Testimony of Orin S. Kerr
Associate Professor, George Washington University Law School
United States House of Representatives
Committee on the Judiciary
Subcommittee on Crime, Terrorism, and Homeland Security
Hearing on Section 212 of the USA Patriot Act
May 5, 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, and specifically on the emergency disclosure provision found in Section 212 of the USA Patriot Act. My testimony will articulate why I believe Section 212 should be retained. In my view, Section 212 and its analogous provisions for content information are important measures that recognize the need for balance in a regime of electronic privacy, help match statutory law to the contours of the Fourth Amendment, and do not threaten civil liberties. I will begin by offering a broad perspective on the Stored Communications Act and Internet privacy, and then turn specifically to the importance of Section 212 of the USA Patriot Act and its analogous provision for contents.

I. The Goal of the Stored Communications Act

An obvious place to start is by understanding why Internet privacy is a problem for Congress to address. In other words, why are we here today? In most investigations into traditional criminal

offenses, the rules regulating government access to private information are provided by the Fourth Amendment to the United States Constitution. The Fourth Amendment's prohibition against unreasonable searches and seizures regulates police conduct by regulating what spaces the police can enter and what physical property they can take away. Entering a private space such as a home is a Fourth Amendment "search," and taking away physical property is a "seizure." Under existing Supreme Court case law, a probable cause warrant is required to enter a home and retrieve evidence unless an exception such as exigent circumstances applies.

The question is, what changes when we switch from traditional physical crime cases to Internet crime cases? The answer is that computer networks add a third-party intermediary to the picture. Evidence is no longer stored exclusively in the home, but now is often stored with Internet service providers, as well. The police can obtain some information not by entering the home and retrieving physical information, but rather by obtaining information from a suspect's Internet service provider. Under existing Supreme Court caselaw, the Fourth Amendment has a difficult time protecting this information. First, the Fourth Amendment generally offers no protection to information disclosed to third parties, which may very well apply to ISPs. Second, under the "private search" doctrine, private parties such as Internet service providers have unlimited power under the Fourth Amendment to search through documents in their possession and disclose the results to law enforcement. As the Supreme Court stated in *United States v. Jacobsen*, 466 U.S. 109, 113 (1984), the Fourth Amendment "is wholly inapplicable to a search or seizure, even an unreasonable one, effected by a private individual not acting as an agent of the Government or with the participation or knowledge of any governmental official."

The gap in constitutional protection creates an obvious need for Congressional regulation. In

1986, Congress answered the call by enacting a comprehensive statutory framework as part of the Electronic Communications Privacy Act ("ECPA"), Pub.L. 99-508, 100 Stat.1848 (1986). ECPA erected a complicated statutory regime that generates the equivalent of Fourth Amendment protections on-line by statute. The statute restricts the power of investigators to compel evidence from ISPs and places limits on the ability of ISPs to voluntarily disclose information about their subscribers. The basic goal of the statute is to create Fourth Amendment-like protections for Internet communications. The Stored Communications Act, 18 U.S.C. §§ 2701-11, is an important part of ECPA. Roughly speaking, the Stored Communications Act regulates the exchange of information between ISPs and the government in the case of stored communications and existing account records. The goal of the statute is to restore the kind of limits on government access that might exist under the Fourth Amendment in the analogous setting of physical-world crimes. *See generally* Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 George Washington Law Review 1208, 1209-13 (2004).

The emergency disclosure provisions at issue in this hearing concern exceptions to the ban on voluntary disclosure by Internet service providers found in the Stored Communications Act. 18 U.S.C. § 2702 generally bans Internet service providers from disclosing to the government either the contents of customer communications (such as private e-mails) or records relating to customer account usage (such as the e-mail addresses a person sent messages to over a period of time). Section 212 of the USA Patriot Act added an exception to that ban: it provides that an Internet service provider can disclose non-content records to the government "if the provider reasonably believes that an emergency involving immediate danger of death or serious physical injury to any person justifies disclosure of the information." 18 U.S.C. § 2702(c)(4). In 2002, the Homeland Security Act, Pub.

L. 107-296, slightly modified the preexisting analogous exception for the disclose of contents to the government. The exception is slightly broader for content information than for non-content records; it provides that an Internet service provider can disclose content to the government "if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of communications relating to the emergency." 18 U.S.C. § 2702(b)(8).

II. The Importance and Role of Emergency Disclosure Provisions Under the Stored Communications Act

The emergency disclosure provisions of 18 U.S.C. § 2702(b)(8) and 18 U.S.C. § 2702(c)(4) do not threaten civil liberties, play an important role in a balanced regime of on-line privacy, and match the privacy protections of the Fourth Amendment. Without emergency exceptions such as these, Internet service providers would be barred from disclosing records and contents of communications to the government even when human life is at stake. The law has long allowed ISPs to disclose communications when their legitimate business interests are implicated, *see* 18 U.S.C. § 2702(b)(5), 18 U.S.C. § 2702(c)(3). It would be deeply troubling if the law valued the business interests of ISPs more highly than innocent human lives. The emergency disclosure provisions of 18 U.S.C. § 2702 recognize the commonsense notion that interests in privacy can be outweighed by competing threats to serious bodily injury and life itself.

When might these exceptions be used? Consider two examples. Imagine someone e-mailed a death threat, and the police needed to know who sent the threat to find the wrongdoer or perhaps

to find co-conspirators. The ISP may know this information: they will know who registered the account, and they have access under 18 U.S.C. § 2701(c)(1) to the sender's e-mail account which may reveal the scope of the conspiracy. Without the emergency exception, however, they would be unable to disclose that information to law enforcement. Alternatively, imagine that a kidnaper made a ransom call from a cell phone, and the police wanted to know where the phone was located so they could find the kidnaper and free his victim. Absent an emergency exception, the ISP would be barred by 18 U.S.C. § 2702 from disclosing the location of the cell phone even to safe the life of the victim.

I was a lawyer at the Computer Crime and Intellectual Property Section of the Justice Department from 1998-2001, before the emergency disclosure provision of Section 212 was added, and I remember the prevailing practices within law enforcement at that time. The police and the ISP were forced to rely on an awkward and time-consuming legal fiction to facilitate disclosure. If an ISP contacted government agents seeking to disclose records in an emergency, the following procedures were used: first, government agents would refuse to accept the disclosure, citing the ban in 18 U.S.C. § 2702; second, government agents would go to a lawyer and get the lawyer to apply for and obtain a court order "compelling" the provider to disclose the information under 18 U.S.C. § 2703; third, a judge would sign the court order, compelling the ISP to disclose the information; and then fourth, the agents would inform the ISP that they could finally accept the disclosure. In cases where time was of the essence, this procedure added considerable delay with little to no added benefit.

The emergency disclosure provisions are also consistent with traditional Fourth Amendment principles. One of the traditional principles of Fourth Amendment law is that exigent circumstances can justify taking investigatory steps without first obtaining a court order. *See, e.g.,* Schmerber v. California, 384 U.S. 757, 770-71 (1966). Emergency situations may arise in which the police must

ack quickly. By the time the court order has been obtained, the evidence may be destroyed, the defendant may escape, an innocent person may be hurt, or "some other consequence improperly frustrating legitimate law enforcement efforts" may occur. United States v. McConney, 728 F.2d 1195, 1199 (9th Cir. 1984) (en banc).. In the physical world, this exception permits the police to enter physical spaces and seize physical property under the so-called exigent circumstances exception to the warrant requirement.

These principles can be carried over to Internet crime cases involving ISPs, and are embodied in the emergency disclosure provisions of Section 2702. Granted, the factual picture is a bit different. The privacy invasion is less severe in a number of ways, for example. The police do not enter any physical spaces and do not seize any physical property. The information is held by a third-party provider, and the question is whether that third party can disclose the information voluntarily, not whether the government can forcibly compel the information. In addition, the range of possible threats to safety or law enforcement interests are narrower: exigencies primarily tend to involve harm to an innocent victim rather than the broader set of interests including destruction of evidence that are implicated regularly in traditional exigent circumstances cases.

At the same time, the emergency disclosure provisions in 18 U.S.C. § 2702 are best understood as the Internet equivalents of the traditional warrant exception for exigent circumstances. The police may conduct warrantless searches and seizures under the exigent circumstances exception when a "plausible claim of specially pressing or urgent law enforcement need" exists and that claim outweighs the nature of the privacy intrusion. *Illinois v. McArthur*, 531 U.S. 326, 331 (2001). The analogous statutory exceptions apply when a plausible or good-faith claim of an "emergency" involving danger of "death or serious physical injury" exists and justifies the disclosure. 18 U.S.C.

§ 2702(b)(8), (c)(4). While the test is not exactly the same, the same principle applies translated to the ISP context. The goal is to permit a balancing of interests between privacy and emergency needs. Section 212 and its content equivalent reflects the same balancing effort found in the exigent circumstances doctrine of the Fourth Amendment.

Thank you for providing me with the opportunity to testify.