Department of Justice

STATEMENT OF

DAVID M. BITKOWER
DEPUTY ASSISTANT ATTORNEY GENERAL
CRIMINAL DIVISION
DEPARTMENT OF JUSTICE

BEFORE THE

SUBCOMMITTEE ON CRIME AND TERRORISM
COMMITTEE ON THE JUDICIARY
UNITED STATES SENATE

AT A HEARING ENTITLED

"CYBER CRIME: MODERNIZING OUR LEGAL FRAMEWORK FOR THE INFORMATION AGE"

PRESENTED

JULY 8, 2015

Statement of
David M. Bitkower
Deputy Assistant Attorney General
Criminal Division
Department of Justice

Before the
Subcommittee on Crime and Terrorism
Committee on the Judiciary
United States Senate

At a Hearing Entitled
"**Cyber Crime: Modernizing our Legal Framework for the Information Age"**

Presented
July 8, 2015

Good afternoon, Chairman Graham, Ranking Member Whitehouse, and Members of the Subcommittee. Thank you for the opportunity to appear before the Subcommittee today to discuss legislative proposals to combat cybercrime. I also particularly want to thank the Chair and Ranking Member for holding this hearing and for their continued leadership on this important issue.

As the Attorney General has made clear, fighting cybercrime is one of the highest priorities of the Department of Justice. Recent revelations about the massive thefts of financial and other sensitive information from both the public and private sector serve as a stark reminder to all of us about how vulnerable we are to those who take advantage of our computer networks to steal our personal and financial information.

Our growing reliance on computer networks and electronic devices in almost every aspect of our lives has been accompanied by an increasing threat from individuals, organized criminal networks, and nation states that victimize American citizens and businesses. Hackers

steal and hold for ransom our most valuable and personal information. They invade our homes by secretly activating webcams. They steal financial information to line their pockets while jeopardizing the financial stability of everyday Americans. A new generation of organized criminals is able to steal the personal information of millions of victims from a computer halfway around the world. These developments also pose a widespread threat to American businesses and the economy. Cyber criminals can orchestrate massive disruptions of businesses and can electronically spirit away trade secrets worth millions of dollars in seconds. Every individual has a stake in protecting computers and computer networks from intrusions and abuse. According to one report, just this past May there were over 44 million new pieces of malicious software — or "malware" — created around the globe. Another report found that in 2014, there were about 24,000 ransomware attacks per day. I'll talk more about ransomware later. A study from last summer estimated that cybercrime costs the global economy approximately $400 billion annually. A study from this past May projects that, by 2019, cybercrime will cost businesses worldwide $2 trillion per year.

An essential part of the mission of the Department of Justice is to protect Americans from emerging criminal threats such as the cyber threats described above and to deter, disrupt, and prosecute the criminals who are responsible for them. These invasions of privacy, for good reason, make us feel vulnerable and unsafe. And that fear is only compounded when we realize that the criminals who hack into our computers often sit on the other side of the world; peddle the stolen information to other criminals; and use the information for financial gain or even to terrorize and extort their victims. As the Deputy Attorney General testified this morning, the Department supports the use of strong encryption to help protect against unauthorized access to

sensitive information. But just as locking your door cannot offer complete protection from crime, cybersecurity cannot provide perfect protection from cyber criminals. That's why the Department's prosecutors, along with agents from the Federal Bureau of Investigation, the United States Secret Service, and other law enforcement agencies, work every day using the legal authorities at our disposal to protect personal information and vindicate the privacy rights of citizens and businesses. But just as our adversaries adapt to new technologies and global realities, so must we. If we want to remain effective in protecting our citizens and businesses, our laws and our resources must keep pace with the tactics and numbers of our adversaries. We ask that Congress continue its support of these critical efforts.

Earlier this year, the President announced new legislative proposals designed to protect the online privacy and security of American citizens and businesses. These proposals include a set of targeted updates to the criminal code to provide additional capabilities to prosecute offenders and deter and disrupt criminal conduct.[1] Some of the proposals will enable the Department to address the growth of specific types of crime, such as the sale of illegal spyware or the use of botnets — networks of victim computers surreptitiously infected with malware. Other proposals address shortcomings in existing statutory capabilities, such as the Government's ability to prosecute cases involving insiders, including Government or corporate employees, who use their access to information systems to misappropriate sensitive and valuable data. The proposals also respond to changes in the threats posed by cyber criminals, such as by adding provisions to enable the prosecution of hacking by organized crime groups and to give

[1] *See* https://www.whitehouse.gov/the-press-office/2015/01/13/securing-cyberspace-president-obama-announces-new-cybersecurity-legislat;
https://www.whitehouse.gov/sites/default/files/omb/legislative/letters/updated-law-enforcement-tools.pdf.

Federal courts the authority to sentence perpetrators of the most significant cybercrimes in line with those who commit similar financial crimes.

Computer Fraud and Abuse Act

One of the most important of the substantive criminal statutes used to bring cyber criminals to justice is the Computer Fraud and Abuse Act, also called the "CFAA." The CFAA is the primary Federal law against hacking. It protects the public against criminals who hack into computers to steal information, install malware, and delete files. The CFAA, in short, reflects our baseline expectation that people are entitled to have control over their own computers and are entitled to trust that the information they store in their computers remains safe.

The law was first enacted in 1984, at a time when the problem of cybercrime was still in its infancy. Over the years, a series of measured, modest changes have been made to the CFAA to reflect new technologies and means of committing crimes and to equip law enforcement to respond to changing threats. The CFAA has not been amended since 2008, and in the intervening years the need again has arisen for the enactment of modest, incremental changes. We support targeted legislative changes to help the CFAA keep up with rapidly-evolving technologies and uses.

Deterring Insider Threats

Ensuring that the law enables us to protect privacy and security without ensnaring harmless or legitimate conduct is particularly important in the context of the CFAA, which protects the privacy and security of computer owners and users. The CFAA applies both to hackers who gain access to victim computers without authorization from halfway around the world, and to those who have some authorization to access a computer — like company

employees entitled to access a sensitive database for specified work purposes — but who intentionally abuse that access. The CFAA needs to be updated to make sure that the statute continues to appropriately deter privacy and data security violations. Targeted legislative changes would maintain the law's key privacy-protecting function while ensuring that trivial violations of things like a website's terms of service do not constitute Federal crimes.

The part of the CFAA that covers the conduct of those who have some authorization to access a computer is the statute that Department prosecutors have used to charge, for example, police officers who take advantage of their access to confidential criminal records databases in order to look up sensitive information about a paramour, sell access to private records to others, or even provide confidential law enforcement information to a charged drug trafficker. We've also used this part of the statute to prosecute a consultant of a health insurer who used his access to the company's sensitive databases to improperly obtain the names and Social Security numbers of thousands of current and former employees.

Unfortunately, recent judicial decisions have limited the Government's ability to prosecute such cases in large parts of the country.[2] As a result of these decisions, insiders may be effectively immunized from punishment even where they intentionally exceed the bounds of their legitimate access to confidential information and cause significant harm to their employers and to the people — often everyday Americans — whose data is improperly accessed.

Let me offer you an example. Suppose a criminal in Eastern Europe hacks into a healthcare database located in California and steals the financial and personal information of millions of Americans. That crime could be charged today under the CFAA because the

[2] *See* http://cdn.ca9.uscourts.gov/datastore/opinions/2012/04/10/10-10038.pdf.

offender accessed the database "without authorization." Now suppose that a customer service employee has access to the healthcare company's records in the ordinary course of the employee's work. Because the database contains sensitive information, the company's rules explicitly state that employees can only access the database for official business. But if the employee intentionally violates those rules, and accesses the private medical records of a political candidate in order to later embarrass that person by publicizing the records, the individual likely could not be prosecuted under the CFAA in one of the affected judicial circuits.

The narrow judicial interpretation of the term "exceeds authorized access" in the CFAA stemmed from the concern that the statute potentially makes relatively trivial conduct a Federal crime. For example, a Federal court feared that the statute could be construed to permit prosecution of a person who accesses the internet to check baseball scores at lunchtime in violation of her employer's strict internet use policy.[3] Or someone who accesses a dating website but lies about his height even though the site's terms of service require users to provide only accurate information.

We understand these concerns. The Department of Justice has no interest in prosecuting harmless violations of use restrictions like these. That's why we've crafted proposed amendments to the CFAA to address these concerns — while making sure thathe law applies to those who commit serious thefts and privacy invasions.

To accomplish this, our proposal does two things. First, it addresses the recent judicial decisions that have posed obstacles to important prosecutions. It does this by clarifying that the definition of "exceeds authorized access" includes the situation where the person accesses the

[3] *Id.*

computer for a purpose that he knows is not authorized by the computer owner. This clarification is necessary to permit the prosecution of, for example, a law enforcement officer who is permitted access to criminal records databases, but only for official business purposes. Second, at the same time, the proposal adds new limitations to make clear that trivial conduct does not constitute an offense. In order to constitute a crime under the new wording, not only must an offender access a protected computer in excess of authorization and obtain information, but the information must be worth $5,000 or more, the access must be in furtherance of a separate felony offense, or the information must be stored on a Government computer.

These changes will empower the Department to prosecute and deter significant threats to privacy and security, but make sure that the CFAA doesn't inadvertently cover trivial conduct.

Sale of U.S. Financial Data Overseas

Another priority in addressing threats to privacy and financial security is shutting down the international black market for Americans' stolen financial information. One of the most common motivations for hacking is the theft of financial information. In recent years, organized, multinational criminal enterprises have emerged that steal large volumes of credit card numbers and other personally identifiable information. Middlemen then sell the stolen data to the highest bidder, often using underground "carding" forums. Statutory reforms should be aimed at making sure that these middlemen — those who profit from the sale of stolen financial data of Americans — can be brought to justice even if they are operating outside of the United States.

Current law makes it a crime to sell "access devices" such as credit card numbers. The law allows the Government to prosecute offenders located outside the United States if the credit card number involved in the offense was issued by an American company *and* meets a set of

additional requirements. In the increasingly international marketplace for stolen financial information, however, these requirements have proven increasingly unworkable in practice. The Government has to prove either that an "article" used in committing the offense moved though the United States, or that the criminal is holding his illicit profits in an American bank. But with the theft of digital data, it's not always clear what "article" is involved. And foreign criminals generally move their money back to their home countries rather than keep it in the United States.

These requirements unduly limit the Department of Justice's ability to prosecute criminals residing outside of the United States who commit crimes that harm Americans. Indeed, law enforcement agencies have identified foreign-based individuals holding for sale vast quantities of credit card numbers issued by American financial institutions where there is not necessarily any evidence that the person selling the numbers is the same person who stole them, and no evidence of "articles" in the United States. The United States has a compelling interest in prosecuting such individuals because of the great harm they cause to U.S. financial institutions and citizens.

A targeted amendment would strike the unnecessary language in the current statute. It would permit the United States to prosecute anyone possessing or trafficking in credit card numbers with intent to defraud as long as the credit cards were issued by a United States financial institution, regardless of where the possession or trafficking takes place. This kind of jurisdiction over conduct that occurs abroad is fully consistent with international norms and other criminal laws aimed at protecting Americans from economic harm. Moreover, in an era of global cybercrime where criminals steal Americans' financial information so that they can traffic it abroad, it is necessary to prevent criminals from victimizing our citizens with impunity.

Botnets

Another striking example of cybercrime that victimizes Americans is the threat from botnets — networks of victim computers surreptitiously infected with malware. Once a computer is infected with the malware, it can be controlled remotely from another computer with a so-called "command and control" server. Using that control, criminals can steal usernames, passwords, and other personal and financial information from the computer user, or hold computers and computer systems for ransom. Criminals can also use armies of infected computers to commit other crimes, such as distributed denial of service (DDoS) attacks, or to conceal their identities and locations while perpetrating crimes ranging from drug dealing to online child sexual exploitation. The scale and sophistication of the threat from botnets is increasing every day. Individual hackers and organized criminal groups are using state-of-the-art techniques to infect hundreds of thousands — sometimes millions — of computers and cause massive financial losses, all while becoming increasingly difficult to detect. If we want security to keep pace with technological innovations by criminals, we need to ensure that we have a variety of effective authorities to combat evolving cyber threats like these.

One powerful method that the Department has used to disrupt botnets and free victim computers from criminal malware is the civil injunction process. Current law gives Federal courts the authority to issue injunctions to stop the ongoing commission of specified fraud crimes or illegal wiretapping, by authorizing actions that prevent a continuing and substantial injury. This authority played a crucial role in the Department's successful disruption of the Coreflood botnet in 2011 and the Gameover Zeus botnet in 2014. These botnets used keystroke logging or "man-in-the-middle" attacks to collect online financial account information, and they transferred

stolen funds to accounts controlled by the criminals. The Gameover Zeus botnet, which infected computers worldwide, was estimated to have inflicted over $100 million in losses on American victims alone, often on small and mid-sized businesses. Because the criminals behind these particular botnets used them to commit fraud against banks and bank customers, existing law allowed the Department to obtain court authority to disrupt the botnets by taking actions such as disabling communication between infected computers and the command and control servers.

The problem is that current law only permits courts to consider injunctions for limited categories of crimes, including certain frauds and illegal wiretapping. Botnets, however, can be used for many different types of illegal activity. They can be used to steal sensitive corporate information, to harvest email account addresses, to hack other computers, or to execute denial of service attacks against websites or other computers. Yet — depending on the facts of any given case — these crimes may not constitute fraud or illegal wiretapping. In those cases, courts may lack the statutory authority to consider an application by prosecutors for an injunction to disrupt the botnets in the same way that injunctions were successfully used to incapacitate the Coreflood and Gameover Zeus botnets.

Appropriate legislative changes would add activities like the operation of a botnet to the list of offenses eligible for injunctive relief. Specifically, our proposal includes an amendment that would permit the Department to seek an injunction to prevent ongoing hacking violations in cases where 100 or more victim computers have been hacked. This numerical threshold focuses the injunctive authority on enjoining the creation, maintenance, operation, or use of a botnet, as well as other widespread attacks on computers using malware (such as “ransomware”).

The same legal safeguards that currently apply to obtaining civil injunctions, and that applied to the injunctions obtained by the Department in the Coreflood and Gameover Zeus cases, would also apply here. Before an injunction is issued, the Government must civilly sue the defendant and demonstrate to a court that it is likely to succeed on the merits of its lawsuit and that the public interest favors an injunction; the defendants and enjoined parties have the right to notice and to have a hearing before a permanent injunction is issued; and the defendants and enjoined parties may move to quash or modify any injunctions that the court issues.

In sum, a targeted amendment would provide the Government with an effective capability to shut down illegal botnets or certain widespread malware, and better match the ways that criminals are using these technologies. It assures that the legal mechanism that has proven effective to date will be available.

Sale of Botnets

The Department has also striven to identify and bring to justice those who create and control botnets. While we have had significant successes to date prosecuting these offenders, we have encountered some shortcomings in the existing law.

Criminals continually find new ways to make money illegally through botnets. Law enforcement officers now frequently observe that those who create botnets not only use the botnets for their own illicit purposes, but also sell or even rent access to the infected computers to other criminals. The criminals who purchase or rent access to botnets then go on to use the infected computers for various crimes, including theft of personal or financial information, the dissemination of spam, for use as proxies to conceal other crimes, or in denial of service attacks

on computers or networks. Americans are suffering extensive, pervasive invasions of privacy and financial losses at the hands of these hackers.

Current criminal law prohibits the creation of a botnet because it prohibits hacking into computers without authorization. It also prohibits the use of botnets to commit other crimes. But it is not similarly clear that the law prohibits the sale or renting of a botnet. In one case, for example, undercover officers discovered that a criminal was offering to sell a botnet consisting of thousands of victim computers. The officers accordingly "bought" the botnet from the criminal and notified the victims that their computers were infected. The operation, however, did not result in a prosecutable U.S. offense because there was no evidence that the seller himself had created the botnet in question or used it for a different crime. While trafficking in botnets is sometimes chargeable under other subsections of the CFAA, this problem has resulted in, and will increasingly result in, the inability to prosecute individuals selling or renting access to many thousands of hacked computers.

We believe that it should be illegal to sell or rent surreptitious control over infected computers to another person, just like it is already clearly illegal to sell or transfer computer passwords. That's why we recommend amending current law to prohibit the sale or transfer not only of "password[s] or similar information" (the wording of the existing statute) but also of "means of access," which would include the ability to access computers that were previously hacked and are now part of a botnet. In addition, the proposal would replace the current requirement that the Government prove that the offender had an "intent to defraud" with a requirement to prove that the offender not only knew his conduct was "wrongful," but that he also knew or should have known that the means of access would be used to hack or damage a

computer. This last change is necessary because, as noted above, criminals don't only use botnets to commit fraud — they also use them to commit a variety of other crimes.

Some commentators have raised the concern that this proposal would chill the activities of legitimate security researchers, academics, and system administrators. We take this concern seriously. We have no interest in prosecuting such individuals, and our proposal would not prohibit such legitimate activity. Indeed, that's precisely why our proposal requires that the Government bear the burden to prove, beyond a reasonable doubt, that the individual intentionally undertook an act (trafficking in a means of access) that he or she knew to be wrongful. And the Government would similarly have to prove that the individual knew or had reason to know that the means of access would be used to commit a crime by hacking someone else's computer without authorization.

This approach makes clear that ordinary, lawful conduct by legitimate security researchers and others is not at risk of criminal prosecution. We want to work with the members of this Subcommittee to make sure any amendment prohibits the pernicious conduct we've described without chilling the activities of those who are trying to improve cybersecurity for all.

Spyware

The widespread use of computers and cellular phones has created a market for malware that allows perpetrators to surreptitiously intercept their victims' communications. For a small fee, people can purchase this software and download it onto a victim's device. Operating secretly in the background, the spyware allows perpetrators to read a victim's email and text messages. They can track a victim's location and listen to their calls. They can even turn on the

microphone in a victim's phone or computer and listen to conversations in the room. They can do all of this from afar and without the victim knowing.

These privacy invasions have far-reaching implications. Spyware can be used by abusive spouses to track, control, and terrorize former partners. Competitors can commit corporate espionage. Spyware can even be used to eavesdrop on law enforcement and national security personnel. As one example, the Department recently prosecuted the maker of a spyware application called "StealthGenie." This application, which was available for the Apple iPhone, Android phones, and Blackberry devices, could surreptitiously record all incoming/outgoing voice calls; it allowed the purchaser to secretly activate the phone to monitor nearby conversations within a 15-foot radius; and it enabled the purchaser to monitor the incoming and outgoing email and text messages. The application was intended for, and I quote from the business development plan: "Spousal cheat: Husband/Wife o[r] boyfriend/girlfriend suspecting their other half of cheating or any other suspicious behaviour or if they just want to monitor them."

The market for this software has made these capabilities widely available to many who would not otherwise have access to them. We need to do more to counter the increase in privacy invasions.

It is already illegal to sell or advertise surreptitious interception devices of this type. Indeed, the Department successfully prosecuted the maker of the "StealthGenie" spyware, and the court fined the offender half-a-million dollars. Yet the people who make and sell these products often reside outside of the United States, making it more difficult to bring them to justice. And they are making millions of dollars of profit selling spyware inside the United

States. These same criminals try to conceal their ill-gotten gains and transfer them out of the reach of law enforcement. Because current law does not authorize the forfeiture of proceeds from the sale of spyware, U.S. law enforcement is unable to disgorge such criminals of the money that they amass.

Our proposal includes an amendment that would expand the scope of the statute that already provides for the forfeiture of surreptitious interception devices themselves to include forfeiture of proceeds from the sale of spyware and property used to facilitate the crime. The proposal includes standard language drawn from other areas of the criminal code regarding the rules and safeguards for civil and criminal forfeiture.

In addition, violators of the surreptitious interception device statute often engage in money laundering by transferring proceeds through multiple overseas accounts to conceal the profits of their criminal enterprise. Because the spyware statute is not listed as a predicate offense in the money laundering statute, however, prosecutors are unable to charge defendants for money laundering activities related to the sale of spyware unless they can link it to some other crime, which will often be difficult or impossible. The proposal therefore adds violations of the spyware statue to the list of money laundering predicate offenses.

Conclusion

I very much appreciate the opportunity to discuss with you the ways in which the Department protects the privacy and security of American citizens and businesses from cyber threats and to discuss targeted legislative changes that would strengthen our ability to counter this increasingly sophisticated threat going forward. We understand how devastating it is to victims of cybercrime who have their personal and financial information siphoned away, whether

by hackers on the other side of the world or by insiders at a company that holds their personal information. The Justice Department is committed to using the full range of investigative capabilities available to us to fight these privacy invasions and protect Americans, and we will continue to use these capabilities responsibly. We appreciate the continued efforts of Congress and this Subcommittee to ensure that statutory authorities to counter cybercrime are updated and effective.

Thank you for the opportunity to discuss this important area of our work, and I look forward to answering any questions you might have.