STATEMENT OF
KEVIN V. Di GREGORY
DEPUTY ASSISTANT ATTORNEY GENERAL
UNITED STATES DEPARTMENT OF JUSTICE
BEFORE THE SUBCOMMITTEE ON THE CONSTITUTION
OF THE HOUSE COMMITTEE ON THE JUDICIARY
on
THE FOURTH AMENDMENT and THE INTERNET
April 6, 2000

Mr. Chairman, Congressman Watt, and Members of the Subcommittee, I thank you for this opportunity to testify on the topic of the Fourth Amendment and the Internet. Throughout the proud history of this nation, the Fourth Amendment has stood as the cornerstone of protecting individual privacy from unwarranted governmental intrusion. This basic and vitally important protection is no less applicable in cyberspace than anywhere else in this nation. Just as the Fourth Amendment protects the rights of Americans in their homes, on their phones, and in their cars, so too it protects them while online. This point is beyond dispute. As this nation and Congress continue to consider the appropriate parameters of governmental conduct in cyberspace, the Department of Justice is pleased to participate in the discussion today.

Privacy and Public Safety

One of the themes that will no doubt be repeated throughout this hearing and in the discussion in the months ahead is the challenge of protecting privacy while also protecting public safety. The founders of this nation, while concerned about the government's disregard and abuse of privacy in England, recognized that in order for our democratic society to remain safe and free, law enforcement must have the ability to investigate, apprehend, and prosecute people for criminal conduct. Recognizing the tension between privacy and public safety, the founders adopted the Fourth Amendment to the Constitution, which by its very terms strikes a balance. Under the Fourth Amendment, the government must satisfy the probable cause standard before obtaining a warrant for a search, arrest, or other significant intrusion on privacy.

Congress and the courts have also recognized that lesser intrusions on privacy should be permitted under a less exacting threshold. In the computer context, the Electronic Communications Privacy Act ("ECPA") establishes a three-tier system by which the government can obtain stored information from electronic service providers. In general, the government needs a search warrant to obtain the content of unopened communications (like e-mail), a court order to obtain transactional records, and a

subpoena to obtain subscriber information. See 18 U.S.C. §§ 2701-11.
Because of the privacy values it protects, the wiretap statute, 18 U.S.C. §§ 2510-22, commonly known as Title III, places a higher burden on the real-time interception of oral, wire and electronic communications than the Fourth Amendment requires. In the absence of a statutory exception, the government needs a court order to wiretap communications, including a showing that normal investigative techniques for obtaining the information have or are likely to fail and that any interception will be conducted to ensure that the intrusion is minimized.

The safeguards to privacy represented by the Fourth Amendment and statutory restrictions on government access to information do not prevent effective law enforcement. Instead, they provide boundaries for law enforcement - clarifying what is acceptable evidence gathering and what is not. At the same time, those who care deeply about protecting individual privacy must also acknowledge that law enforcement has a critical role to play in this vital function. When law enforcement successfully investigates, apprehends, and prosecutes a criminal who has stolen a citizen's personal information from a computer system, law enforcement is undeniably working to protect privacy and deter further privacy violations. The same is true when law enforcement apprehends a hacker who compromised the financial records of a bank customer.

As we move into the 21st century, we must ensure that the needs of privacy and public safety remain in balance and are appropriately reflected in the new and emergency technologies that are changing the face of communications. Although the primary mission of the Department of Justice is law enforcement, Attorney General Reno and the entire Department understand and share the legitimate concerns of all Americans with regard to personal privacy. The Department has been and will remain committed to protecting the privacy rights of individuals. We look forward to working with Congress and other concerned individuals to address these important matters in the months ahead.

Law Enforcement challenges in cyberspace:

While the Fourth Amendment is over 200 years old, the Internet, relatively speaking, is still in its infancy. Yet the technological advances of the past five to fifteen years have changed forever the landscape of society, not just in America, but worldwide. The Internet has resulted in new and exciting ways for people to communicate, transfer information, engage in commerce, and expand their educational opportunities. These are but a few of the wonderful benefits of this rapidly changing technology. But as has been the case with every major technological advance in our history, we are seeing individuals and groups use this technology to commit criminal acts. As Deputy Attorney General Eric Holder told the Crime Subcommittee of this Committee in February, our vulnerability to computer crime is astonishingly high and threatens not only our financial well-being and our privacy, but also this nation's critical infrastructure.

Many of the crimes that we confront everyday in the physical world are beginning to appear in the online world. Crimes like threats, extortion, fraud, identity theft, and child pornography are migrating to the Internet. The Fourth Amendment and laws addressing

privacy and public safety serve as a framework for law enforcement to respond to this new forum for criminal activity. If law enforcement fails to properly respect individual privacy in its investigative techniques, the public's confidence in government will be eroded, evidence will be suppressed, and criminals will elude successful prosecution. If law enforcement is too timid in responding to cybercrime, however, we will, in effect, render cyberspace a safe haven for criminals and terrorists to communicate and carry out crime, without fear of authorized government surveillance. If we fail to make the Internet safe, people's confidence in using the Internet and e-commerce will decline, endangering the very benefits brought by the Information Age. Proper balance is the key.

In this vein, it is important to note the distinction between computer security and responding to computer crime. As the President made clear during the Cyber-security summit he held with Internet leaders in February, enhancing computer security - like designing locks on doors - is primarily, though not entirely, the responsibility of the private sector, not the government. The reason is straightforward -- most networks and computer systems are in private hands. Without private sector cooperation, a "full-court press" by the Government would end up installing only a few locks on the cyber-doors of our Nation.

When a crime does occur online - when the locks are broken and a person or company is victimized - law enforcement, whether local, state or federal, has an obligation to respond. Enhanced computer security is vital, but ultimately it will take the combined efforts of the private sector, law enforcement, and the online public to make cyberspace secure. Indeed, just yesterday, the Attorney General and numerous representatives from United States Attorneys Offices and law enforcement met with industry leaders in California to discuss issues related to Internet security, particularly matters of mutual concern that arise after an intrusion has occurred.

I would also note that although my testimony primarily focuses upon the technical and legal challenges faced today, the third challenge - resources - also bears directly on preserving individual privacy. The ability to recruit, train, equip, and retain law enforcement in all aspects of combating cybercrime is essential to our success. The Department of Justice believes that any comprehensive training program must include education on the privacy-related aspects of online investigation.

In developing a response to crime online, there are a number of factors that must be given careful consideration. There are, as the Deputy Attorney General recently stated, essentially three categories of major challenges facing law enforcement in cyberspace today. These are:

1. Technical challenges that hamper law enforcement's ability to locate and prosecute criminals that operate online;

2. Certain substantive and procedural laws that have not kept pace with the changing technology, creating significant legal challenges to effective investigation and prosecution of crime in cyberspace; and

3. Resource needs that must be addressed to ensure that law enforcement can keep pace with changing technology and has the ability to hire and train people to fight cybercrime.

For purposes of this hearing - the Fourth Amendment and the Internet - my testimony will focus primarily on the first two challenges: the technical barriers to investigation and the need to update existing laws to fully account for emerging technologies.

Technical Challenges:

Recent history has shown that tracking a criminal online is not always an impossible task. For example, last year federal and state law enforcement combined to successfully apprehend the creator of the Melissa virus and the individual who created a fraudulent Bloomberg News Service website in order to artificially drive up the stock price of PairGain, a telecommunications company based in California. While we are proud of these important successes, we still face significant challenges as online criminals become more and more sophisticated.

In nearly every online case, tracking the online criminal requires law enforcement to attempt to trace the "electronic trail" from the victim back to the perpetrator. In effect, this "electronic trail" is the fingerprint of the twenty-first century - only much harder to find and not as permanent as its more traditional predecessor. In the physical world, a criminal and his victim are generally in the same location. But cybercriminals do not have to physically visit the crime scene. Instead they cloak their illegal activity by weaving communications through a series of anonymous remailers, by creating forged e-mail headers with powerful point and click tools readily downloadable from hacker websites, or by using a "free-trial" account or two - and then are often able to "wipe clean" the logging records that would be evidence of their activity.

In some cases, the criminal may not even be in the same country as the victim. The global nature of the Internet, while one of the greatest assets of the Internet to law-abiding citizens, allows criminals to conduct their illegal activity from across the globe. In these cases, the need to respond quickly and track the criminal is increasingly complicated and often frustrated by the fact that the activity takes place throughout different countries. With more than 190 countries connected to the Internet, it is easy to understand the coordination challenges that face law enforcement. Furthermore, in these cases, time is of the essence and the victim may not even realize they have been victimized until the criminal has long since signed-off. Clearly, the technical challenges for law enforcement are real and profound.

This fact was made clear in the findings and conclusions reached in the recently released report of the President's Working Group on Unlawful Conduct on the Internet, entitled, "The Electronic Frontier: The Challenge of Unlawful Conduct Involving the Use of the Internet." This extensive report highlights in detail the significant challenges facing law enforcement in cyberspace. As the report states, the needs and challenges confronting law enforcement, "are neither trivial nor theoretical." The Report outlines a three-

pronged approach for responding to unlawful activity on the Internet:

1. Conduct on the Internet should be treated in the same manner as similar conduct offline, in a technology neutral manner.
2. The needs and challenges of law enforcement posed by the Internet - including the need for resources, up-to date investigative tools and enhanced multi-jurisdictional cooperation - are significant.
3. Finally, continued support for private sector leadership in developing tools and methods to help Internet users to prevent and minimize the risks of unlawful conduct online.

I would encourage anyone with an interest in this important topic to review carefully the report of the Working Group. The report can be found on the Internet by visiting the website of the Department of Justice's Computer Crime and Intellectual Property Section, located at www.cybercrime.gov. In addition to the report, www.cybercrime.gov also contains other useful information on a wide array of Internet related issues, including the topic of today's hearing - privacy.

Despite the type of difficulties outlined in the Unlawful Conduct Report and discussed today, the Justice Department and law enforcement across this nation are committed to continuing to work together and with their counterparts in other countries to develop and implement investigative strategies to successfully track, apprehend, and prosecute individuals who conduct criminal activity on the Internet. In so doing, the same privacy standards that apply in the physical world remain effective online.

Mr. Chairman, the Department of Justice has taken a proactive leadership role in making cyberspace safer for all Americans. The cornerstone of our cybercrime prosecutor program is the Criminal Division's Computer Crime and Intellectual Property Section, known as CCIPS. CCIPS was founded in 1991 as the Computer Crime Unit, and became a Section in 1996. CCIPS has grown from five attorneys in 1996 to twenty today - and we need more to keep pace with the demand for their expertise. The attorneys in CCIPS work closely on computer crime cases with Assistant United States Attorneys known as "Computer and Telecommunications Coordinators," or CTC's, in U.S. Attorney's Offices around the nation. Each CTC receives special training and equipment and serves as the district's expert on computer crime cases. CCIPS and the CTC's work together in prosecuting cases, spearheading training for local, state and federal law enforcement, working with international counterparts to address difficult international challenges, and providing legal and technical instruction to assist in the protection of this nation's critical infrastructures. We are very proud of the work these people do and we will continue to work diligently to help stop criminals from victimizing people online.

Legal Challenges:

In order to effectively deter and punish computer criminals it takes more than just dedicated investigators and prosecutors. A legal structure that will support detection and prosecution of offenders is essential. However, the laws defining computer offenses and the legal tools needed to investigate criminals using the Internet have lagged behind the

technological and social changes of recent years and the effect on law enforcement has been significant.

For example, the Computer Fraud and Abuse Act, 18 U.S.C. § 1030, one of the primary statutes used to prosecute computer criminals, arguably does not reach a computer hacker who causes a significant amount of damage to a network of computers if no one computer sustains over $5,000 in damage. The Department of Justice has encountered several instances in which an intruder has gained unauthorized access to both private and publicly owned protected computers used in critical infrastructure systems, such as those used by hospitals to store private and sensitive information, or those used by the military to defend this nation. However, in many of these instances, proof of damage in excess of $5,000 to any one computer has been difficult to attain. This loophole needs to be closed.

Another emerging concern is the growing problem of online threats or harassment - serious harassment that amounts to cyberstalking. Current law does not clearly address situations where a cyberstalker uses unwitting third parties to bombard a victim with messages, or transmit private personal data about that person, such as the route the victim's children take to school, in order to place the victim or their family in fear of injury.

One particularly harrowing example involves a California woman who was awakened repeatedly during the night to find men knocking on her door "offering" to rape her. The woman later discovered that a man whose romantic overtures she had rejected had posted personal advertisements on the Internet pretending to be her. The advertisements contained her home address and telephone number and claimed that she fantasized about being raped. This is criminal activity occurring online. Law enforcement has a responsibility to respond, and the American people have the right to expect that in responding, law enforcement will have the tools necessary to bring this criminal to justice. The fact that this criminal used the Internet rather than the telephone should not enable him to elude prosecution.

In addition to modest adjustments to the substantive laws, the tools used by investigators to track online criminals - generally written in language reflecting the pre-Internet telephone technology - need to be updated. For instance, the trap and trace and pen register statutes, 18 U.S.C. § 3121-27, used to identify the destination and origin telephone calls and computer communications, needs to be recalibrated. Under current law, law enforcement may have to obtain court orders in multiple jurisdictions to trace a single communication. Obtaining court orders in multiple jurisdictions does not advance any legitimate or reasonable privacy safeguard and serves as a substantial impediment to an investigation that must move quickly to have any chance at success. As both the Attorney General and the Deputy Attorney General have told Congress recently, the ability to provide nationwide effect for trap and trace orders would help computer crime investigations without impacting personal privacy.

Privacy in cyberspace:

Mr. Chairman, Members of the Subcommittee, I offer these few examples of the challenges posed by the migration to online crime for two reasons. First, it is important to understand the difficulty that law enforcement faces in cyberspace. Second, we must recognize that crime in cyberspace is real and occurring everyday. Law enforcement has an obligation to respond.

In that regard, I note that public education is an important component of the Attorney General's strategy on combating computer crime. As she often notes, the same children who recognize that it is wrong to steal a neighbor's mail or shoplift do not seem to understand that it is equally wrong to steal a neighbor's e-mail or copy a proprietary software or music file without paying for it. To remedy this problem, the Department of Justice, together with the Information Technology Association of America (ITAA), has embarked upon a national campaign to educate and raise awareness of computer responsibility and to provide resources to empower concerned citizens. The "Cybercitizen Awareness Program" seeks to engage children, young adults, and others on the basics of critical information protection and security and on the limits of acceptable online behavior. The objectives of the program are to give children an understanding of cyberspace benefits and responsibilities, an awareness of consequences resulting from the misuse of the medium and an understanding of the personal dangers that exist on the Internet and techniques to avoid being harmed.

Conclusion:

Mr. Chairman, I want to thank you again for this opportunity to testify today. This issue is an important one. Ultimately, the decision as to the appropriate parameters of law enforcement activity lies squarely within the Constitution and the elected representatives of the people, the Congress. The need to protect the privacy of the American people - not just from the government but also from criminals - is a paramount consideration, not just in the context of the Internet, but in general. The Department of Justice stands ready to work with this Subcommittee and others to achieve the proper balance between the important need for protecting privacy and the need to respond to the growing threat of crime in cyberspace.

Mr. Chairman, that concludes my prepared statement. I would be pleased to attempt to answer any questions that you may have at this time.