Department of Justice

STATEMENT

OF

WILLIAM E. MOSCHELLA
ASSISTANT ATTORNEY GENERAL
OFFICE OF LEGISLATIVE AFFAIRS
DEPARTMENT OF JUSTICE

BEFORE THE

SUBCOMMITTEE ON CRIME, TERRORISM, AND HOMELAND SECURITY
COMMITTEE ON THE JUDICIARY
HOUSE OF REPRESENTATIVES

CONCERNING

THE EMERGENCY DISCLOSURE PROVISION OF THE USA PATRIOT ACT (§ 212)

PRESENTED ON

MAY 5, 2005

Statement of
William E. Moschella
Assistant Attorney General
Office of Legislative Affairs
Department of Justice

Before the
Subcommittee on Crime, Terrorism, and Homeland Security
Committee on the Judiciary
United States House of Representatives

Concerning
The Emergency Disclosure Provision of the USA PATRIOT Act (§ 212)

May 5, 2005

Chairman Coble, Ranking Member Scott, and Members of the Subcommittee:

It is my pleasure to appear before you today to discuss section 212 of the USA PATRIOT Act. On September 11, 2001, our Nation suffered a great tragedy. In the wake of this horrendous attack on American soil, we mourned the loss of the thousands of citizens who perished on that fateful day. Almost immediately, the Federal government took steps to prevent such a tragedy from ever happening again. Members of both parties worked to develop comprehensive legislation to achieve four objectives: (1) ensure that law enforcement was provided with the tools necessary to uncover and disrupt terrorist plots; 2) update federal law in light of new information and technology; 3) facilitate information sharing; and 4) safeguard our citizens' civil rights and liberties.

Overwhelming bipartisan majorities in both the House and the Senate passed the USA PATRIOT Act, which was signed into law on October 26, 2001. Since that time, it is difficult to overstate how important the USA PATRIOT Act has been to the Government's ability to preserve and protect our nation's liberty in the face of continuing terrorist threats and serious criminal activity. Thanks in part to this statute, and to the hard work of federal, state and local

law and intelligence investigators around the globe, we have been able to identify terrorist operatives, dismantle terrorist cells, disrupt terrorist plots, and capture terrorists before they have been able to strike.

Sixteen provisions of the USA PATRIOT Act are set to expire on December 31, 2005, including section 212, which we are addressing today. The tools contained in the USA PATRIOT Act have been essential weapons in our arsenal to combat terrorists and criminals alike. We must never forget that terrorist groups pose a continuing and real threat to the safety and security of the American people today. For this reason, I strongly urge Congress to reauthorize all provisions of the USA PATRIOT Act that are scheduled to sunset at the end of this year. We live in a post-9/11 world, and our laws must reflect such circumstances.

Prior to the enactment of the USA PATRIOT Act, Federal law contained no special provisions that would allow electronic communication service providers to voluntarily disclose customer records or communications to Federal authorities in emergency situations. For example, if an Internet service provider (ISP) possessed information that could have prevented an imminent terrorist attack if disclosed to the Government, and the ISP ultimately disclosed the information voluntarily, the ISP could be sued civilly by the customer whose records or communications had been released. Providing such information did not fall within one of the statutory exceptions to the limitations on disclosure contained in the Electronic Communications Privacy Act (ECPA), even if that disclosure was necessary to save lives. Moreover, Federal law did not expressly permit an ISP to voluntarily disclose non-content customer records (i.e. a subscriber's login records) to the Government to protect itself against hacking. The law did, however, allow providers to disclose the content of the customer's communications for this

reason. This created an anomaly in the law – the right to disclose the content of communications should logically imply the less-intrusive ability to disclose non-content records.

Section 212 of the USA PATRIOT Act corrected both of the aforementioned inadequacies. First, section 212 amended 18 U.S.C. § 2702(b)(6) to permit, *but not require*, a service provider to disclose either content or non-content customer records to Federal authorities in emergencies involving an immediate risk of death or serious physical injury to any person. Notably, this provision does not obligate service providers to review customer communications in search of such imminent dangers, nor does it impose an obligation to disclose records once the provider becomes aware of an emergency - it is a purely voluntary authority. Second, section 212 amended ECPA to allow service providers to disclose non-content information in an effort to protect their own rights and property. *See* 18 U.S.C. § 2702(c)(3).

Plainly, section 212 of the USA PATRIOT Act allows electronic communications service providers to disclose either customer records or the content of customers' communications to a government entity in any emergency situation that involves an immediate danger of death or serious physical injury. This is analogous to allowing citizens to tell police that, while attending a party at a friend's house, they overheard two people discussing a violent crime they were about to commit.

Furthermore, section 212 works in practice. It has been used often and has already saved lives. To give just a few examples, section 212 was utilized recently in a case involving serious e-mail threats against an Islamic mosque located in Detroit, Michigan. In this case, Michael Bratisax and John Barnett both allegedly sent threatening e-mail messages on different occasions from their home computers in New York to the Imam of the Islamic Center of America in Detroit. The threats included death to the Imam, as well as general threats against all Muslims in

America in response to events in the Middle East. For example, the e-mails included threats such as: "I have an oath too! It is to kill all you [expletive]"; "I pray to get the opportunity to kill a Muslim"; and "I pray every one of Allahs [sic] followers enjoys hell...that's where you belong. Going to send one myself."

The threats were initially reported by the administrator of the mosque to the FBI and thereafter, the FBI conducted an investigation into the matter. During the course of the investigation, due to the life-threatening nature of these e-mail messages, the FBI contacted an Internet service provider asking the ISP to provide subscriber information immediately. The Internet service provider provided the FBI with the requested information the same day the request was made. Section 212 permitted the Internet service provider to voluntarily turn over the necessary subscriber information in this case without fear of civil liability, which allowed the FBI to identify Bratisax and Barnett quickly.

Bratisax and Barnett have been arraigned and charged with the federal crimes of obstructing the free exercise of religious beliefs and transmitting threatening communications in interstate commerce. They are currently awaiting trial.

Section 212 was used in the investigation of a bomb threat against a high school. An anonymous person, claiming to be a student at the high school, posted a disturbing death threat on the Internet, singling out a faculty member and several students to die by bomb and gun. The operator of the Internet site initially resisted disclosing any information about the suspect to law enforcement for fear that he could be sued if he volunteered the information. Once a prosecutor explained that section 212 allowed for voluntary release of information in emergencies, the owner turned over evidence that led to the timely identification of the individual responsible for the bomb threat. The suspect ultimately confessed to making the threats.

Section 212 was also invaluable in the swift resolution of an attack on a computer that controlled the life support systems for the 50 scientists living at the South Pole Research Station in 2003. Authorities, furthermore, used section 212 to foil an alleged kidnapping plot that turned out to be an extortion racket.

Section 212 and other USA PATRIOT Act authorities were also critical to the safe recovery of an 88-year-old Wisconsin woman who was kidnapped and held for ransom in February 2003. Investigators swiftly used sections 210, 212, and 220 of the USA PATRIOT Act to gather information, including communications provided on an emergency basis from Internet service providers, that assisted in identifying several suspects and accomplices and then quickly locating the elderly victim. When the victim was found, she was bound in an unheated shed during a cold Wisconsin winter several feet from a suspect's residence. Thankfully, the victim fully recovered from her ordeal, which had lasted for several days. Without a doubt, the information obtained using section 212 and other provisions of the USA PATRIOT Act was instrumental in solving the case quickly and thus saving the victim's life. The suspect was eventually arrested and was prosecuted and convicted by Wisconsin authorities after it was determined the victim was not transported across state lines and, thus, could be more effectively prosecuted in state court.

Section 212 has further proven to be extremely useful in cases involving missing children. Section 212 assisted authorities with the rescue of a 13-year-old girl who had been lured from her home and was being held captive by a man she met online. In early 2002, FBI agents received a report from the local police department that the girl had disappeared the previous day from her parents' home. The agents interviewed the parents and the girl's friends, one of whom reported that the girl had discussed leaving home with a 38-year-old man she had

met online. In the next couple of days, an anonymous caller contacted the FBI and stated that he had chatted online recently with an individual claiming to have taken a girl from Pittsburgh. Based on information provided by the anonymous caller, FBI agents in Pittsburgh quickly requested information from an Internet service provider pursuant to section 212. With the information provided in response to that request, agents were able to locate the perpetrator. They immediately went to his residence in Herndon, Virginia. At his residence, they rescued the child victim who was found chained up in his bedroom, and, in his basement, investigators discovered what amounted to a dungeon -- filled with various torture devices. The suspect subsequently was arrested, pleaded guilty to charges of travel with intent to engage in sexual activity with a minor and sexual exploitation of a minor, and was sentenced to a prison term of over 19 years. Had the provision of the information by the ISP been slowed, as it would if section 212 were allowed to sunset, who knows what unspeakable horrors that 13-year-old girl would have been subjected by this dangerous predator.

Some opponents of section 212 argue that ISPs should be prohibited from voluntarily disclosing content and non-content communications of their customers in emergency situations, and should only disclose such information when presented with a court order or grand jury subpoena from the Government. These examples make clear, however, that precious time would be wasted in an emergency situation if a court order or grand jury subpoena were required. For example, in a situation where an ISP becomes aware of an emergency that poses a threat to life and limb, the ISP would first have to contact authorities and provide a sufficient basis for authorities to seek a court order; authorities would then have to obtain the order and serve it on the provider. Only then would the critical information be made available. Requiring such a time-consuming procedure would eliminate the vital benefits provided by section 212 because in

some emergency situations, even a matter of minutes may mean the difference between life and death.

The Department of Justice is called upon each and every day to preserve American lives and liberty. In prosecuting the war on terrorism, the Department has taken every appropriate step to prevent acts of terrorism, protect innocent lives, and respect the civil rights and liberties of every citizen. The USA PATRIOT Act has played a vital role in the Department's efforts to preserve America's system of ordered liberty for future generations. The Department strongly urges Congress to remove the uncertainty that comes with having a "sunset" on criminal and national security law authorities by completely repealing section 224 of the USA PATRIOT Act. Thank you and I look forward to answering any questions you may have.