Department of Justice

STATEMENT OF

MYTHILI RAMAN
ASSISTANT ATTORNEY GENERAL
DEPARTMENT OF JUSTICE

BEFORE THE

COMMITTEE ON THE JUDICIARY
UNITED STATES SENATE

AT A HEARING ENTITLED

"PRIVACY IN THE DIGITAL AGE:
PREVENTING DATA BREACHES AND COMBATING CYBERCRIME"

PRESENTED
FEBRUARY 4, 2014

Statement of

Mythili Raman

Acting Assistant Attorney General

Department of Justice

Before the

Committee on the Judiciary

United States Senate

At a Hearing Entitled

"Privacy in the Digital Age: Preventing Data Breaches and Combating Cybercrime"

Presented

February 4, 2014

Good afternoon, Chairman Leahy, Ranking Member Grassley, and Members of the Committee. Thank you for the opportunity to appear before the Committee today to discuss the Department of Justice's fight against cybercrime. I also particularly want to thank the Chair for holding this hearing and for his continued leadership on these important issues.

At the Department of Justice, we are devoting significant resources and energy to fighting computer hacking and other types of cybercrime. The recent revelations about the massive thefts of financial information from large retail stores have served as a stark reminder to all of us about how vulnerable we are to cyber criminals who are determined to steal our personal information. The Justice Department is more committed than ever to ensuring that the full range of government enforcement tools is brought to bear in the fight against cybercrime.

Cybercrime has increased dramatically over the last decade, and our financial infrastructure has suffered repeated cyber intrusions. As we all know, it is becoming far too commonplace an occurrence that our email accounts are hijacked, our financial information siphoned away, and our personal information compromised. The technology revolution – which has brought enormous benefits to individuals, U.S. companies and our economy as a whole – has also facilitated these criminal activities, making available a wide array of new methods that

identity thieves can use to access and exploit the personal information of others. Skilled criminal hackers are now able to perpetrate large-scale data breaches that leave, in some cases, tens of millions of individuals at risk of identity theft. Today's criminals, who often sit on the other side of the world, can hack into computer systems of universities, merchants, financial institutions, credit card processing companies, and data processors to steal large volumes of sensitive and valuable information. They then peddle the stolen information to other criminals, use the information for their own financial gain, or sometimes even terrorize and extort their victims.

Last December, Target, the second-largest U.S. discount chain, announced that credit and debit card data for as many as 40 million consumers who shopped in its stores between November 27 and December 15 may have been compromised. Target then disclosed on January 10 that thieves had also accessed the personal information, including names, phone numbers, home addresses, and/or email addresses, of as many as 70 million people – information that is valued by criminals because it can be used to lure victims with fake emails or hack into other accounts. The U.S. Secret Service, within the Department of Homeland Security, and the Department of Justice are investigating this massive data breach.

A few days later, retailer Neiman Marcus Inc. reported that it also was the victim of a suspected cyberattack over the holidays in which some of its customers' credit card information may have been stolen. Target and Neiman Marcus are just two of the latest known victims.

The Justice Department is vigorously responding to hacking and other cybercrimes through the tenacious work of the Criminal Division's Computer Crime and Intellectual Property Section, also known as CCIPS, which partners with Computer Hacking and Intellectual Property Coordinators in U.S. Attorney's Offices across the country as part of a network of almost 300 Justice Department cybercrime prosecutors. In addition, the Federal Bureau of Investigation has made combating cyber threats one of its top national priorities, working through Cyber Task Forces in each of its 56 field offices and continuing to strengthen the National Cyber Investigative Joint Task Force. Every day, these prosecutors and agents strive to hold to account cyber criminals who victimize Americans.

Consider, for instance, the case of Vladislav Horohorin, which was prosecuted here in the District of Columbia by CCIPS and the United States Attorney's Office, based on an investigation by the FBI and U.S. Secret Service. Horohorin, known by the online nickname "BadB," used online criminal forums to sell stolen credit and debit card information to individuals around the world to enable fraudulent transactions by other cyber criminals. At the time of his arrest, he possessed more than 2.5 million stolen credit and debit card numbers. In one instance, he participated in a criminal group that, in a single 12-hour crime spree, stole over $9.4 million through fraudulent transactions at over 2,100 ATMs in 280 cities around the world. As a result of a massive investigation spanning several years – and several countries – we located and charged him, and he was arrested after leaving Russia for France. In April 2013, Horohorin was sentenced to serve 88 months in prison.

Our investigation of the Coreflood botnet is another example of our commitment to stopping massive computer crimes by using the most innovative law enforcement techniques. A botnet is a network of secretly hacked computers, sometimes numbering in the millions, which are located in homes, schools, and offices. The computers are infected with sophisticated malicious software, or "malware," and once the malware is installed, hackers can put these bots to countless illegal uses. The Coreflood botnet, for example, hijacked hundreds of thousands of computers for the purpose of stealing private personal and financial information – including usernames and passwords – from unsuspecting computer users. In one example, the Coreflood botnet software illegally monitored Internet communications between a computer user and her bank, took over an online banking session, and then emptied the user's bank account. Overall losses from the scheme were staggering, estimated to be in the tens of millions of dollars.

Although the individuals controlling the Coreflood network resided overseas and were largely outside the direct reach of U.S. law enforcement, in 2011, CCIPS, the United States Attorney's Office for the District of Connecticut, and the FBI used a combination of civil and criminal legal authorities to seize key control servers, shut down the network, and work with private sector partners to help disinfect victims' computer systems. Among other things, as part

of this ground-breaking law enforcement operation, the Justice Department obtained a court order authorizing the government to respond to signals sent from infected computers in the United States to stop the Coreflood software from running, and thus to prevent further harm to hundreds of thousands of Americans whose computers were under the control of the botnet. And, in a relatively short period of time, the Coreflood botnet was dismantled.

The Department has continued to place a high priority on arresting and deterring those who create botnets. CCIPS and the U.S. Attorney's Office in Atlanta just last week announced the guilty plea of a Russian citizen named Aleksandr Panin for developing and distributing malware called "SpyEye." The SpyEye malware created botnets that stole personal and financial information such as credit card information, banking credentials, usernames, passwords, and personal identification numbers. Panin sold his software to at least 154 criminal "clients," who in turn used it to infect an estimated 1.4 million computers around the world. The FBI arrested Panin on July 1, 2013, while he was flying through Hartsfield-Jackson Atlanta International Airport.

Hacking can have terrifying consequences even when conducted on a smaller scale, and we have vigorously pursued hackers who have used the Internet to invade Americans' privacy. In 2011, for example, in a case investigated by the FBI, the United States Attorney's Office in Los Angeles successfully prosecuted a hacker named Luis Mijangos. Mijangos hacked for sexual thrill. He infected the computers of victims with malicious software that gave him complete control over their computers. He deliberately targeted teens and young women, reading their emails, turning on their computer microphones and listening to conversations taking place in their homes, and, most importantly for him, watching them through their webcams as they undressed. Even more frightening, Mijangos then extorted certain victims by threatening to post intimate pictures on the Internet unless the victims provided him with even more salacious images or videos of themselves. When one victim shared Mijangos's threats with a friend, Mijangos retaliated by posting nude pictures of the victim on her friend's social networking page. In another instance, Mijangos had infected the computers of a college student,

her boyfriend, and her roommate. When the victim called her boyfriend, and they discussed calling the police, Mijangos reportedly sent the boyfriend an anonymous instant message that said: "I know you're talking to each other right now!" The victim then decided to call the police. But when she did, she got a message, too. "I know you just called the police," he wrote. His message was unmistakable: he was in control; he knew everything; and he had the power to hurt the victim further if she reported the crime. At the time of his arrest, FBI computer forensics experts had determined that Mijangos had infected more than 100 computers that were used by approximately 230 individuals, at least 44 of them minors. The Court sentenced Mijangos to 72 months in federal prison.

There are many other examples of the Department's recent work to bring cyber criminals to justice. There is the takedown of Silk Road, a hidden website designed to enable its users to buy and sell illegal drugs and other unlawful goods and services, and charges against the alleged operator of the site by the U.S. Attorney's Offices for the Southern District of New York and the District of Maryland. There is the prosecution by CCIPS and the U.S. Attorney's Office in New Hampshire of Adrian-Tiberiu Oprea, a Romanian who recently received a 15-year sentence in September for leading an international, multimillion-dollar scheme to remotely hack into and steal unsuspecting customers' payment card data from U.S. merchants' computers. The case was investigated by the U.S. Secret Service. There is the recent indictment by CCIPS and the U.S. Attorney's Office for the Western District of Wisconsin of Sinovel Wind Group Co. Ltd., a China-based manufacturer and exporter of wind turbines, which is alleged to have stolen trade secrets from an American company for the purpose of producing wind turbines and retrofitting existing wind turbines with the stolen technology. And on January 23, the FBI arrested two men for conspiring to hack into victims' email accounts to steal nude photos that were later posted on the "revenge porn" website isanyoneup.com. The U.S. Attorney's Office for the Central District of California charged the men with violating the Computer Fraud and Abuse Act.

The recent disclosures about the massive data breaches at retailers have underscored that cybercrime is a real, present threat, and one that is growing. Cyber criminals steal the personal

and financial information of individuals, carry out Distributed Denial of Service (or DDOS)[1] attacks on networks, and purloin sensitive corporate or military data. These criminals can easily prey on victims halfway around the world. They sometimes use virtual currencies to enrich themselves while hiding their identities and avoiding leaving their fingerprints in the traditional banking system. Despite these challenges, the Justice Department is staying ahead of these threats. We are using all of the tools available to us to identify cyber criminals, wherever in the world they are located, break up their networks, and bring them to justice. We are developing meaningful partnerships with foreign law enforcement to strengthen our collective capacity to fight cybercrime. And we use our tools responsibly and consistent with established legal safeguards that protect against abuse. But without the tools we have been provided, we would not be able to bring offenders to justice. And we must ensure that the statutes we enforce keep up with technology so that we can keep pace with the cyber criminals, who are constantly developing new tactics and methods.

Computer Fraud and Abuse Act

In addition to the important law enforcement techniques that we must use to successfully investigate cyber criminals, our prosecutors also rely on substantive criminal statutes to bring cyber criminals to justice. One of the most important of these laws 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 malicious software, 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 information they store in their computers remains safe.

The CFAA was first enacted in 1986, 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

[1] A Distributed Denial of Service attack is one in which a criminal uses many compromised computer systems to send information to a single target computer. The flood of incoming information to the target computer makes it unable to function correctly, thereby denying service to the legitimate users of the system.

CFAA to reflect new technologies and means of committing crimes and to equip law enforcement with tools to respond to changing threats. The CFAA has not been amended since 2008, and the intervening years have again created the need for the enactment of modest, incremental changes. The Administration's May 2011 legislative proposal proposed revisions to keep Federal criminal law up-to-date. We continue to support changes like these that will keep up with rapidly-evolving technologies and uses.

Deterring Insider Threats

Another portion of the CFAA that has received considerable attention is the way that the law addresses the threat posed by insiders – those who have some right to access a system but who abuse that right, such as employees of a business who unlawfully make off with their employers' intellectual property. The CFAA addresses this problem by criminalizing conduct by those who "exceed authorized access" to a protected computer.

Some commentators have contended that the CFAA's provision criminalizing exceeding authorized access should be limited or abolished because the provision is subject to misuse or overuse. Some have worried, for example, that the statute permits prosecution of people who merely lie about their age when going to a dating site, or harmlessly violate the terms of service of an email provider. To that end, we are open to addressing these concerns by working with Congress to develop appropriate statutory amendments, such as new statutory thresholds regarding the value or sensitivity of the information improperly accessed under 1030(a)(2), or new language making more explicit that the statute does not permit prosecution based on access restrictions that are not clearly understood.

At the same time, insider hackers pose a serious threat to American businesses and citizens. Examples of insiders include employees at a credit card company or stock broker who regularly deal with sensitive information. There is generally no way to encrypt and password-protect every piece of data on a system to eliminate the insider threat, because employees need to be able access the data to do their jobs. Thus, written policies between employers and employees – which are simply a contractual means of ensuring trust – are an important way to secure

information. Violating these written restrictions harms businesses. Just as businesses justifiably rely on the criminal law to deter thefts of physical property, so they also should be able to rely on it to deter misappropriation of their private, sensitive data – data that is often far more valuable than equipment or supplies.

In recent years, two courts of appeals have interpreted the CFAA to bar certain "insider" cases, creating a circuit split. Compare *United States v. Nosal*, 676 F.3d 854 (9th Cir. 2012) (*en banc*) and *WEC Carolina Energy Solutions LLC v. Miller*, 687 F.3d 199 (4th Cir. 2012), with *United States v. John*, 597 F.3d 263 (5th Cir. 2010); *United States v. Rodriguez*, 628 F.3d 1258 (11th Cir. 2010); and *Int'l Airport Ctrs., LLC v. Citrin*, 440 F.3d 418 (7th Cir. 2006). Specifically, the Fourth and Ninth Circuits have interpreted the statute not to permit prosecution as long as an insider was authorized to access the database or information in question for any purpose. Under this interpretation, the CFAA would not apply where a police officer accessed an arrest record for the purpose of harassing a romantic rival, because the officer was authorized to access the records to assist in criminal investigations. Similarly, under this interpretation, the CFAA would not apply where a bank employee accessed customer records for the purpose of selling them to organized crime members, because the employee was authorized to access the records to resolve customer complaints. This interpretation makes it substantially more challenging for DOJ to protect American companies from the misappropriation of their intellectual property and sensitive data – misappropriation that may also directly harm American citizens when that data includes their personal or financial information.

We look forward to working with Congress to address these important issues.

Data Breach Notification

While the Justice Department continues to use all of the tools at its disposal to combat cybercrime, the Administration recommends the establishment of a strong, uniform Federal standard requiring certain types of businesses to report data breaches and thefts of electronic personally identifiable information. Businesses should be required to provide prompt notice to consumers in the wake of a breach. We should balance the need to safeguard consumers and

hold compromised entities accountable, while setting clear standards that avoid undue burdens on industry. We should include a safe harbor for breaches with no reasonable risk of harm or fraud. This approach would protect the privacy of individuals while holding firms accountable for failure to safeguard personal data.

In 2011, the Administration put forth a package of recommended cybersecurity amendments that included a data breach notification proposal.[2] The 2011 proposal is based upon the belief that American consumers should know when they are at risk of identity theft or other harms because of a data security breach. In addition, to strengthen the tools available to law enforcement to investigate data security breaches and to combat identity theft, the proposal would require that business entities notify the Federal government of a data security breach in a timely fashion so that law enforcement can promptly pursue the perpetrators of cyber intrusions and identity theft. The proposal has several sections of particular note.

First, under this proposal, following the discovery of a security breach, business entities must notify any individual whose sensitive, personally identifiable information has been, or is reasonably believed to have been, accessed or acquired, unless there is no reasonable risk of harm. Business entities covered under this requirement are those that use, access, transmit, store, dispose of, or collect sensitive, personally identifiable information about more than 10,000 people during any 12-month period. But the Administration believes that business entities which have demonstrated that they have effective data breach prevention programs should be exempt from notice to individuals if a risk assessment concludes that there is no reasonable risk that a security breach has harmed, or will harm, the individuals whose information was compromised. The proposal would also recognize that such harm may be avoided where the stolen data has been rendered unusable by criminals; for example, through encryption, or through programs that block unauthorized financial transactions and provide effective notice to affected victims. The

---

[2] The Administration's Privacy and Innovation Blueprint, released in February 2012, also called for a data breach notification law.

proposal also includes certain exceptions for notice that would impair law enforcement investigations or national security.

Because of the importance of bringing the perpetrators of data breaches to justice, the Administration's proposal would also require business entities to notify law enforcement agencies if the security breach involves (1) the sensitive information of more than 5,000 people; (2) a database or other data system containing sensitive information of more than 500,000 people nationwide; (3) databases owned by the Federal government; or (4) primarily the sensitive information of Federal employees and contractors involved in national security or law enforcement. Businesses would report to a single entity that would then promptly disseminate the reported information to key Federal law enforcement agencies. In recognition of the time-sensitivity of data breach investigations, the notice required under this section would be provided as promptly as possible, but no later than 72 hours before notification to an individual or 10 days after discovery of the events requiring notice, whichever comes first.

Millions of Americans every year are faced with the potential for fraud and identity theft from online breaches of their sensitive, personally identifiable information. The nation clearly needs strong protections for consumers' rights and privacy, and accountability for businesses that do not safeguard credit card and social security numbers, names and addresses, medical records, and other sensitive information. The Administration's proposal creates a strong national standard to notify consumers with clear, actionable information when their personal information is compromised. Responsible entities will be held accountable through these disclosures. At the same time, a consistent national standard and reasonable exemptions for harmless breaches will reduce unnecessary compliance costs. This proposal meets the dual challenge of ensuring privacy, security, and safety without burdening economic prosperity and innovation.

Access Device Fraud

To ensure that we can take action when cyber criminals acting overseas steal data from U.S. financial institutions, we also recommend a modification to what is known as the access device fraud statute, 18 U.S.C. § 1029. One of the most common motivations for hacking crime

is to obtain financial information. The access device fraud statute proscribes the unlawful possession and use of "access devices," such as credit card numbers and devices such as credit card embossing machines. Not only do lone individuals commit this crime, but, more and more, organized criminal enterprises have formed to commit such intrusions and to exploit the stolen data through fraud.

The Department of Justice recommends that the statute be expanded to prosecute offenders in foreign countries who directly and significantly harm United States financial institutions and citizens. Currently, a criminal who trades in credit card information issued by a U.S. financial institution, but who otherwise does not take one of certain enumerated actions within the jurisdiction of the United States, cannot be prosecuted under section 1029(a)(3). Such scenarios are not merely hypothetical. United States law enforcement agencies have identified foreign-based individuals selling vast quantities of credit card numbers issued by U.S. financial institutions where there is no evidence that those criminals took a specific step within the United States to traffic in the data. The United States has a compelling interest in prosecuting such individuals given the harm to U.S. financial institutions and American citizens, and the statute should be revised to cover this sort of criminal conduct.

Deterring the Spread of Cell Phone Spying

The Department of Justice further recommends a legislative change to enable law enforcement to seize the profits of those who use cell phone spyware. The spread of computers and cellular phones in recent years has created a new market in malicious software that allows perpetrators to intercept victims' communications without their knowledge or consent. This is illegal under current law, and current law also provides that law enforcement can forfeit the surreptitious interception devices themselves. It does not, however, enable forfeiture of the proceeds of the sale or use of those devices, or the forfeiture of any property used to facilitate their manufacture, advertising, or distribution. Further, the surreptitious interception of communications is currently not listed as a predicate offense in the money laundering statute, 18 U.S.C. § 1956. Because perpetrators of these crimes often act from abroad, making it more

difficult to prosecute them, it is particularly important that law enforcement be able to seize the money that the criminals make from engaging in this criminal surveillance, and seize the equipment they use.

Selling Access to Botnets

We also recommend amending current law to address the proliferation of botnets, such as the Coreflood botnet I discussed earlier. Botnets can be used for various nefarious purposes, including theft of personal or financial information, the dissemination of spam, and cyberattacks, such as Distributed Denial of Service attacks. But creators and operators of botnets do not always commit those crimes themselves – frequently they sell, or even rent, access to the infected computers to others. The CFAA does not clearly cover such trafficking in botnets, even though trafficking in infected computers is clearly illegitimate, and can be essential to furthering other criminal activity. We thus propose that the CFAA be amended to cover trafficking in access to botnets.

In addition, section 1030(a)(6) presently requires proof of intent to defraud. Such intent is often difficult to prove because the traffickers of unauthorized access to computers often have a wrongful purpose other than the commission of fraud, or do not know or care why their customers are seeking unauthorized access to other people's computers. This has made it more challenging in many cases for prosecutors to identify a provable offense even when they can establish beyond a reasonable doubt that individuals are selling access to thousands of infected computers. We therefore recommend that Congress consider amending the CFAA to address this shortcoming.

Conclusion

I very much appreciate the opportunity to discuss with you the ways in which the Department protects American citizens and businesses by aggressively investigating and prosecuting hackers – both outsiders and insiders. 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 might hold their personal information. The Justice Department is committed to using the full range of investigative tools and laws available to us to fight these crimes and protect Americans. And, we will continue to use these tools responsibly.

Thank you for the opportunity to discuss the Department's work in this area, and I look forward to answering any questions you might have.