegrams).

In light of these cases, current law points to the use of orders to compel evidence as being constitutional in the Fourth Amendment in most if not all cases without a requirement of probable case. The most difficult and least clear cases are orders to compel content records, such as the contents of e-mails and sealed letters. In most circumstances, however – and clearly in the case of non-content records such as library records – orders to compel evidence do not require probable cause under the Fourth Amendment.
