Department of Justice

STATEMENT OF

JASON WEINSTEIN
DEPUTY ASSISTANT ATTORNEY GENERAL
CRIMINAL DIVISION

BEFORE THE

COMMITTEE ON JUDICIARY
UNITED STATES SENATE
SUBCOMMITTEE ON PRIVACY, TECHNOLOGY AND THE LAW

ENTITLED

"PROTECTING MOBILE PRIVACY:
YOUR SMARTPHONES, TABLETS, CELL PHONES AND YOUR PRIVACY"

PRESENTED

May 10, 2011

Good afternoon, Chairman Franken, Ranking Member Coburn, and Members of the Committee. Thank you for this opportunity to testify on behalf of the Department of Justice regarding privacy and mobile devices.

Over the last decade, we have witnessed an explosion of mobile computing technology. From laptops and cell phones to tablets and smart phones, Americans are using more mobile computing devices, more extensively, than ever before. We can bank, shop, conduct business, and socialize remotely with our friends and loved ones instantly, almost anywhere. These devices drive new waves of innovation, personal convenience, and professional resources. They also present increasingly tempting targets for identity thieves, cyberstalkers and other criminals.

Last month, one study concluded that 64% of American cell phone users were using smart phones.1 The speed and scale of that growth makes the topic of this hearing particularly timely. As mobile devices penetrate our daily lives, it is appropriate to evaluate the effect that these new devices have on our safety and privacy. We must also ensure that the law provides sufficient resources to investigators and prosecutors who investigate and prevent crimes against Americans who increasingly conduct their lives using this new medium. I thank the committee for giving me the opportunity to address these issues.

Prosecuting cybercriminals and identity thieves

One of the Department of Justice's core missions is protecting the privacy of Americans and prosecuting criminals who violate that privacy. Americans today face a wide range of threats to their privacy, including risks from using mobile devices. Foreign and domestic actors of all types, including cyber criminals, routinely and unlawfully access data that most people would regard as highly personal and private. Unlike the government – which must comply with the Constitution and laws of the United States and is accountable to Congress, courts, and ultimately the people – malicious cyber actors do not respect our laws or our privacy. The government has an obligation to prevent, disrupt, and deter such intrusions.

1 *March Mobile Mix Report*, Millennial Media, available at http://www.millennialmedia.com/research/mobilemix/.

Every day, criminals hunt for our personal and financial data so that they can use it to commit fraud or sell it to other criminals. The technology revolution has facilitated these activities, making available a wide array of new methods that identity thieves can use to access and exploit the personal information of others. Skilled hackers have perpetrated large-scale data breaches that left hundreds of thousands—and in many cases, tens of millions—of individuals at risk of identity theft. Today's criminals can remotely access the computer systems of government agencies, universities, merchants, financial institutions, credit card companies, and data processors to steal large volumes of personal information—including personal financial information. As Americans accomplish more and more of their day-to-day tasks using smart phones and other mobile devices, criminals will increasingly target these platforms.

The most significant threats are continuing to evolve, and now increasingly include threats to corporate data. A report just released by McAfee and Science Applications International Corporation confirms this trend in cyber crime. According to this report, which was based on a survey of more than 1,000 senior IT decision makers in several countries, "high-end" cyber criminals have shifted from targeting credit cards and other personal data to the intellectual capital of large corporations. This includes extremely valuable trade secrets and product planning documents. These threats come both from outside hackers as well as insiders who gain access to critical information from within companies and government agencies. As entities make their key proprietary information available via mobile platforms, so that users can access it wherever and whenever it is most relevant, criminals and other actors will attack those devices as well.

The kinds of criminals we are up against are organized, international, and profit-driven. For example, in October 2009, nearly 100 people were charged in the U.S. and Egypt as part of an operation known as Phish Phry—one of the largest cyber fraud cases to date and the first joint cyber investigation between Egypt and the United States. Phish Phry was the latest action in what FBI Director Mueller described as a "cyber arms race" where law enforcement must coordinate and collaborate in order to keep up with its cyber adversaries. The defendants in

Operation Phish Phry targeted U.S. banks and victimized hundreds of account holders by stealing their financial information and using it to transfer about $1.5 million to bogus accounts they controlled. More than 50 individuals in California, Nevada, and North Carolina and nearly 50 Egyptian citizens have been charged with crimes including computer fraud, conspiracy to commit bank fraud, money laundering, and aggravated identity theft. Led by the FBI and the United States Attorney's Office for the Central District of California, this investigation required close coordination with state and local law enforcement, the Secret Service, and our Egyptian counterparts. In late March, five more people were convicted of federal charges for their roles in this phishing operation, bringing the total number of convictions to date to 46.

One increasingly common form of online crime involves the surreptitious infection of a computer with code that makes it part of a "botnet" – a collection of compromised computers under the remote command and control of a criminal or foreign adversary. Criminals and other malicious actors can extensively monitor these computers, capturing every keystroke, mouse click, password, credit card number, and e-mail. Unfortunately, because many Americans are using such infected computers, they are suffering from an extensive, pervasive invasion of privacy at the hands of these actors.

Just last month, the Department announced the successful disruption of the Coreflood botnet, an international botnet made up of hundreds of thousands of computers that had been infected by malicious software (often referred to as "malware"). The Coreflood malware allowed criminals to remotely control the infected computers in order to steal private personal and financial information from unsuspecting computer users, including users on corporate computer networks. Through a combination of civil and criminal authorities, including a temporary restraining order, the FBI seized the servers that the criminals used to control the botnet and set up a substitute "command and control" server. The Coreflood malware was programmed to automatically contact the Coreflood command and control servers for instructions on a routine basis; after FBI intervention, those requests were instead routed to the FBI's substitute server. The FBI then replied to bot queries with an "exit" command that put the bots to sleep and stopped them from collecting further private data and causing more harm to hundreds of

thousands of unsuspecting users of infected computers in the United States. As I'll discuss later in my testimony, the Department is concerned that as mobile devices become increasingly capable, they will be integrated into such botnets, or used to control them.

The Department's Organizational Response

The Department has organized itself to aggressively investigate and prosecute cyber crime wherever it occurs, including in the context of mobile devices and smart phones. Investigating and disrupting cyber crimes and cyber threats is a priority for the United States Attorney community, and the Attorney General's Advisory Committee has a subcommittee dedicated to cybercrime and intellectual property enforcement issues. A nationwide network of 230 Computer Hacking and Intellectual Property (CHIP) Assistant United States Attorneys in our USAOs focuses on these crimes, in coordination with the Criminal Division's Computer Crime and Intellectual Property Section (CCIPS). CCIPS provides core expertise on these issues, prosecutes cutting edge cases and provides litigation assistance to United States Attorneys' Offices. CCIPS also provides resources such as manuals, and trains prosecutors across the country, often in conjunction with Assistant United States Attorneys. Department prosecutors also work closely with our law enforcement partners.

In FY 2008 through FY 2010, United States Attorneys' Offices brought approximately 4,000 identity fraud cases. In addition, many of the large scale fraud cases prosecuted by the Fraud Section of the Department's Criminal Division also included identity fraud conduct.

The Office of International Affairs (OIA) enhances international cooperation efforts by expediting the sharing of critical electronic evidence with foreign law enforcement partners and by marshaling efforts to secure the extradition of international fugitives. The Office of Enforcement Operations guides investigative policy in numerous areas, including approvals for wiretaps and policy relating to use of tracking devices. It is a combination of these resources both in Main Justice and in the United States Attorneys' Offices that enables prosecutors across the country to tackle these complex and demanding cases.

The FBI Cyber Division is addressing the cybercrime threat from mobile devices through the Financial Threat Focus Cell (FTFC) and the Telecommunications Initiative. Through the FTFC the FBI Cyber Division is working with the largest U.S. based Financial Institutions (FIs) to determine the types, dates and level of mobile banking that those FIs are implementing. The FTFC is also working with FI organizations such as the FS-ISAC, BITS Financial Services Roundtable - Remote Channel Fraud Subgroup and the National Cyber-Forensics & Training Alliance's (NCFTA) Telecommunications Initiative. These organizations provide insight to the FBI so that law enforcement is more cognizant of current and future trends in terms of mobile banking product releases, new business alliances (e.g. AT&T, Verizon and Discover Card's recent product) and new mobile banking vendor companies.

In addition to the FI aspect to the mobile banking threat, the FTFC is working with the telecommunications sector through the Telecommunications Initiative (TI). As a part of the TI, the FBI is working with telecommunication organizations such as the Communication Fraud Control Association (CFCA) and the CTIA – The Wireless Association to address mobile banking and other telecommunications fraud matters. Through the relationship between both the FIs and the TIs the FBI has been able to develop fraud matters such as remote call forwarding, phishing fraud matters and telephonic denial of service (TDOS) attacks against high net worth FI customers. The FBI has ongoing relationships with a number of FI and TI partners to help organize the proactive sharing of fraud information to help mitigate or prevent economic loss. Furthermore, the FBI is beginning to share real-time intelligence with its international law enforcement (LE) partners in regards to global mobile threats. Finally, the FBI is proactively working with several anti-virus companies to stay on the forefront of mobile virus attacks and vulnerabilities.

The Department's work, and the work of our law enforcement partners, has helped to deter national and transnational cyber crime. The Verizon 2011 Data Breach Investigations Report, which is a joint study produced by Verizon, the U.S. Secret Service and the Dutch High Tech Crime Unit, found that more cyber crime investigations were conducted in 2010 than in any previous year, and concluded that the successful prosecution of identity thieves and other

cybercriminals was having a significant impact. The report's leading hypothesis, in fact, was that "the successful identification, prosecution, and incarceration of the perpetrators of many of the largest breaches in recent history is having a positive effect."

Cyber crime in the mobile context

As mobile devices become more prevalent, identity thieves and other cybercriminals will begin to target the users of these devices. In fact, this may already be happening. In March, it was widely reported by technology researchers and journalists in the Washington Post, the New York Times, and elsewhere, that more than 50 apps for the Android mobile operating system had been modified to invade user privacy. According to the reports, these modified apps, infected by malware dubbed "Droid Dream," secretly installed malicious code on the device in addition to their apparent functions. This secret malware enabled the apps to steal sensitive information from the device, receive instructions from the criminals who had made the initial modifications, and even update their malicious capabilities. This activity is an example of the migration of criminal malware attacks that have targeted personal computers for years to targeting smart phones and mobile devices. As cell phones functionality expands, the line between mobile devices and personal computers becomes thinner. For criminals, this raises the prospect of millions of new sources of valuable personal and financial data, and millions of new devices to infect with malware and transform into "bots."

For acts that are particularly egregious – such as blatant theft of financial information or the malicious installation of malware I just described – criminal liability seems both appropriate and warranted. The Department of Justice has extensive experience with investigating and successfully prosecuting criminals who distribute malware and profit from their operation. It is the policy of the Department not to comment on ongoing criminal investigations, but criminal prosecution may be the most appropriate response to deter acts of this type and severity.

When deciding whether to bring an indictment under the Computer Fraud and Abuse Act (18 U.S.C. § 1030) ("CFAA"), Department prosecutors consider a wide range of factors, including the particular facts of the case, the law of the applicable circuit, the severity of the conduct, and the needs of justice. As mobile devices and services offered to mobile device users continue to expand, it will be important to distinguish between those cases that warrant criminal prosecution and those that may be best resolved through regulatory action. For certain less egregious actions, civil enforcement by the Federal Trade Commission might be more appropriate than criminal prosecution.

In addition to collection, it is also important to consider communications providers' ability to disclose the data that they collect from their customers. In this regard, it is important to note that under current law, communications providers may voluntarily disclose or sell any non-content data – such as information about a user's location – for any reason without restriction to anyone other than state, local, and federal government agencies. The Electronic Communications Privacy Act (ECPA) provides a broad exception for covered providers to disclose appropriately collected customer information to "any person other than a governmental entity." 18 U.S.C. § 2702(c)(6). This exception was included in ECPA at a time when there was great concern over ensuring the flexible development of the then-nascent Internet industry. As the commercial landscape changes, it will be important to ensure that our laws strike the appropriate balance and adequately protect consumers' privacy.

Cyberstalking

One important consequence of the proliferation of mobile devices and services that collect location and other personal information about their users is the risk that stalkers, abusive spouses, and others intent on victimizing the user could use information from their mobile device to determine their whereabouts and activities. Stalking is not a new crime, and it is one that the Department of Justice takes very seriously. The increase in the use of mobile devices, however, raises new challenges that must be confronted.

The Department's Office on Violence Against Women (OVW) funds a number of projects that target the intersection of technology and the crimes of stalking, sexual assault, domestic violence, and dating violence. The Office recognizes that stalkers are increasingly misusing a variety of telephone, surveillance, and computer technologies to harass, terrify, intimidate, and monitor their victims, including former and current intimate partners. Perpetrators are also misusing technology to stalk before, during, and after perpetrating sexual violence. For young victims in particular, new technologies bring the risk of digital abuses such as unwanted and repeated texts, breaking into personal email accounts, and pressure for private pictures. Three OVW-funded projects, in particular, focus on "high-tech" stalking and the dangers that new technologies pose for victims.

First, for over ten years, OVW has funded the Stalking Resource Center, a program of the National Center for Victims of Crime, to provide training and technical assistance to OVW grantees and others on developing an effective response to the crime of stalking. The Stalking Resource Center has trained over 40,000 multi-disciplinary professionals nationwide, with an emphasis on the use of technology to stalk. Among other projects, the Resource Center has co-hosted nine national conferences that specifically focused on the use of technology in intimate partner stalking cases. In addition, with funding from the Department's Office for Victims of Crime, the Stalking Resource Center is currently developing two new training tools designed to help law enforcement officers, victim advocates, and allied professionals understand the most common forms of technology used by stalkers.

Second, since 2007, OVW has supported the National Network to End Domestic Violence's Safety Net Project, which works to identify best practices for using technology to assist victims. It is also concerned with training victim service providers to understand how stalkers may misuse technology and what strategies victims can use to increase their safety. In the past three years, the Safety Net Project has trained over 10,000 professionals and provided over 2,200 technical assistance consultations to OVW grantees and others.

Third, OVW funds the Family Violence Prevention Fund's "That's Not Cool" campaign to assist teens in understanding, recognizing and responding to teen dating violence. A critical part of this project is to help teens define their "digital line" as it relates to relationship and dating abuse. The website www.thatsnotcool.com was launched in January 2009 to help teens identify digital dating abuse and to encourage them to define for themselves what is and is not appropriate. So far the campaign has produced strong results, including over 900,000 website visits and 47,400 Facebook fans.

The Department has also strongly responded to the cyberstalking challenge through the prosecution of violations of the federal cyberstalking prohibition, 18 U.S.C. § 2261A. This statute allows for the prosecution of individuals who stalk using "the mail, any interactive computer service, or any facility of interstate or foreign commerce." This encompasses the use of the Internet through computers, smart phones and other mobile devices. Cases have been prosecuted under this statute based on conduct involving MySpace, Facebook and other social networking sites.

In one example of an egregious case charged under this statute, a defendant, posing as the victim, and using the victim's real name and address, posted photographs of the victim's children on a pornographic web site. Many men responded to this invitation.

The federal prohibition, however, is limited by the statutory requirement that the stalker and the victim be in different states, a requirement not found in other threatening statutes. This additional requirement may prevent prosecutors from charging cases, even where the conduct includes the most egregious acts. If an abusive spouse uses his spouse's phone to determine when she visits law enforcement for assistance, or to find where she is when she takes refuge with a friend, this may not violate 18 U.S.C. § 2261A as currently drafted because the two live in the same state. Similarly, a stalker from a victim's home town could potentially use location data from her phone to track her without violating the cyberstalking prohibition for the same reason. In fact, the case described in the previous paragraph was chargeable under 18 U.S.C. § 2261A only because the stalker and the victim, who met on the Internet, lived in different states. The

Department is considering ways to address this limitation and looks forward to working with Congress on this issue. I hope that this Committee and Congress will take the necessary steps to ensure that law enforcement can continue to protect victims of cyberstalking, and deter their tormenters.

Investigative resources for prosecuting computer crimes

Investigating and prosecuting multi-actor, multi-national crimes is extremely resource intensive. It is expensive to train and equip investigators and prosecutors to address the threat of cyber crime. As the proliferation of mobile devices provides criminals with new targets, the task of law enforcement will only get more demanding. Ensuring that law enforcement has the resources it needs to prosecute these crimes is a vital component to ensuring the safety and privacy of Americans.

For more specific details of the Department of Justice's needs for the coming year, I would direct you to the President's 2012 proposed budget, which outlines our detailed requests. In particular, the budget includes a request for funding for the Department to establish six Department of Justice Attaché positions that would emphasize the investigation and prosecution of laws prohibiting international computer hacking and protecting intellectual property rights at embassies around the world. Because computer crime is so often transnational in nature, it is vital that the Department have strong overseas representation to ensure that we can work more quickly and effectively with our international partners when investigating and prosecuting international computer crimes that target American citizens. The program would establish Department representatives at hotspots for computer and intellectual property crime around the world, and would help ensure that we can continue to protect American citizens' privacy, both at home and abroad. I hope that Congress will provide the resources that we need to establish this program and expand our resources to fight international computer crime.

Enhancing Criminal Investigations and Prosecutions

In addition to the resource demands of combating cyber crime, law enforcement must have the authority to collect electronic evidence to investigate privacy invasions and protect public safety. One key statute that addresses this need, while also ensuring a fundamental balance between privacy and public safety, is the Electronic Communications Privacy Act. ECPA empowers law enforcement to collect the evidence it needs to prosecute a wide range of crimes. Department of Justice attorneys regularly use ECPA to obtain crucial evidence from mobile devices for all manner of investigations, including terrorism, drug trafficking, violent crime, kidnappings, computer hacking, sexual exploitation of children, organized crime, gangs, and white collar offenses. But it is important to understand that it plays a central role in the investigation of criminal invasions of privacy as well. When considering how best to protect the privacy of American citizens, I would ask that the Committee remember the important role that law enforcement plays in protecting Americans from privacy threats, and how ECPA is critical to our ability to continue to pursue that role.

One particular area of concern for the Department in collecting digital evidence – and one which bears directly on this hearing's topic – is ensuring that law enforcement can successfully track criminals who use their smart phones to aid the commission of crimes. When connecting to the Internet, smart phones, like computers, are assigned Internet Protocol (IP) addresses. When a criminal uses a computer to commit crimes, law enforcement may be able, through lawful legal process, to identify the computer or subscriber account based on its IP address. This information is essential to identifying offenders, locating fugitives, thwarting cyber intrusions, protecting children from sexual exploitation and neutralizing terrorist threats – but only if the data is still in existence by the time law enforcement gets there.

In my recent testimony in January before the House Judiciary Subcommittee on Crime, Terrorism, and Homeland Security, I outlined some of the serious challenges faced by law enforcement in this area in the more traditional computer context. ISPs may choose not to store IP records, may adopt a network architecture that frustrates their ability to track IP assignments and network transactions back to a specific account or device, or may store records for only a

very short period of time. In many cases, these records are the only evidence that allows us to investigate and assign culpability for crimes committed on the Internet. In 2006, forty-nine Attorneys General wrote to Congress to express "grave concern" about "the problem of insufficient data retention policies by Internet Service Providers." They wrote that child exploitation investigations "often tragically dead-end at the door of Internet Service Providers (ISPs) that have deleted information critical to determining a suspect's name and physical location."

In one heart-wrenching example of the harm that a lack of data retention can cause, an undercover investigation that discovered a movie depicting the rape of a two-year-old child that was being traded on the internet was stymied because the ISP that had first transmitted the video had not retained information concerning the transmitter. Despite considerable effort, the child was not rescued and the criminals involved were not apprehended.

These challenges are equally serious in the context of smart phones and mobile devices. As the capabilities of smart phones expand, law enforcement increasingly encounters suspects who use their smart phones as they would a computer. For example, criminals use them to communicate with confederates and take other actions that would ordinarily provide pivotal evidence for criminal investigations. Just as some ISPs may not maintain IP address records, many wireless providers do not retain records that would enable law enforcement to identify a suspect's smart phone based on the IP addresses collected by websites that the suspect visited. When this information is not stored, it may be impossible for law enforcement to collect essential evidence.

In addition to collecting electronic evidence, it is vital to the success of the Department's mission that the scope and definition of criminal offenses is broad enough to allow us to prosecute the wide range of cybercrimes that are developing in today's increasingly networked society. This is particularly the case in the mobile context, where rapidly developing technology and services continue to provide opportunities for criminal acts. Some of the most egregious acts of privacy invasion that may be perpetrated on the users of mobile devices certainly rise to the

level of criminal action under the CFAA. These include the installation of malware, theft of financial and personal information, and similarly severe acts, some examples of which I mentioned earlier. The Department takes these crimes very seriously, and, where criminal prosecution is warranted, is committed to vigorously prosecuting offenders. To date, we have not experienced shortcomings in the CFAA vis-à-vis mobile devices. We are continuing to review these authorities but do not have any particular proposals at this time.

* * *

I appreciate the opportunity to share with you information about some of the challenges the Department sees on the horizon as Americans' use of smart phones and tablets continues to grow, and how the Department works to protect the privacy of users of mobile devices. We look forward to continuing to work with Congress as it considers these important issues.

This concludes my remarks. I would be pleased to answer your questions.