ONLINE PRIVACY, SOCIAL NETWORKING, AND CRIME VICTIMIZATION

HEARING

BEFORE THE

SUBCOMMITTEE ON CRIME, TERRORISM, AND HOMELAND SECURITY

OF THE

COMMITTEE ON THE JUDICIARY
HOUSE OF REPRESENTATIVES

ONE HUNDRED ELEVENTH CONGRESS

SECOND SESSION

JULY 28, 2010

Serial No. 111–144

Printed for the use of the Committee on the Judiciary

Available via the World Wide Web: http://judiciary.house.gov

U.S. GOVERNMENT PRINTING OFFICE
57–673 PDF WASHINGTON : 2010

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

COMMITTEE ON THE JUDICIARY

JOHN CONYERS, JR., Michigan, *Chairman*

HOWARD L. BERMAN, California
RICK BOUCHER, Virginia
JERROLD NADLER, New York
ROBERT C. "BOBBY" SCOTT, Virginia
MELVIN L. WATT, North Carolina
ZOE LOFGREN, California
SHEILA JACKSON LEE, Texas
MAXINE WATERS, California
WILLIAM D. DELAHUNT, Massachusetts
STEVE COHEN, Tennessee
HENRY C. "HANK" JOHNSON, JR., Georgia
PEDRO PIERLUISI, Puerto Rico
MIKE QUIGLEY, Illinois
JUDY CHU, California
TED DEUTCH, Florida
LUIS V. GUTIERREZ, Illinois
TAMMY BALDWIN, Wisconsin
CHARLES A. GONZALEZ, Texas
ANTHONY D. WEINER, New York
ADAM B. SCHIFF, California
LINDA T. SÁNCHEZ, California
DANIEL MAFFEI, New York
JARED POLIS, Colorado

LAMAR SMITH, Texas
F. JAMES SENSENBRENNER, JR., Wisconsin
HOWARD COBLE, North Carolina
ELTON GALLEGLY, California
BOB GOODLATTE, Virginia
DANIEL E. LUNGREN, California
DARRELL E. ISSA, California
J. RANDY FORBES, Virginia
STEVE KING, Iowa
TRENT FRANKS, Arizona
LOUIE GOHMERT, Texas
JIM JORDAN, Ohio
TED POE, Texas
JASON CHAFFETZ, Utah
TOM ROONEY, Florida
GREGG HARPER, Mississippi

PERRY APELBAUM, *Staff Director and Chief Counsel*
SEAN MCLAUGHLIN, *Minority Chief of Staff and General Counsel*

SUBCOMMITTEE ON CRIME, TERRORISM, AND HOMELAND SECURITY

ROBERT C. "BOBBY" SCOTT, Virginia, *Chairman*

PEDRO PIERLUISI, Puerto Rico
JERROLD NADLER, New York
ZOE LOFGREN, California
SHEILA JACKSON LEE, Texas
MAXINE WATERS, California
STEVE COHEN, Tennessee
ANTHONY D. WEINER, New York
MIKE QUIGLEY, Illinois
TED DEUTCH, Florida

LOUIE GOHMERT, Texas
TED POE, Texas
BOB GOODLATTE, Virginia
DANIEL E. LUNGREN, California
J. RANDY FORBES, Virginia
TOM ROONEY, Florida

BOBBY VASSAR, *Chief Counsel*
CAROLINE LYNCH, *Minority Counsel*

CONTENTS

JULY 28, 2010

ONLINE PRIVACY, SOCIAL NETWORKING, AND CRIME VICTIMIZATION

WEDNESDAY, JULY 28, 2010

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

The Subcommittee met, pursuant to notice, at 2:19 p.m., in room 2141, Rayburn House Office Building, the Honorable Robert C. "Bobby" Scott (Chairman of the Subcommittee) presiding.

Present: Representatives Scott, Lofgren, Quigley, Deutch, Gohmert, Goodlatte, and Lungren.

Staff present: (Majority) Bobby Vassar, Subcommittee Chief Counsel; Jesselyn McCurdy, Counsel; Ron LeGrand, Counsel; Joe Graupensperger, Counsel; Liliana Coronado, (Fellow) Federal Public Defender's Office Detailee; Veronica Eligan, Professional Staff Member; (Minority) Caroline Lynch, Counsel; Kimani Little, Counsel; Art Baker, FBI Detailee; and Kelsey Whitlock, Legislative Assistant.

Mr. SCOTT. Subcommittee will now come to order. And I want to apologize for starting late. We had a Judiciary Committee bill on the floor, and the rules prohibit us having a bill on the floor and meeting at the same time, so I am glad that that bill didn't take very long.

I am pleased to welcome you today to this hearing before the Subcommittee on Crime, Terrorism and Homeland Security about Internet Privacy, Social Networking and Crime Victimization.

The Internet presents individuals, in their personal and professional capacities, numerous opportunities to share personal information. Some of the information disclosed by individuals is done so incidental to the use of the Internet.

So for example, in order to use various online accounts for services such as e-mail, shopping and messaging, consumers also must establish passwords, reveal credit card numbers, and divulge other personally identifiable information.

In other circumstances, the sharing of information is central to a particular use of the Internet. For example, some Internet users actively share information, much of it extremely personal, through social networking sites.

Both categories of information present unique privacy challenges. This hearing will examine these issues and risks of criminal victimization.

Of course, we know that criminals are constantly devising new ways to infect the computers of Internet users with various types of malware. Much of this malware is intended to capture the private information of individuals and report it back to the criminal to be used in the next step to the scheme, often involving some form of identity theft.

We have Federal and state laws prohibiting this type of crime, but it is important that consumers know what they can do to protect themselves and that we demand that the Internet companies take appropriate steps to ensure the security of this information.

This is part of what we will focus on today, but we also want to pay particular attention to the special risk to victimizations based on participation in social networking.

Based on the widespread popularity of social networking sites, such as Facebook, there is no doubt that these sites provide an enjoyable and unique experience to their users. Those who use these sites are able to share information with their friends, find old friends, and establish new friendships. And in so doing, they share and broadcast some of the most sensitive and intimate details of their lives.

Unfortunately, there are those who seek out and exploit the details to perpetrate criminal acts. For example, personal details shared on these sites may allow criminals to guess a user's forgotten password clues for various online accounts.

Burglars have targeted people's homes based on information found on Facebook pages that the resident is on vacation and not at home. And based on fears about possible victimization of young people by Internet predators, Facebook has agreed to install a panic button on user pages hosted on its U.K. Web site so suspicious behavior can be reported to the authorities immediately.

One scheme that has proliferated involves hijacking of a Facebooker's user's account by a criminal who sends a financial distress call to the user's friends on that Facebook page, asking them to wire money to an account which is, unbeknownst to them, actually that of the criminal.

To discuss all these types of issues, we have a panel of witnesses representing a broad spectrum of experience and various Internet privacy issues from perspectives of law enforcement, industry, and privacy advocacy.

Before we proceed with their testimony, it is my pleasure to recognize the Ranking Member of the Subcommittee, my colleague from Texas, Judge Gohmert.

Mr. GOHMERT. Thank you, Mr. Chairman. I do appreciate you holding this hearing on a very important topic, privacy, social networking and crime victimization have become competing interests as the Internet continues to revolutionize the way we conduct commerce, seek employment, keep up with family and friends, make new friends, and communicate in general.

The Internet's impact on communication and on society is often compared to the impact that the invention of the printing press had on the literary market. We are in the midst of a technology evolution like never seen before.

Every year, or even more frequently, there is some new gadget that is faster and smaller than its predecessor, or capable of doing

something that was never thought possible. This has certainly been true in all aspects of personal computing and the development and access to the Internet.

The Internet has not only facilitated communication, but other aspects of everyday life, as well. We no longer have to go to the post office to pay a bill. We can buy books, food, furniture, just about every other thing without going to a store. We can now look for a new home or a new car at any hour of the day simply by logging on.

Unfortunately, with these benefits and conveniences come new ways to commit crimes and new ways to exploit our personal information. The conveniences generally seem to outweigh the risk. But by educating ourselves about the potential risk and vulnerabilities created by these conveniences, Internet users can help prevent the spread of identity theft and other crimes on the Web.

Identity thieves who hack into your personal computer or a merchant computer, steal your personal information, have received considerable attention by the media and Congress. People have become aware of identity theft, interchanging their habits to prevent becoming a victim.

You don't have to look any further than the popularity of personal shredding machines to realize that habits do often change when there is awareness of the risk.

But there are new schemes and new variations of old schemes employed by criminals to defeat the security measures and actions taken by a concerned public. For instance, within the last few months, staff of this Committee received e-mails supposedly from a former staffer asking that money be wired immediately to a certain account as a sender claimed to be the victim of a robbery while touring London.

When the sender could not answer basic questions, the communications stopped. Later, it was learned the former staffer's Internet address book had been compromised, and everyone in it received the same plea for help. This scam has also apparently been attempted using social networking sites.

The dramatic increase in the popularity of social networking sites has perhaps overshadowed some of the risk of sharing too much information in those forums. Unlike the sensitive but relatively limited information needed to make an online purchase, these social networking sites provide the opportunity and the temptation to incrementally put more and more personal information into cyberspace.

Most users who have no real sense of who can see this information, or what can be done with it or what steps can be taken to prevent it from being exploited, and all of this information is a potential treasure trove for identity thieves and for the facilitation of other crimes. Some in the information industry refer to personal information as "The new currency of crime."

According to a recent national survey of 2,000 online households conducted by the Consumer Reports National Research Center, two out of three online U.S. households use social networks, nearly twice as many as a year ago. But millions who use these services put themselves and their families at risk by exposing very sensitive personal information. If a picture is really worth 1,000 words, some

of the visuals that are posted on these sites say way too much, and in all likelihood can assist a predator in choosing their prey.

Again, I want to thank the Chairman for holding this hearing. I firmly believe that making the public aware of some of the new dangers associated with the ever-expanding Internet is an important tool for Internet users, particularly teenagers and children, to protect themselves.

This is particularly true here in Congress, where we have software and hardware that is so secure that only we and the Chinese have access to all our secrets.

With that, I yield back, and thank you for the time, Chairman.

Mr. SCOTT. Thank you. And we have one panel of witnesses with us. Excuse me, does the gentleman from Virginia have a comment?

Mr. GOODLATTE. Just briefly, Mr. Chairman, I want to thank you for holding this hearing. As the co-chairman of the bipartisan Congressional Internet Caucus and chairman of the House Republican High-Tech Working Group, this is a very, very important discussion about how to prevent crime and keep people safe on the Internet.

It is a rapidly evolving technology, and we have got to make sure that the Internet does not become the wild, Wild West of the 21st century. But there are a lot of exciting new developments going on not only to make new services available to people, but also to empower them to, in many ways, get a better handle on controlling their access to the Internet in terms of the information that they provide and that they can determine how to provide it.

In addition, social networking technologies like Facebook—and Facebook, quite frankly, has been a leader in this regard—have done a great service to the Internet by making greater transparency for the people who are legitimately and honestly using the Internet. If you go on a technology like Facebook, you have got to disclose who you are, and therefore you can see, as you participate, who you are and decide for yourself who you want to share that information with.

But it also is a move away from people thinking that they can anonymously undertake activities on the Internet to perform various types of criminal activities. The more we promote that type of activity, the fact that you identify yourself and who you are, and you decide for yourself what information you are going to share, I think the greater progress we will make in being able to crack down on the people who want to think that they are operating in the shadows of the Internet and conducting crime.

Now, there are lots that people have to learn about that as they do it so that they can understand how they best can protect themselves, and the technologies need to evolve further to root out people who would conduct criminal activity on the Internet.

But I think that is what we should be learning about today and encouraging today so that the Internet can continue to grow and continue to be the educational tool, the tool for commerce, the tool for entertainment that it has become and is enjoyed by hundreds of millions of Americans and billions of people around the world. So I look forward to hearing from our witnesses today.

Thank you, Mr. Chairman.

Mr. SCOTT. Thank you. And I would like to thank you for your hard work on a lot of the technology issues that many of us have trouble understanding. You and our other colleague from Virginia, Mr. Boucher, have done a lot of work in a bipartisan way in cooperation, which is very helpful to the Committee. So we want to thank you for your leadership.

Our first witness today will be Gordon Snow, who is assistant director of FBI's cyber division. He has had a distinguished career with the FBI, including positions as a section chief in cyber national security section and the director, the National Cyber Investigative Joint Task Force.

Our second witness will be Michael Merritt, who is assistant director of the Secret Service's Office of Investigations. He oversees the Secret Service's criminal investigations, including those of electronic and financial crimes.

Our third witness will be Joe Sullivan, who is the chief security officer for Facebook. He is a former assistant U.S. attorney and has the daily responsibility for overseeing Facebook's security policies.

Our fourth witness will be Mark Rotenberg, who is the executive director of the Electronic Privacy Information Center. His organization is one of the leading advocates of online privacy rights and has taken a special interest in these interests as they relate to social networking.

Our fifth and final witness will be Joe Pasqua, who is the vice president of research for Symantec Corporation. He has led the efforts in that corporation in areas such as online safety, reputation-based security and data protection.

Each of our witnesses' written statements will be entered into the record in its entirety. We ask our witnesses to summarize his or her testimony in 5 minutes or less. And to help stay within the time, there is a timing device at the table which will begin green, and when 1 minute is left, it will turn to yellow, and turn red when 5 minutes have expired.

Also want to recognize our colleague from Florida, Mr. Deutch. Did you have a comment? Okay. Thank you very much.

So we will begin with Assistant Director Snow.

TESTIMONY OF GORDON M. SNOW, ASSISTANT DIRECTOR, FEDERAL BUREAU OF INVESTIGATION, UNITED STATES DEPARTMENT OF JUSTICE, WASHINGTON, DC

Mr. SNOW. Good afternoon, Chairman Scott, Ranking Member Gohmert and Members of the Subcommittee. I appreciate the opportunity to testify before you today regarding the FBI's efforts to combat cybercrime as it relates to social networking sites.

Regardless of which social networking is used, online——

Mr. SCOTT. Mr. Snow, could you bring your mic a little closer to you?

Mr. SNOW. Regardless of which social networking site is used, online users continue to be fooled by persons claiming to be somebody else. Individuals can misrepresent everything about themselves while they communicate online, their names and business affiliations, and also their gender, age and location, identifiers that are far more difficult to fake in person.

Years ago, we called these type of people "confidence men," or con men. Today, we refer to them as being engaged in social engineering.

There are a variety of Internet fraud schemes being used by cyber criminals at any given time. By way of example, a recent fraud scheme involves a cyber criminal gaining access to an unsuspecting users' e-mail account or social networking account, claiming to be the account holder and sending messages to many of the users' friends.

In the message, the con man states that he is on travel and has been robbed of his credit cards, passport, money and cell phone. He also states the need for money is immediate. Without realizing the message is from a criminal, the victims of the fraud account holder contacts often wires money to an overseas account without validating the claim.

Another tool used by criminals to exploit social networking sites is a technique called phishing. Phishing schemes attempt to make Internet users believe that they are receiving messages from a trusted source.

Phishing attacks on members come in various formats, including messages within the social networking site, either from strangers or from compromised friends' accounts, links or videos within a social networking profile leading to something harmful, or e-mails sent to users claiming to be from the social network site itself.

Users fall victim to the schemes due to higher level of trust typically displayed while using social networking sites. Users often accept into their private sites people they do not actually know, or they sometimes fail to set privacy settings on their profile which might help avoid these attacks.

Cyber-thieves also used data mining techniques on social networking sites to extract sensitive information about the victims. For example, a "Getting To Know You" quiz sent to a large list of social networking site users, while not appearing malicious, may mimic the same questions that are asked by financial institutions or e-mail account providers when the individual has forgotten their password. An e-mail address in the answer to the quiz questions can provide the cyber-criminal with the tools to enter your bank account, your e-mail account or credit card in order to transfer money or siphon off your savings and investments.

The potential for considerable profits in this realm is enticing young criminals and resulted in the creation of a large economy known as the cyber-underground. The underground is governed by rules and logic that closely mimic those of the legitimate business world, including a unique language, a set of expectations about its members' conduct, and a system of stratification based on knowledge and skill, activities and reputation.

Beyond cyber-crime, valuable national security information can also be inadvertently exposed by military or government personnel via their social networking site profile. In a recently publicized case, an individual created a fake profile on multiple social networking sites posing as an attractive female intelligence analyst and extended friend requests to government contractors, military and other government personnel. Many of the friend requests were accepted. According to press accounts, the deception provided its

creator with access to a fair amount of sensitive data, including a picture from a soldier taken on patrol in Afghanistan that contained embedded data identifying his exact location.

Mr. Chairman, the Department of Justice and the FBI, in collaboration with our inter-agency partners, have been working closely with the new cyber-security office at the White House to address the President's national efforts to investigate and prosecute cyber-crime. To this end, we have established cyber-squads in each of our 56 field offices around the country, with more than 1,000 specially trained agents, analysts and digital forensic experts.

Still, we cannot combat this threat alone. Some of the best tools in the FBI's arsenal are our longstanding partnerships with federal, state, local and international law enforcement agencies, as well as with private sector and academia.

These relationships include our partnerships with the National White Collar Crime Center at the Internet Crime Complaint Center, the National Cyber Forensic and Training Alliance, and the InfraGard program. We also partner with the Information Sharing and Analysis Centers and the National Center for the Missing and Exploited Children.

Chairman Scott, Ranking Member Gohmert and Members of the Subcommittee, in the interest of time today, I have touched upon some of the more pervasive methods of criminal activity via social networking. I would be more than happy to further expand upon any of these issues during questioning, and I appreciate the opportunity to come before you today and share the work with FBI is doing to address the threat posed by cyber-criminals in this country and around the world.

[The prepared statement of Mr. Snow follows:]

PREPARED STATEMENT OF GORDON M. SNOW

STATEMENT OF GORDON M. SNOW
ASSISTANT DIRECTOR, CYBER DIVISION
FEDERAL BUREAU OF INVESTIGATION
BEFORE THE HOUSE JUDICIARY SUBCOMMITTEE ON CRIME, TERRORISM, AND HOMELAND SECURITY

JULY 28, 2010

Good morning, Chairman Scott, Ranking Member Gohmert and Members of the Subcommittee. I appreciate the opportunity to testify before you today regarding the FBI's efforts to combat cyber crime as it relates to social networking sites.

Let me begin by acknowledging that the rapid expansion of the Internet has allowed us to learn, to communicate, and to conduct business in ways that were unimaginable 20 years ago. Still, the same technology, to include the surge in the use of social networking sites over the past two years, has given cyber thieves and child predators new, highly effective avenues to take advantage of unsuspecting users. These cyber criminals are using a variety of schemes to defraud or victimize innocent social networking site users, some of which I would like to highlight today.

Social Engineering

Regardless of the social networking site, users continue to be fooled online by persons claiming to be somebody else. Unlike the physical world, individuals can misrepresent everything about themselves while they communicate online, ranging not only from their names and business affiliations (something that is fairly easy to do in-person as well), but extending as well to their gender, age, and location (identifiers that are far more difficult to fake in-person). Years ago, we called these types of people confidence or "con"-men. Perhaps as a result of today's hi-tech times, con artists are now referred to as being engaged in social engineering. It should come as no surprise to learn that the FBI is investigating classic investment fraud schemes, such as Ponzi schemes, that are now being carried out in virtual worlds. Other con artists are able to conduct Identity Theft crimes by misidentifying themselves on social networking sites and then tricking their victims into giving them their account names and passwords as well as other personally identifiable information.

In addition to Identity Theft crimes, child predators routinely use social networking sites to locate and communicate with future victims and other pedophiles. In at least one publicized case from last year, an individual attempted to extort nude photos of teenage girls after he gained control of their email and social networking accounts. That particular FBI investigation led to an 18 year federal sentence for the offender, reflecting that these crimes are serious and will not be tolerated.

Fraud Schemes

There are a variety of Internet fraud schemes being used by cyber criminals at any given time. By way of example, a recent fraud scheme involves a cyber criminal gaining access to an unsuspecting user's email account or social networking site. The fraudster, who claims to be the account holder, then sends messages to the user's friends. In the message, the fraudster states that he is on travel and has been robbed of his credit cards, passport, money, and cell phone; and is in need of money immediately. Without realizing that the message is from a criminal, the friends wire money to an overseas account without validating the claim.

Phishing Scams

Phishing schemes attempt to make Internet users believe that they are receiving e-mail from a trusted source when that is not the case. Phishing attacks on social networking site users come in various formats, including: messages within the social networking site either from strangers or compromised friend accounts; links or videos within a social networking site profile claiming to lead to something harmless that turns out to be harmful; or e-mails sent to users claiming to be from the social networking site itself. Social networking site users fall victim to the schemes due to the higher level of trust typically displayed while using social networking sites. Users often accept into their private sites people that they do not actually know, or sometimes fail altogether to properly set privacy settings on their profile. This gives cyber thieves an advantage when trying to trick their victims through various phishing schemes.

Social networking sites, as well as corporate websites in general, provide criminals with enormous amounts of information to send official looking documents and send them to individual targets who have shown interest in specific subjects. The personal and detailed nature of the information erodes the victim's sense of caution, leading them to open the malicious email. Such email contains an attachment that contains malicious software designed to provide the email's sender with control over the victim's entire computer. Once the malware infection is discovered, it is often too late to protect the data from compromise.

Cyber criminals design advanced malware to act with precision to infect, conceal access, steal or modify data without detection. Coders of advanced malware are patient and have been known to test a network and its users to evaluate defensive responses. Advanced malware may use a "layered" approach to infect and gain elevated privileges on a system. Usually, these types of attacks are bundled with an additional cyber crime tactic, such as social engineering or zero day exploits. In the first phase of a malware infection, a user might receive a spear phishing email that obtains access to the user's information or gains entry into the system under the user's credentials. Once the cyber criminal initiates a connection to the user or system, they can further exploit it using other vectors that may give them deeper access to system resources. In the second phase, the hacker might install a backdoor to establish a persistent presence on the network that can no longer be discovered through the use of anti-virus software or firewalls.

Data Mining

Cyber thieves use data mining on social networking sites as a way to extract sensitive information about their victims. This can be done by criminal actors on either a large or small scale. For example, in a large-scale data mining scheme, a cyber criminal may send out a "getting to know you quiz" to a large list of social networking site users. While the answers to these questions do not appear to be malicious on the surface, they often mimic the same questions that are asked by financial institutions or e-mail account providers when an individual has forgotten their password. Thus, an e-mail address and the answers to the quiz questions can provide the cyber criminal with the tools to enter your bank account, e-mail account, or credit card in order to transfer money or siphon your account. Small-scale data mining may also be easy for cyber criminals if social networking site users have not properly guarded their profile or access to sensitive information. Indeed, some networking applications encourage users to post whether or not they are on vacation, simultaneously letting burglars know when nobody is home.

The Cyber Underground

The impact of cyber crime on individuals and commerce can be substantial, with the consequences ranging from a mere inconvenience to financial ruin. The potential for considerable profits is enticing to young criminals, and has resulted in the creation of a large underground economy known as the cyber underground. The cyber underground is a pervasive market governed by rules and logic that closely mimic those of the legitimate business world, including a unique language, a set of expectations about its members' conduct, and a system of stratification based on knowledge and skill, activities, and reputation.

One of the ways that cyber criminals communicate within the cyber underground is on website forums. It is on these forums that cyber criminals buy and sell login credentials (such as those for e-mail, social networking sites, or financial accounts); where they buy and sell phishing kits, malicious software, access to botnets; and victim social security numbers, credit cards, and other sensitive information. These criminals are increasingly professionalized, organized, and have unique or specialized skills.

In addition, cyber crime is increasingly transnational in nature, with individuals living in different countries around the world working together on the same schemes. In late 2008, an international hacking ring carried out one of the most complicated and organized computer fraud attacks ever conducted. The crime group used sophisticated hacking techniques to compromise the encryption used to protect data on 44 payroll debit cards, and then provided a network of "cashers" to withdraw more than $9 million from over 2,100 ATMs in at least 280 cities worldwide, including cities in the United States, Russia, Ukraine, Estonia, Italy, Hong Kong, Japan and Canada. The $9 million loss occurred within a span of less than 12 hours. The cyber underground facilitates the exchange of cyber crime services, tools, expertise, and resources, which enables this sort of transnational criminal operation to take place across multiple countries.

Beyond Cyber Crime

Apart from the cyber crime consequences associated with social networking sites, valuable information can be inadvertently exposed by military or government personnel via their social networking site profile. In a recently publicized case, an individual created a fake profile on multiple social networking sites posing as an attractive female intelligence analyst and extended friend requests to government contractors, military and other government personnel. Many of the friend requests were accepted, even though the profile was of a fictitious person. According to press accounts, the deception provided its creator with access to a fair amount of sensitive data, including a picture from a soldier taken on patrol in Afghanistan that contained embedded data identifying his exact location. The person who created the fake social networking sites, when asked what he was trying to prove, responded: "The first thing was the issue of trust and how easily it is given. The second thing was to show how much different information gets leaked out through various networks." He also noted that although some individuals recognized the sites as fake, they had no central place to warn others about the perceived fraud, helping to ensure 300 connections in a month.

This last point is worth expanding upon. Some social networking sites have taken it upon themselves to be model corporate citizens by voluntarily providing functions for users to report acts of abuse. A number of sites have easy to use buttons or links that, with a single click, will send a message to the system administrator alerting them of potentially illegal or abusive content. Unfortunately though, many sites have not followed the lead. Some sites provide users with no ability to report abuse, while others either intentionally or unintentionally discourage reporting by requiring users to complete a series of onerous steps every time they want to report abuse.

FBI Cyber Mission and Strategic Partnerships

The Department of Justice leads the national effort to prosecute cyber crime, and the FBI, in collaboration with other Federal law enforcement agencies, investigates cyber crime. The FBI's cyber crime mission is four-fold: first and foremost, to stop those behind the most serious computer intrusions and the spread of malicious code; second, to identify and thwart online sexual predators who use the Internet to meet and exploit children and to produce, possess, or share child pornography; third, to counteract operations that target U.S. intellectual property, endangering our national security and competitiveness; and fourth, to dismantle national and transnational organized criminal enterprises engaging in Internet fraud. To this end, we have established cyber squads in each of our 56 field offices around the country, with more than 1,000 specially trained agents, analysts, and digital forensic examiners. Still, we can not combat this threat alone.

Some of the best tools in the FBI's arsenal for combating any crime problem are its long-standing partnerships with federal, state, local and international law enforcement agencies, as well as with the private sector and academia. At the federal level, and by Presidential mandate, the FBI leads the National Cyber Investigative Joint Task Force (NCIJTF) as a multi-agency national focal point for coordinating, integrating, and sharing

pertinent information related to cyber threat investigations in order to determine the identity, location, intent, motivation, capabilities, alliances, funding, and methodologies of cyber threat groups and individuals. In doing so, the partners of the NCIJTF support the US Government's full range of options across all elements of national power.

The FBI also partners closely with not-for-profit organizations, including extensive partnerships with the National White Collar Crime Center (NW3C) in establishing the Internet Crime Complaint Center (IC3), the National Cyber-Forensic and Training Alliance (NCFTA), the InfraGard National Members Alliance in establishing InfraGard, the Financial Services Information Sharing & Analysis Center (FS-ISAC), and the National Center for Missing and Exploited Children (NCMEC).

Just one recent example of coordination highlights how effective we are when working within these closely established partnerships. Earlier this year, Romanian police and prosecutors conducted one of Romania's largest police actions ever - an investigation of an organized crime group engaged in Internet fraud. The investigation deployed over 700 law enforcement officers who conducted searches at 103 locations, which led to the arrest of 34 people. Over 600 victims of this Romanian crime ring were US citizens. The success in bringing down this group was based in large part on the strength of our partnership with Romanian law enforcement and our domestic federal, state and local partners. Through extensive coordination by the FBI's Legal Attache (Legat) in Bucharest, the Internet Crime Complaint Center provided the Romanians with over 600 complaints it had compiled from submissions to the www.IC3.gov reporting portal. In addition, and again in close coordination with the FBI's Legat, over 45 FBI field offices assisted in the investigation by conducting interviews to obtain victim statements on Romanian complaint forms, and by obtaining police reports and covering other investigative leads within their divisions.

Working closely with others, sharing information, and leveraging all available resources and expertise, the FBI and its partners have made significant strides in combating cyber crime. Clearly, there is more work to be done, but through a coordinated approach we have become more nimble and responsive in our efforts to bring justice to the most egregious offenders.

Conclusion

Chairman Scott, Ranking Member Gohmert and Members of the Subcommittee, I appreciate the opportunity to come before you today and share the work that the FBI is doing to address the threat posed by cyber criminals in this country and around the globe. I am happy to answer any questions.

Mr. SCOTT. Thank you, Mr. Snow.

We have been joined by the gentlelady from California, Ms. Lofgren, who has taken a strong interest in this issue, and thank you for coming.

Mr. Merritt?

TESTIMONY OF MICHAEL P. MERRITT, ASSISTANT DIRECTOR, UNITED STATES SECRET SERVICE, UNITED STATES DEPARTMENT OF HOMELAND SECURITY, WASHINGTON, DC

Mr. MERRITT. Good afternoon, Chairman Scott, Ranking Member Gohmert and other distinguished Members of the Committee. Thank you for the opportunity to testify on the Secret Service's role investigating cyber and computer-related crimes.

As the original guardian of the Nation's financial infrastructure, the Secret Service has a long, distinguished history of protecting American consumers and financial institutions from fraud. Over the last 145 years, our criminal investigators have confronted all types of financial fraud, from paper to plastic to computer-based attacks targeting our financial payment schemes.

In recent years, our investigations have revealed a significant increase in the quantity and complexity of cyber cases involving various computer networks in the United States. Broader access to advanced computer technologies and the widespread use of the Internet have fostered the growth of transnational cyber criminals, which has resulted in a marked increase in computer-related crimes targeting our Nation's financial infrastructure.

Current trends show an increase in network intrusions, hacking attacks, malicious software, and account takeovers, resulting in data breaches affecting every sector of the American economy. In addition, social networking sites have become prime targets for cyber-criminals to expand their prospects for facilitating malicious or fraudulent activity.

As documented in the 2010 Secret Service Verizon data breach investigative report, the use of social engineering tactics to obtain personally identifiable information has increased. While cyber-criminals operate anonymously in a world without borders, the law enforcement community is limited by jurisdictional boundaries. Thus, the international scope of these cyber-crime cases has increased the time and resources required for successful investigation and adjudication.

In addition, the level of collaboration among these transnational cyber-criminals has raised the complexity of these cases and the potential for greater harm.

To address the emerging threats posed by these transnational groups, the Secret Service has adopted a multifaceted approach to investigating these crimes while working to prevent future attacks. A central component of our approach is the training provided through our electronic crime special agent program. Today, roughly 1,300, or more than half of our field office special agents, have received training in forensic identification and the preservation and retrieval of electronically stored evidence.

In addition, since 2008, the Secret Service, through the National Computer Forensics Institute, has provided computer forensics training to 836 state and local law enforcement officials rep-

resenting over 300 agencies from all 50 states and two territories. As cyber-crimes continue to increase in size, scope and depth, the Secret Service is committed to sharing information and best practices with our law enforcement partners, academia, and the private sector.

To accomplish this, we have established 29 electronic crime task forces, including the first international task force, based in Rome, Italy.

Currently, membership in our ECTFs includes approximately 5,500 partners from law enforcement and the private sector and academia. These partners have access to the resources provided through our international network of ECTFs. To coordinate these investigations at the headquarters level, the Secret Service has enhanced our cyber-intelligence section to focus on generating new leads in support of our cyber-investigations.

The men and women who work in this section have been instrumental in our success in infiltrating online cyber-criminal networks around the world. These successful investigations include two of the largest known network intrusion cases to date, TGX and the Heartland Payment Systems case. These intrusions resulted in the compromise of approximately 40 million accounts and 130 million accounts respectively and the indictment of dozens of suspects.

As detailed in my written statement, the Secret Service has implemented a number of initiatives to combat the scourge of cyber and computer-related crimes. Today, social networking sites provide yet another target-rich environment for cyber-criminals to exploit personal identifiable information.

Responding to the growth in these types of crimes and the level of sophistication these criminals employ will demand an increase in resources and greater collaboration between law enforcement and the private sector. Accordingly, the Secret Service will focus its resources on increasing public awareness through education, providing training for our local law enforcement partners, and adjusting our investigative techniques to stay ahead of the criminal trends.

The Secret Service is committed to our mission of safeguarding our Nation's critical financial infrastructure and will continue to aggressively investigate cyber and computer-related crimes to protect American consumers and financial institutions from harm.

Chairman Scott, Ranking Member Gohmert and distinguished Members of the Committee, this concludes my prepared statement. Thank you again for this opportunity to testify on behalf of the Secret Service. I will be pleased to answer any questions at your convenience.

Thank you.

[The prepared statement of Mr. Merritt follows:]

PREPARED STATEMENT OF MICHAEL P. MERRITT

Statement of Mr. Michael P. Merritt
Assistant Director
Office of Investigations
U.S. Secret Service

Before the House Committee on the Judiciary
Subcommittee on Crime, Terrorism and Homeland Security
U.S. House of Representatives

July 28, 2010

Good morning, Chairman Scott, Ranking Member Gohmert and distinguished members of the Subcommittee. Thank you for the opportunity to testify on the subject of cyber and computer-related crimes and the role of the U.S. Secret Service (Secret Service) in cyber investigations.

While the Secret Service is perhaps best known for protecting our nation's leaders, we were established in 1865 to investigate and prevent the counterfeiting of United States currency. As the original guardian of the nation's financial payment system, the Secret Service has a long history of protecting American consumers, industries, and financial institutions from fraud. Congress continues to recognize the Secret Service's 145 years of investigative expertise in financial crimes and over the last two decades has expanded our statutory authorities to include access device fraud (18 USC §1029), which includes credit and debit card fraud. Congress has also given the Secret Service concurrent jurisdiction with other law enforcement agencies for identity theft (18 USC §1028), computer fraud (18 USC §1030), and bank fraud (18 USC §1344). As a result, the Secret Service is recognized worldwide for our investigative expertise and innovative approaches to detecting, investigating, and preventing financial crimes.

Trends in Cyber and Computer-Related Crimes

In recent years, the Secret Service has observed a significant increase in the quality, quantity, and complexity of cyber-cases in which perpetrators target financial institutions within the United States and abroad. Advances in computer technology and greater access to personal information via the Internet have created a virtual marketplace for transnational cyber criminals to share stolen information. As a result, the Secret Service has observed a marked increase in cyber and computer-related crimes targeting private industry and critical infrastructures. These crimes include network intrusions, hacking attacks, malicious software, and account takeovers leading to significant data breaches affecting every sector of the world economy. As large companies

have adopted more sophisticated defenses against cyber-crime, criminals have increased their attacks against small and medium-sized businesses, banks, and data processors. Unfortunately, many smaller businesses do not have the resources to adopt and continuously upgrade the sophisticated protections needed to safeguard data from being compromised.

The Secret Service is concerned about cases involving network intrusions at businesses to include attempts to exploit popular social networking sites such as Facebook, MySpace, and LinkedIn. These acts can often result in the compromise of users' personal information which can subsequently be misused to facilitate fraud or perpetrate other types of crimes (e.g., stalking). The social networking sites in particular are attractive targets because of their large memberships, the abundant amount of personal information contained in users' profiles and messages, and the trust members have that they are actually receiving communications from their online friends. According to a recent news report, a private Internet security company was able to view highly personal information from 40 percent of 200 Facebook users who chose to add a fictitious member to their Facebook accounts. The company created this fictional member to illustrate how vulnerable people can be when using social networks. In addition, cyber criminals view these sites as highly effective distribution points for malware, as well as the command and control centers for bot networks.

A portion of this type of electronic theft appears to be attributable to organized cyber-groups, many of them based abroad, which pursue both the intrusions and the subsequent exploitation of the stolen data. Stolen credit card information is often trafficked in units that include more than just the card number and expiration date. These "full-info cards" include additional information, such as the card holder's full name and address, mother's maiden name, date of birth, Social Security number, a Personal Identification Number (PIN), and other personal information that allows additional criminal exploitation of the affected individual.

Although network intrusions can be devastating to a company of any size, the theft of data and customer information often has more dire consequences on a small or medium-sized company that most likely does not have the resources or expertise necessary to properly protect their networks and data, resulting in the loss of personal identifying information. For example, in October 2007, the Secret Service identified a complex fraud scheme in which servers owned by a payroll company were compromised by a network intrusion. Subsequently, four debit card accounts belonging to a small Midwestern bank were compromised, distributed online, and used in a coordinated attack resulting in Automated Teller Machine (ATM) withdrawals in excess of $5 million. The withdrawals involved 9,000 worldwide transactions in less than two days resulting in the victim bank filing for Chapter 11 bankruptcy protection. Our investigation revealed that the criminals compromised the payroll company's database, reset PINs, loaded balances onto the accounts, and removed account withdrawal limits or set the limits at extremely high levels.

Through this investigation, the Secret Service also identified another organized cyber-group in New York City trafficking stolen credit card data that was transmitted by multiple suspects operating in Russia and the Ukraine. Following the investigative leads generated in this case, the Secret Service was able to prevent additional losses by notifying victims of the intrusion and compromise, often before the victims became aware of the illicit activity. For example, the

Secret Service discovered that the computer network of a U.S. bank had been compromised. Subsequent notification by the Secret Service enabled the bank to significantly reduce its exposure and avoid potential losses exceeding $15 million. Based on these investigative efforts, the Secret Service identified 15 compromised financial institutions, $3 million in losses, 5,000 compromised accounts, and prevented more than $20 million in potential losses to U.S. financial institutions and consumers.

The increasing level of collaboration among cyber-criminals raises both the complexity of investigating these cases and the level of potential harm to companies and individuals alike. Illicit Internet carding portals allow criminals to traffic stolen information in bulk quantities globally. These portals, or "carding websites," operate like online bazaars where criminals converge to trade personal financial data and cyber-tools of the trade. The websites vary in size, from a few dozen members to some of the more popular sites boasting memberships of approximately 8,000 users. Within these portals, there are separate forums moderated by notorious members of the carding community. Members meet online and discuss specific topics of interest. Criminal purveyors buy, sell, and trade malicious software, spamming services, credit, debit, and ATM card data, personal identification data, bank account information, hacking services and other contraband.

Although difficult to accomplish, the Secret Service has managed to infiltrate many of the "carding websites." One such infiltration allowed the Secret Service to initiate and conduct a three-year investigation that led to the identification and high-profile indictment of 11 perpetrators involved in hacking nine major U.S. retailers and the theft and sale of more than 40 million credit and debit card numbers. The investigation revealed that defendants from the United States, Estonia, China, and Belarus successfully obtained credit and debit card numbers by hacking into the wireless computer networks of major retailers — including TJX Companies, BJ's Wholesale Club, OfficeMax, Boston Market, Barnes & Noble, Sports Authority, and Dave & Buster's. Once inside the networks, they installed "sniffer" programs that would capture card numbers, as well as password and account information, as they moved through the retailers' credit and debit processing networks. After the data was collected, the conspirators concealed the information in encrypted computer servers that they controlled in the United States and Eastern Europe. The credit and debit card numbers were then sold through online transactions to other criminals in the United States and Eastern Europe. The stolen numbers were "cashed out" by encoding card numbers on the magnetic strips of blank cards. The defendants then used these cards to withdraw tens of thousands of dollars at a time from ATMs. The defendants were able to conceal and launder their fraud proceeds by using anonymous Internet-based electronic currencies within the United States and abroad, and by channeling funds through bank accounts in Eastern Europe.

In both of these cases, the ripple effects of the criminal acts extend well beyond the companies compromised. In one example alone, millions of individual card holders were affected. Although swift investigation, arrest, and prosecution prevented many consumers from direct financial harm, all of the potential victims were at risk for misuse of their credit cards, overall identity theft, or both. Also, costs suffered by businesses, such as the need for enhanced security measures, reputational damage, and direct financial losses, are ultimately passed on to consumers.

Collaboration with Other Federal Agencies; State and Local Law Enforcement; Private Sector; and Academia

While cyber-criminals operate in a world without borders, the law enforcement community does not. The multi-national, multi-jurisdictional nature of these cyber-crime cases has increased in complexity and, accordingly, increased the time and resources needed for successful investigation and adjudication. As an example, the partnerships developed through our Electronic Crimes Task Forces, the support provided by our Cyber Intelligence Section, the liaison established by our overseas offices, and the training provided by Electronic Crimes Special Agent Program were all instrumental to the Secret Service's successful investigation into the network intrusion of Heartland Payment Systems (HPS). An August 2009 indictment alleged that a transnational organized criminal group used various network intrusion techniques to breach security, navigate the credit card processing environment, and plant a "sniffer," a data collection device, to capture payment transaction data.

The Secret Service investigation revealed data from more than 130 million credit card accounts were at risk of being compromised and ex-filtrated to a command and control server operated by an international group directly related to other ongoing Secret Service investigations. During the course of the investigation, the Secret Service uncovered that this international group committed other intrusions into multiple corporate networks to steal credit and debit card data. The Secret Service relied on various investigative methods, including subpoenas to identify three main suspects, search warrants, and Mutual Legal Assistance Treaties with our foreign law enforcement partners. As a result of this investigation, the three suspects in the case were indicted and prosecuted for various computer-related crimes. This case represents the largest and most complex data breach investigation ever prosecuted in the United States.

Recognizing these complexities, several federal agencies are collaborating to investigate cases and identify proactive strategies. Greater collaboration within the federal, state, and local law enforcement community enhances information sharing, promotes efficiency in investigations, and facilitates efforts to de-conflict in cases of concurrent jurisdiction. As a part of these efforts and to ensure that information is shared in a timely and effective manner, the Secret Service has personnel detailed to the following DHS and non-DHS entities:

- National Protection and Program Directorate's (NPPD) – Office of the Under Secretary;
- NPPD's National Cyber Security Division (US-CERT);
- NPPD's Office of Infrastructure Protection;
- Department of Homeland Security's Science and Technology Directorate (S&T);
- White House Homeland Security Staff;
- Department of Justice National Cyber Investigative Joint Task Force (NCIJTF);
- Each Federal Bureau of Investigation Joint Terrorism Task Force (JTTF), including the National JTTF;
- Department of the Treasury - Terrorist Finance and Financial Crimes Section
- Department of the Treasury - Financial Crimes Enforcement Network (FinCEN);
- Central Intelligence Agency;
- National Security Council;

- The Drug Enforcement Administration's International Organized Crime and Intelligence Operations Center;
- EUROPOL; and
- INTERPOL

To continue to fulfill our obligation to protect our financial infrastructure, industry, and the American public, the Secret Service has adopted a multi-faceted approach to aggressively combat cyber and computer-related crimes. The Secret Service has dismantled and continues to dismantle some of the largest known transnational cyber-criminal organizations by:

- providing the necessary computer-based training to enhance the investigative skills of special agents through our **Electronic Crimes Special Agent Program (ECSAP)**;
- collaborating with other law enforcement agencies, private industry, and academia through our 29 **Electronic Crimes Task Forces (ECTF)**;
- identifying and locating international cyber-criminals involved in network intrusions, identity theft, credit card fraud, bank fraud, and other computer-related crimes through the analysis provided by our **Cyber Intelligence Section (CIS)**;
- providing state and local law enforcement partners with the necessary computer-based training, tools, and equipment to enhance their investigative skills through the **National Computer Forensics Institute (NCFI)**;
- maximizing partnerships with international law enforcement counterparts through our **international field offices**; and
- maximizing technical support, research and development, and public outreach through the Secret Service **CERT Liaison Program (CLP)** at Carnegie Mellon University.

Electronic Crimes Special Agent Program (ECSAP)

A central component of the Secret Service's cyber-crime investigations is its Electronic Crimes Special Agent Program (ECSAP). This program is comprised of 1343 Secret Service special agents who have received at least one of three levels of computer crimes-related training. These agents are deployed in more than 98 Secret Service offices throughout the world and have received extensive training in forensic identification, preservation and retrieval of electronically-stored evidence. ECSAP agents are computer investigative specialists and among the most highly-trained experts in law enforcement, qualified to conduct examinations on all types of electronic evidence. This core cadre of special agents is equipped to investigate the continually evolving arena of electronic crimes and have proven invaluable in the successful prosecution of criminal groups involved in computer fraud, bank fraud, identity theft, access device fraud, and various other electronic crimes targeting our financial institutions and private sector.

The ECSAP program is divided into three levels of training and focus:

Level I – Basic Investigation of Computers and Electronic Crimes (BICEP) The BICEP training program focuses on the investigation of electronic crimes and provides a brief overview of several aspects involved with electronic crimes investigations. This program is designed to provide Secret Service agents and our state and local law enforcement partners with a basic understanding of computers and electronic crime investigations. The BICEP program has

proven so effective that the Secret Service has incorporated it into its core curriculum for newly hired special agents.

Level II – Network Intrusion Responder (ECSAP-NI) ECSAP-NI training provides special agents with specialized training and equipment that allows them to respond to and investigate network intrusions. These may include intrusions into financial sector computer systems, corporate storage servers, or various other targeted platforms. The Level II trained agent will be able to identify critical artifacts that will allow effective investigation of identity theft, malicious hacking, unauthorized access, and various other related electronic crimes.

Level III – Computer Forensics (ECSAP-CF) ECSAP-CF training provides special agents with specialized training and equipment that allows them to investigate and forensically obtain legally admissible digital evidence. The forensically obtained digital evidence is utilized in the prosecution of various electronic crimes cases, as well as criminally focused protective intelligence cases.

Electronic Crimes Task Forces (ECTF)

In 1996, the Secret Service established the New York Electronic Crimes Task Force (ECTF) to combine the resources of academia, the private sector, and local, state, and federal law enforcement agencies to combat computer-based threats to our financial payment systems and critical infrastructures. Congress has since directed the Secret Service in Public Law 107-56 to establish a nationwide network of ECTFs to "prevent, detect, and investigate various forms of electronic crimes, including potential terrorist attacks against critical infrastructure and financial payment systems."

The Secret Service has established 29 ECTFs, including the first international ECTF based in Rome, Italy. Membership in our ECTFs include: over 299 academic partners; over 2,100 international, federal, state, and local law enforcement partners; and over 3,100 private sector partners. The Secret Service ECTF model is unique in that it is an international network with the capabilities to focus on regional issues. For example, the New York ECTF, based in the nation's largest banking center, focuses heavily on protecting our financial institutions and infrastructure. By joining our ECTFs, all of our partners enjoy the resources, information, expertise, and advanced research provided by our international network of members while focusing on issues with significant regional impact.

Cyber Intelligence Section (CIS)

Our Cyber Intelligence Section (CIS) collects, analyzes, and disseminates data in support of Secret Service investigations worldwide and generates new investigative leads based upon its findings. CIS leverages technology and information obtained through private partnerships to monitor developing technologies and trends in the financial payments industry for information that may be used to enhance the Secret Service's capabilities to prevent and mitigate attacks against the financial and critical infrastructures.

CIS has developed an operational unit that investigates international cyber-criminals involved in cyber-intrusions, identity theft, credit card fraud, bank fraud, and other computer-related crimes.

The information and coordination provided by CIS is a crucial element to successfully investigating, prosecuting, and dismantling international criminal organizations.

National Computer Forensics Institute (NCFI)

The National Computer Forensics Institute (NCFI) initiative is the result of a partnership between the Secret Service, the Department of Homeland Security (DHS), the State of Alabama, and the Alabama District Attorney's Association. The goal of this facility is to provide a national standard of training for a variety of electronic crimes investigations. The program offers state and local law enforcement officers, prosecutors, and judges the training necessary to conduct computer forensics examinations. Investigators are trained to respond to network intrusion incidents and conduct basic electronic crimes investigations.

Since opening on May 19, 2008, the Secret Service has provided critical training to 836 state and local law enforcement officials representing over 300 agencies from all 50 states and two U.S. territories.

Collaboration of International Partners

One of the main obstacles that agents investigating transnational crimes encounter is the jurisdictional limitations. The Secret Service believes that to fundamentally address this issue, appropriate levels of liaison and partnerships must be established with our foreign law enforcement counterparts. Currently, the Secret Service operates 22 offices abroad, each having regional responsibilities to provide global coverage. The personal relationships that have been established in those countries are often the crucial element to the successful investigation and prosecution of suspects abroad.

Computer Emergency Response Team (CERT)

In August 2000, the Secret Service and Carnegie Mellon University Software Engineering Institute (SEI) established the Secret Service CERT Liaison Program (CLP). The role of the CLP is threefold: (1) technical support; (2) research and development; and (3) public outreach and education.

The CLP is a collaborative effort with over 150 scientists and researchers engaged in the fields of computer and network security, malware analysis, forensic development, training and education. Supplementing this effort is research into emerging technologies being employed by cyber-criminals and development of technologies and techniques to combat them.

The objectives of the CLP are: to broaden the Secret Service's knowledge of software engineering and networked systems security; to expand and strengthen Secret Service partnerships and relationships with the technical and academic communities; to provide an opportunity for the Secret Service to work closely with CERT, SEI, and Carnegie Mellon University; and to provide public outreach and education.

Conclusion

Today, hundreds of companies specialize in data mining, data warehousing, and information brokerage. The movement toward increasing use of cloud-computing technologies will mean that even more information and personally identifiable data will be stored in cyber space. This wealth of available personal information creates a target-rich environment for today's sophisticated cyber criminals. However, with proper network security, businesses can provide a first line of defense by safeguarding the information they collect. Such efforts can significantly limit the opportunities for these criminal organizations. Furthermore, the prompt reporting of major data breaches involving sensitive personally identifiable information to the proper authorities will help ensure a thorough investigation is conducted. The Secret Service and Department of Homeland Security continue to collaborate closely with the private sector to improve coordination and communication on cyber issues.

As I have highlighted here, the Secret Service has implemented a number of initiatives on cyber and computer-related crimes. Responding to the growth in these types of crimes and the level of sophistication these criminals employ demands an increasing amount of resources and greater collaboration with law enforcement and its public and private partners. Accordingly, we dedicate significant resources to increasing awareness, educating the public, providing training for law enforcement partners, and improving investigative techniques. The Secret Service is committed to our mission of safeguarding the nation's critical infrastructure and financial payment systems. We will continue to aggressively investigate cyber and computer-related crime to protect consumers.

In conclusion, I would like to reiterate that cyber-crime remains an evolving threat. It is not a threat of the future; it is very much here. Law enforcement agencies must be able to adapt to emerging technologies and criminal methods. The Secret Service is fully involved in the federal government's new approach to cybersecurity. We are dedicated to the government's collective effort to be innovative in our approach to cyber-crime and cybersecurity and to stay ahead of this ever-changing threat. The Secret Service is pleased that the Committee recognizes the magnitude of these issues and the constantly evolving nature of these crimes. To effectively fight these crimes, our criminal statutes must be amended to safeguard sensitive personally identifiable information and to afford law enforcement the appropriate resources to investigate data breaches.

Chairman Scott, Ranking Member Gohmert, and distinguished members of the Subcommittee, this concludes my prepared statement. Thank you again for this opportunity to testify on behalf of the Secret Service. I will be pleased to answer any questions at this time.

Mr. SCOTT. Thank you, Mr. Merritt.

Mr. Sullivan, I believe you came off a vacation to be with us today. We certainly appreciate that. We certainly notice that, and thank you for being with us.

Mr. Sullivan?

TESTIMONY OF JOE SULLIVAN, CHIEF SECURITY OFFICER (CSO), FACEBOOK, INC., PALO ALTO, CA

Mr. SULLIVAN. Certainly. It is my pleasure to be here. So thank you, Chairman Scott, Ranking Member Gohmert and Subcommittee Members for this opportunity.

As Facebook's chief security officer, and as a former Federal prosecutor who specialized in high-tech crime in Silicon Valley, this topic has special meaning for me. At Facebook, I work every day on developing high product security standards, engaging people outside the company, such as educators, parents, students and other Internet users, to learn about and promote safe Internet practices. And I also work closely with law enforcement around the world to help ensure that those who are responsible for online abuse are held accountable.

While the Internet now connects nearly two billion people, until recently, it was a useful but very passive repository of information. But in just a few years, it is really evolved to an interactive social experience defined by your connections, interests, and your communities.

These developments enlist people not just as passive viewers but also as creators of online content, frequently in a framework that is social and involves forums or communities defined by people themselves. And since its creation, Facebook has been at the forefront of this change, growing from a network of students at a handful of universities to a worldwide community.

Today, Facebook and other social technologies have the power to enrich people's lives in ways that were unimagined even 5 years ago. Facebook's become an invaluable communication tool, allowing individuals to connect for myriad purposes, to communicate with family near and far, for charitable causes, in the political realm for grassroots organizing and for local community-building.

In the same way that Facebook has brought innovation to communication, on the security team and across the company, we try and bring innovation to Internet security. We are constantly working to enhance online safety and address new and emerging security threats.

And because those efforts are frequently behind the scenes, I particularly appreciate the opportunity to highlight a few of them for you today. We believe that our proactive efforts and innovations in security are the key to providing a positive online experience.

In my written testimony, I focus on a number of different areas. One of those important areas is key partnerships. As a company, we reach out to law enforcement and Internet privacy, safety and security experts everywhere to learn about best practices and to build on them.

For example, last year we created a Safety Advisory Board consisting of representatives from five of the leading online safety organizations. And we have regular meetings with them and almost daily feedback from them on things that we can do in particular in the area of teen safety.

The Board has been a great resource. One example has been their contributions to the improved safety and security messaging that we have launched in the last few months.

I am also proud of the strong relationships with the law enforcement agencies here at the table today. The FBI has long been a leader in cyber-crime investigation, and we are working closely with the FBI on several large, multi-jurisdictional cases right now against malware distributors and spammers who have attempted to take advantage of the scale of social networking sites. We have also worked with them on child safety cases.

And the Secret Service is resourceful and innovative not only on the Internet threat cases that they prioritize, but also on other types of electronic crime investigations where we have turned to them for assistance.

Following up on the comments of Congressman Goodlatte, before Facebook, I think the common wisdom was that the Internet was a place where people should avoid using their real names or sharing information. Facebook was the first major web service that required people to build their profiles and networks using real names, while at the same time giving them privacy controls so that they can limit who accesses their information.

This was an important policy and technical architecture choice which both allowed people using Facebook to become more connected and made the service safer. In a culture of authentic identity, your actions are observed by your real-world friends, and it makes Facebook less attractive to predators and other bad actors. And to be honest, those people, they stand out like sore thumbs on our site.

We also make it easier for people to control what they want to share, with whom and when. In my written testimony, I give several examples, both in the context of privacy and in security, where we give people controls over who sees what and how they manage the security of their account.

On the back end, we are also very proactive. So, for example, we became a level one PCI-compliant company, meeting heightened data security standards even though, as a business, we don't even meet the standard of those requirements being necessary for our business.

We will also develop proprietary technologies that allow us to continuously improve on our online safety efforts. We generally don't discuss the back-end algorithms and things that we use in that context, but these technologies allow us to perform ongoing authentication checks and also to engage our users in types of community verification.

Our technology has also helped us to obtain and take legal action against people who try to do things that they shouldn't. Congress enacted the CAN-SPAM Act, and I am proud to say that Facebook is responsible for the two largest judgments in the history of that Act, $873 million against Adam Guerbuez and $711 million against the notorious spammer, Sanford Wallace.

I see that my time is up, so I would just like to maybe go on a little bit and mention that, as we come here today, I think that security requires vigilance, and Congress has been vigilant in enacting targeted statutes to address Internet security problems. It is an ongoing chess match, and there is more to be done.

A couple of examples of things where we hope to continue to work closely with the government are building out that national

database of convicted sex offenders that was called for in the KIDS Act that Congress passed a couple years ago. We need access to that national database today. And if we had access to it, we would use it.

We need continued investment in cyber-literacy in particular for teens and parents. An example, to get really in the weeds, is we need broader access to the hashes of known images of exploitation of children. With these hashes, we would be able to run that list against our site and identify any known image of child pornography and make sure that it was not on our service. Facebook is the largest photo-sharing Web site on the Internet, and that type of technology would be very helpful.

We also need, I think law enforcement to receive more resources for training. They need better technology in the office, and they need better training on how to, in particular, work on the international cases.

Unfortunately, the vast majority of the significant cyber-crime that is going on today is cross-jurisdictional, and it brings up new challenges that law enforcement have not had to deal with on a day-in, day-out basis. For example, collection of electronic data can involve service of legal process in multiple countries and numerous jurisdictions across the United States. As a result, these cases move too slowly, and many international cases never get prosecuted at all.

In conclusion, I would just like to say that Facebook has always sought to provide a safer environment than was generally available, and we will continue to innovate in order to enhance the safety and security of our community of users.

And on behalf of Facebook, I thank the Subcommittee for its leadership and dedication to Internet innovation and safety.

[The prepared statement of Mr. Sullivan follows:]

PREPARED STATEMENT OF JOE SULLIVAN

Testimony of Joe Sullivan

Chief Security Officer

Facebook

July 28, 2010

Before the U.S. House of Representatives Committee on the Judiciary,

Subcommittee on Crime, Terrorism, and Homeland Security

Hearing on: Online Privacy, Social Networking, and Crime Victimization

Summary of Key Points

Promoting a Real Name Culture: Facebook's real name culture creates accountability and deters bad behavior since people using Facebook understand that their actions create a record of their behavior.

Empowering People with Privacy and Safety Controls: Facebook' mission is to give people the power to find, connect, and share information with their friends and the people around them, and we make it easy for people to decide what they want to share, with whom, and when.

Deploying Hidden Security Systems and Safety Tools: Facebook has developed and deployed proprietary technologies that allow us to continuously improve online safety and combat emerging online threats. These technologies enable Facebook to perform ongoing authentication checks, including technical and community verification of users' accounts. We also have dedicated teams responsible for investigating specific scams perpetrated against our users, and to use legal means to go after the people behind them.

Addressing Special Needs of Teens Online: We have developed a number of tools and technology innovations designed to enhance the privacy and safety of teenagers on Facebook. We have led efforts around the world to help combat cyberbullying and combat suicide and self harm, and we have built a strong track record in helping to locate missing teens. Finally, while only a tiny fraction of a single percent of users will ever encounter sexual predators or content involving child pornography on Facebook, we focus on safeguards in these areas because we take them very seriously.

Driving Collaborating Among Key Stakeholders in the Online Safety Community: We have built strong relationships with child safety and security experts, and we work closely with government and law enforcement agencies around the country, and around the world.

More Can be Done With the Help of Congress: To combat criminals and miscreants who would use the Internet to engage in scams, identity theft, and fraud:

- We need to move forward with creation of a national database of convicted sex offenders that includes online identifiers and is accessible to industry and the online safety community.

- We need renewed investment in youth and parent Internet education programs.

- We need to give internet companies broader access to hashes of known images of sexual exploitation of children.

- We need more resources to train law enforcement officers on social technologies, and they need better technology to do their job.

- We need better cooperation between law enforcement entities in different jurisdictions. Most interstate cases move too slowly, and most international cases never get prosecuted at all.

From its beginnings, Facebook sought to provide a safer environment than was generally available to people on the web, and as we have expanded beyond college students, we have worked hard to deliver a safer online experience for all of our users. The five hundred million people across the globe who actively use Facebook have driven innovation in ways that few would have predicted a decade ago, and Facebook will continue to innovate in order to enhance the safety and security of our thriving community.

Thank you Chairman Scott, Ranking Member Gohmert, and Subcommittee Members. My name is Joe Sullivan, and I am Facebook's Chief Security Officer. As Facebook's CSO – and also as a former federal prosecutor and a founding member of the first of the Justice Department's Computer Hacking and Intellectual Property Units, a special team created by now F.B.I. Director Robert Mueller and located in the heart of Silicon Valley, - this topic has special resonance for me. At Facebook I work to develop and promote high standards for product security, engage educators, parents, students and other Internet users externally to promote safe Internet practices. I also oversee a team that partners closely with law enforcement to help ensure that those responsible for spam, fraud and other abuse are held accountable. Facebook is constantly innovating to foster a safer online environment and to address new and emerging security threats. We believe these proactive efforts and innovations – some that are visible and others that are not – are a key to providing a positive online experience.

While the Internet now connects nearly 2 billion people around the world,[1] until recently it was a useful but passive repository of information. People visited Web sites, read articles, and gathered information, but had little if any meaningful interaction with one another on the Web. In just a few short years, however, the Internet has evolved from an impersonal, anonymous medium to an interactive social experience defined by a person's connections, interests, and communities. That transformation occurred in tandem with what has been called "Web 2.0," an explosion in innovative functionalities that was unimaginable during the Internet's infancy. These developments provide interactive experiences and allow people to generate and define relevant content. They enlist people as both the viewers *and* creators of online content, frequently in a framework that is social and involves forums or communities defined by the users themselves.

Since its creation in a Harvard dorm room by Mark Zuckerberg in 2004, Facebook has been at the forefront of this change, growing from a network of students at a handful of universities to a worldwide community in over 180 countries. As Facebook expanded, we continually innovated and implemented new tools, responding to the immense public demand for more and better ways to share and connect. Today, Facebook and other social technologies have the power to enrich people's lives—and society as a whole—in ways that were un-imagined five years ago. Facebook has become an invaluable communication tool, allowing individuals and families to connect for myriad purposes—for charitable causes, in the political realm, for grassroots organization, and for local community building.

---

1 *Internet Usage Statistics, The Internet Big Picture*, World Internet Users and Population Stats, http://www.Internetworldstats.com/stats.htm.

From the beginning, Facebook sought to provide a safer environment than was generally available to people on the web, and as we have expanded beyond college students, we have worked hard to deliver a safer online experience for all of our users.[2] We reach out to law enforcement and Internet privacy, safety, and security experts everywhere to learn about best practices and to build on them. For example, in December, we convened a Safety Advisory Board consisting of representatives from five leading online safety organizations (Childnet International, Common Sense Media, ConnectSafely.org, the Family Online Safety Institute, and WiredSafety) to provide independent advice on teen online safety. Both to share our insights and to stay fully informed, Facebook has participated in many online safety initiatives around the world, such as the US State Attorneys General Internet Technical Task Force, the UK Home Office Task Force on Child Safety, the EU Safer Internet initiative, the Australia Attorney General's Online Safety Working Group and others.

No discussion of key stakeholders in ensuring internet safety would be complete without recognizing the excellent work done by law enforcement across America. I'm proud to say that we have forged strong working relationships with the law enforcement agencies here at the table today. The FBI has long been a leader in cybercrime investigations, and is working closely with us on several large multi-jurisdictional cases right now against malware distributors and spammers who have attempted to take advantage of the scale of social networking sites. The FBI is very focused on child safety—with many agents across the country playing leadership roles in ICAC taskforces. And we have found the Secret Service to be very resourceful and innovative not only on the threat cases they prioritize but also on other types of electronic crimes investigations where we have turned to them for assistance.

Today I would like to discuss some of the important ways that Facebook innovation helps promote a safer online environment.

Summary of Key Points

I will discuss five areas in which our innovations are helping to make our site safer and deliver the best experience to the people who use Facebook:

1. **Promoting a Real Name Culture;**
2. **Empowering People with Privacy and Safety Controls;**

[2] Facebook is not directed at children less than 13 years of age residing in the United States and does not knowingly collect information from any children under 13 in the United States.

3. **Deploying Hidden Security Systems and Safety Tools;**
4. **Addressing Special Needs of Teens Online;**
5. **Driving Collaboration Among Key Stakeholders in the Online Safety Community.**

Promoting a Real Name Culture

Before Facebook, the common wisdom was that Internet users should avoid using their real names or sharing information online. Facebook was the first major web service that required people to build their profiles and networks using real names while, at the same time, giving them privacy tools to control who could access that information. This was an important policy and technical architecture choice, which both allowed people using Facebook to become more connected and made the site safer.

A culture of authentic identity has made Facebook less attractive to predators and other bad actors who generally do not like to use their real names or email addresses. At the same time, Facebook's real name culture attracts users who are more likely to adhere to community rules, as set forth in our Statement of Rights and Responsibilities, than users of other online services. [3] People are less likely to engage in negative, dangerous, or criminal behavior online when their friends can see their name, their speech and the information they share. Our real name culture creates accountability and deters bad behavior since people using Facebook understand that their actions create a record of their behavior. When someone's actions violate our SRR or the law, we can assign corrective action – which in serious and/or potentially criminal matters usually involves account termination and/or referral to law enforcement – to the specific account involved. Similarly, Facebook is often able to detect fake user accounts because of the types of connections made by them, and we routinely block the registration of accounts under common fake names.

Our real name culture also empowers users to become "community policemen," and to report those whose behavior violates Facebook's SRR. People who use Facebook expect authentic identities and interactions, and when they encounter something different, they are quick to notice and report that behavior. They also regularly use our report links, found on nearly every page throughout the service. This substantially multiplies the number of people reviewing content and behavior on Facebook and greatly enhances safety on the service. Our robust reporting infrastructure leverages Facebook's 500

[3] Facebook's community rules are set out in our Statement of Rights and Responsibilities ("SRR"), *available at:* http://www.facebook.com/terms.php?ref=pf

million users to monitor and report offensive or potentially dangerous content. This infrastructure includes systems to prioritize the most serious reports and a trained team of reviewers who respond to reports and escalate them to law enforcement as needed.

We recently adopted a policy, modeled on the Fair and Accurate Credit Transactions Act, to enable persons whose accounts have been compromised to access information about fraudulent activity associated with accounts opened using their identification. This makes it easier for our members to protect their identities and their reputations. When it comes to finding new ways to safeguard the people who use Facebook, we constantly strive to be ahead of the curve. Indeed, the techniques we use to safeguard people as they engage in ever-increasing numbers of financial transactions to obtain digital goods through Facebook lead the industry. We became a Level One Payment Card Industry (PCI) compliant company well before required to do so by the PCI rules. We have a team of fraud investigators on staff monitoring transactions for anomalies – for example, a purchase made from one location with a credit card from another. Now, we are forging ahead with making sure that people feel secure in doing business with our virtual currency – Facebook Credits.

Empowering People with Privacy and Safety Controls

Facebook's mission is to give people the power to find, connect, and share information with their friends and the people around them. We have learned that the more *control* people have over their information, the more comfortable they will feel about using this service. For this reason, we make it easy for people to decide what they want to share, with whom, and when. People using Facebook must accept a request from another user to be connected - Facebook never makes that choice for them. If someone feels uncomfortable connecting with a particular person, he or she may decline or ignore the friend request. Further, if someone begins to feel that a friend on Facebook is annoying, spamming, harassing, and/or troubling, she may de-friend that person at any time, which terminates the connection between the users.[4] A user may also "block" another user in order to shut off profile access and prevent any further contact. And, anyone may at any time use our ubiquitous report button to draw Facebook's attention to inappropriate behavior.

Knowledge and awareness are both key to giving people meaningful control, and we work extremely hard to make sure that Facebook users are aware of and understand the controls we provide.

---

[4] It should be noted that the de-friending and blocking occur without notification, so the connection is simply, elegantly, electronically severed without drawing attention to the ending of the connection. We also encourage people on Facebook to report activity that they feel may be dangerous.

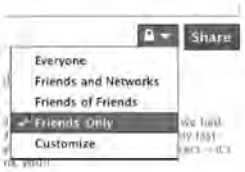
Two examples include our notice and comment process for governance of the Facebook site, and our December 2009 privacy transition tool.

Notice and Comment Process. In February 2009, we introduced an unprecedented level of user control that notifies users about proposed changes to Facebook's Statement of Rights and Responsibilities and our privacy policy – and enables them to review and comment on these changes - *before* they take effect. This process also calls for a user vote on proposed changes that trigger substantial feedback. We are aware of no other Internet-based company, large or small, that goes to such lengths to publicize and incorporate user feedback into those key documents.

Privacy Transition Tool. Last December, when we rolled out a new privacy framework, we took the equally unprecedented step of requiring all users to navigate through a privacy transition tool to confirm or change their sharing settings. As a result, hundreds of millions of people took time to meaningfully engage with the concept of privacy and consider whether their settings reflected their preferences. No other company – on or off the Internet – has gone to such lengths to ensure that users were aware of and had a meaningful opportunity to affect their privacy choices.

As indicated above, whenever we add new features to our service we also provide additional controls so people can determine what they want to share, with whom, and when. To address increasing complexity – both with respect to the Facebook service and with respect to the privacy tools and features - last year we embarked on an effort to simplify our controls while giving people enhanced and real-time control over how they share content on Facebook. In this process we implemented several new controls, including a contextual privacy control and a one-click sharing control.

Contextual Privacy Control. We recognize that a user might want to share some information more openly (such as a comment about a world event) and other information to a narrower audience (such as a photo of their child). Our contextual privacy control allows users to control – easily, and at the time they share information - who is able to see each and every one of their posts. To exercise this control, all a user has to do is click on the "lock" icon before he or she shares the information and selects the intended audience:



We designed the tool to include a warning to make sure users are aware of what it means to share their information with "Everyone." The first time they decide to share content using that setting they see the following:

One-Click Sharing Control. To address increasing complexity, we deployed a simplified control for sharing that lets people manage over twenty categories of information with just one click. This one-click console provides more granular control to those users who prefer to customize the information they share on Facebook. This setting not only makes it easy for people to restrict the information they share in the future, it permits them to adjust the visibility of information they have shared in the past.[5]

We recently launched two additional innovative tools for helping users stay in control of their accounts. The first allows people to create a list of approved devices for Facebook logins and then to be notified immediately by both email and text message any time their account is accessed from a device not on that list. The second applies to all Facebook users. When we detect something unusual about a login attempt, we require the person logging in to verify his or her identity as the account owner before granting access. For example, if an account is typically accessed from Palo Alto, CA, and a login is attempted from Siberia, the person logging in will have to authenticate him or herself either by entering a code sent via text message or by completing a series of questions that only the account owner should be able to answer.

[5] We do not, however, make previously shared information more visible, even when someone adjusts their settings.

Developer Responsibility

We introduced Facebook Platform in 2007 to enable developers to offer innovative social experiences to people using Facebook. Since then it has given become one of the leading platforms for innovation and investment by the more than one million developers developing Facebook applications today. As Platform has evolved, we have developed more sophisticated, easier to use tools to enable people to control access to their personal information, and sharing of this information, by third-party developers: In June, we became the first platform provider to require developers to obtain "granular" data permissions before being able to access a user's information. Facebook Platform developers must tell users which specific categories of information they need to provide their application, and must obtain permission for each data category before the information can be accessed. Further, when an application provider wishes to offer users a new service, we require that the application (i) provide clear notice about any additional data it would need and (ii) obtain the user's consent. This innovative permissions model gives people more control than they have on other leading application platforms, while allowing developers to continue the vibrant innovation that has marked the Platform economy.

Deploying Hidden Security Systems and Safety Tools

Facebook's safety innovations extend to the development and use of proprietary technologies that allow us to continuously improve online safety and combat emerging online threats. Although we do not generally discuss these publicly in order to limit attempts to compromise or circumvent the safeguards, these technologies allow Facebook to perform ongoing authentication checks, including technical and community verification of users' accounts. We look for anomalous behavior in the aggregate data produced by the Facebook community and employ automated systems to block it, warn the user, and in some cases, disable the account. For example, if an adult sends an unusual number of friend requests to minors that are ignored or rejected, our systems could be triggered, sending up a red flag and initiating a Facebook inquiry and, where appropriate, remedial actions.

In addition to our technical systems and educational efforts, we have dedicated teams responsible for investigating specific scams perpetrated against our users, and to use legal means to go after the people behind them. These teams have leveraged the CAN-SPAM Act to win the two largest U.S. spam judgments in history: $873 million against Adam Guerbuez, a Montreal-based spammer, in November 2008, and $711 million against the notorious spammer Sanford Wallace in October 2009. Wallace was also referred to the US Attorney's office for criminal prosecution, which means that in addition to the judgment, he now faces possible jail time, a rare occurrence in this type of case. In fact, in

every case where we have taken legal action against a spammer, the abuse has stopped. Our aggressive approach has had a noticeable deterrent effect on would-be spammers as well, as evidenced by discussion in various online criminal forums we monitor.

Addressing Special Needs of Teens Online

As stated earlier, Facebook is neither directed at children younger than 13 years of age, nor does Facebook knowingly collect information of those under 13. While today there is no tool available to online site operators that can reliably verify the age of a user, we work hard to prevent children under 13 from establishing an account in the first place. We require those entering Facebook.com to type in their age on the very first screen, and when someone enters a birth date that that establishes his or her age to be under 13, our age gate technology blocks the registration and places a persistent cookie on the device used to establish the account, preventing subsequent attempts to circumvent the screen by modifying his or her birth date. Although this age gate deters children, we understand that it does not always prevent their registration. Providing inaccurate birth date information is a violation of our SRR, however, and we ask people to notify us if they believe we might have information from a child under 13. We created a dedicated channel for people to report accounts belonging to children under 13, and we remove these accounts when we learn of them.

While research has shown that the risks minors face online are "in most cases not significantly different than those they face offline,"[6] Facebook has developed a number of tools and technology innovations designed to enhance the privacy and safety of our teenage users, some of which provide safeguards that may not be available in the offline environment.

In addition to our COPPA-compliant age screening process designed to prevent registration by children under 13, Facebook restricts contact between adults and minors in a manner that is designed to reduce opportunities for adults to pose as minors. For example, when a minor who is new to our service sends a friend request, we might interpose a message along the lines of "Is this someone you know from

[6] *See, Enhancing Child Safety and Online Technologies: Final Report of the Internet Safety Technical Task Force to the Multi-State Working Group on Social Networking of State Attorneys General of the United States,* The Berkman Center for Law & Society at Harvard University, 2008 at 4 ("The Task Force asked a Research Advisory Board comprising leading researchers in the field to conduct a comprehensive review of relevant work in the United States to date. The Literature Review shows that the risks minors face online are complex and multifaceted and are in most cases not significantly different than those they face offline, and that as they get older, minors themselves contribute to some of the problems.")
http://cyber.law.harvard.edu/sites/cyber.law.harvard.edu/files/ISTTF_Final_Report.pdf

your school?" or "Is this someone whom you or your parents know from your community?" We also limit the number of friend requests that anyone can send in a set period of time to further reduce unwanted contact between unrelated users. While those over 18 on Facebook can share information with everyone if they choose, Facebook automatically limits the sharing of users under 18 to a much smaller subset of users, such as the minor's friends, friends of those friends, and their verified networks, generally associated with their schools. This limitation substantially reduces the visibility of minors to non-minors that they do not know.

Similarly, Facebook has led efforts around the world to help combat cyberbullying. In the US, Facebook was a founding member of the StopCyberbullying Coalition. We regularly partner with organizations like MTV and the National Crime Prevention Council to educate our users about this important issue, and have created and distributed lists of safety tips on how to combat and report cyberbullying if it occurs on Facebook. We have also taken steps to combat suicide and self harm by encouraging users to report postings related to self-harm. We review reported postings, removing inappropriate content and alerting organizations like the National Suicide Prevention Lifeline where appropriate.

We are particularly proud of our track record in helping to locate missing teens. Law enforcement has generously praised Facebook for expediting requests for Internet Protocol ("IP") location information accompanied by appropriate legal process where it might help locate a missing child. (See attached letter from Detective Victor A. Kenuedy, of the Moutgomery County, Maryland Police Departmeut.) For example, in just one week last February, we helped authorities in Fairfax, Virgiuia and Menlo Park, California locate two missing teens. Last July, we received a request for IP data and basic user information for a minor who had gone missing. We worked closely with law enforcement over email and by telephone, and ultimately, the minor was found using the exact IP data we had provided. Similarly, a Facebook user went missing in Canada, and a demand for ransom was made. The Royal Canadian Mounted Police contacted us and we followed our procedure for immineut threats. As soon as a message was seut from the missing persou's accouut, we were able to provide data that euabled the RCMP to locate and return the person to safety. We also just recently launched a new Amber Alert program in Canada, and we are in discussions with the U.S. Department of Justice and National Center for Missing and Exploited Children to do so throughout the U.S. as well. The Amber Alert program enables law enforcement officials too easily and without cost broadcast an urgent message to the members of the community most able to help.

Finally, while only a tiny fraction of a single percent of users will ever encounter sexual predators or content involving child pornography on Facebook,[7] we focus on safeguards in these areas because we take them very seriously. For example, we prohibit access to Facebook by Registered Sex Offenders (RSOs) and employed an outside contractor to collect a list of RSOs from all of the states periodically. We regularly compare our compilation of RSO names to our user list; we do not wait for law enforcement to request that we do so. Our internal team of investigation professionals evaluates any potential matches more fully. If we find that someone on a sex offender registry is a likely match to someone on Facebook, we notify law enforcement and disable the account (unless law enforcement has asked us to leave an account active so that they may investigate the user further). We have also worked proactively to establish a publicly available national database of registered sex offenders that enables real-time checks and includes important information like email addresses and IM handles. We've drafted model legislation for states, and partnered with a number of state attorneys general to receive and compare against our site the Internet identifiers that they collect from the released sex offenders they supervise.

Facebook takes substantial steps to stop any trafficking in child sexual exploitation materials, commonly referred to as child pornography. We use automated tools to prohibit the sharing of known links to these materials, and we have a highly trained team dedicated to responding on those rare occasions when child pornography is detected on our site. That team sends incident reports to the National Center for Missing and Exploited Children (NCMEC) and the U.S. Department of Justice for potential prosecution.

Driving Collaborating Among Key Stakeholders in the Online Safety Community

Recognizing the importance of collaborating with others to innovate in this area, In December, Facebook formalized our longstanding relationships with child safety and security experts by creating a global Safety Advisory Board of outside experts who advise us, and, on occasion, our community about how to keep teens safe online. We also regularly consult with other experts in the field. Facebook also continues to work closely with law enforcement agencies around the country, and around the world. We are particularly proud of our work with the state attorneys general. In 2008, Facebook actively participated in the Internet Safety Technical Task Force at the behest of the attorneys general to examine

[7] *See, Enhancing Child Safety and Online Technologies: Final Report of the Internet Safety Technical Task Force to the Multi-State Working Group on Social Networking of State Attorneys General of the United States,* The Berkman Center for Law & Society at Harvard University, 2008 ("Social network sites are not the most common space for solicitation and unwanted exposure to problematic content, but are frequently used in peer-to-peer harassment, most likely because they are broadly adopted by minors and are used primarily to reinforce pre-existing social relations.")

these issues. In May, we announced another new partnership – with the National PTA (Parent Teacher Association), which is designed to get important educational materials to teachers, parents, and students.

In April, we launched our new Safety Center to provide teens, parents, educators, and members of the law enforcement community with updated educational materials and information about how to utilize our innovative privacy and security tools to enhance online safety. Just yesterday, we launched our Facebook Safety Page (facebook.com/FBsafety), which complements our industry-leading efforts to keep users safe on our service and elsewhere on the Web. We hope people will "like" this page to receive automatic updates in their News Feed on a range of relevant information, including new initiatives by Facebook to keep users safe, valuable educational materials from Internet safety experts, relevant news coverage and links to other online resources with important safety tips. Earlier this week, we launched a Safety Page that will complement our Safety Center to provide dynamic content to every user who "Likes" the page. Next month, for the second year in a row, I am going to be a keynote speaker at the biggest annual child safety conference, in Dallas, where we will train law enforcement and other child safety officials from around the world on best practices in doing online investigations.

MORE CAN BE DONE WITH THE HELP OF CONGRESS

Of course, Facebook cannot protect online users on its own. The involvement of the federal government is also needed, for example, to guard against criminals and miscreants who would use the Internet to engage in scams, identity theft, and fraud. That is why we applaud Congress for enacting targeted statutes to address these problems without cabining the creative freedom that is the life force of the Internet. The Computer Fraud and Abuse Act, the Child Online Privacy Protection Act, and the Controlling the Assault of Non-Solicited Pornography and Marketing Act (the "CAN-SPAM" Act) all have served to protect the public from some of the Internet's dangers and annoyances. But there is more to be done. For example:

- We need to move forward with creation of a national database of convicted sex offenders that includes online identifiers and is accessible to industry and the online safety community. . We actively supported passage of the KIDS Act, which will called for creation of just such a database, and were glad to see it signed into law (in 2008). But the Act needs to be implemented now - not some indeterminate date in the future.

- We need renewed investment in youth and parent Internet education programs. We've worked closely with private organizations on a variety of safety and security curricula, but a program taught at schools around the country and aimed at teaching kids the rules of the road would drastically reduce the number of bad incidents. Digital literacy needs to improve most

dramatically among those who have the most impact—parents and teachers- and those who are exposed to the greatest risks – students.

- We need to give internet companies broader access to hashes of known child pornography images. We report instances of child pornography to the National Center for Missing and Exploited Children whenever we find them or users bring them to our attention. With better technology, however, we could block these images upfront and identify those responsible so we can preserve information and notify law enforcement as quickly as possible. NCMEC has given us a small list, but law enforcement has access to lists that are orders of magnitude larger in volume.

- We need more resources to train law enforcement officers on social technologies, and they need better technology to do their job.

- We need better cooperation between law enforcement entities in different jurisdictions. Most interstate cases move too slowly, and most international cases never get prosecuted at all.

- Finally, Congress can assist Facebook and similar companies in advancing online safety by providing incentives for innovation and by ensuring that regulators do embrace technological and policy innovation in this area.

CONCLUSION: FACEBOOK WILL CONTINUE TO INNOVATE BUT CONGRESS MUST HELP

The five hundred million people across the globe who actively use Facebook have driven innovation in ways that few would have predicted a decade ago. The promise of this thriving community is limitless. From its beginnings, Facebook sought to provide a safer environment than was generally available to people on the web, and we will continue to innovate in order to enhance the safety and security of our thriving community.

We thank this Subcommittee for its leadership and dedication to internet innovation and safety. Thank you for your consideration.

Mr. SCOTT. Thank you very much.
Mr. Rotenberg?

TESTIMONY OF MARC ROTENBERG, EXECUTIVE DIRECTOR, ELECTRONIC PRIVACY INFORMATION CENTER (EPIC), WASHINGTON, DC

Mr. ROTENBERG. Thank you, Chairman Scott, Ranking Member Gohmert, Members of the Subcommittee. I appreciate the opportunity to be here this afternoon.

My name is Mark Rotenberg. I am the executive director of EPIC, and we are a leading privacy organization. We are particularly concerned about the privacy issues related to Facebook.

As you know, Facebook has become enormously influential on the Internet. It has more than 500 million members. Someone pointed out recently that, if it were a country, it would be larger than the United States, Japan, and Germany combined. So it is a very big player on the Internet.

At the same time, Facebook also has an enormous impact by what it chooses to do or not do on the privacy of Internet users. And when Facebook has changed its privacy policies and the privacy settings of Internet users, it is raised real privacy concerns.

In fact, my organization, EPIC, has filed two complaints at the Federal Trade Commission resulting from these changes in privacy settings because we believe they significantly disadvantaged Internet users and created new risks to privacy.

Now, to be clear, the service is very useful. In fact, in preparing for this hearing, I actually posted on my own Facebook wall a question to Facebook users. I said, "What concerns do you have that I should share with Committee Members?"

And many people responded, some who I know well, some who I don't know particularly well, but the comments were helpful. And I incorporated them in my prepared statement for you today to give you some sense of the concerns that Facebook users have.

And this point about changing the privacy settings came back again and again and again. And I bring this to your attention today, because I know in this discussion about the risk of online victimization, which is a real threat, oftentimes people talk about the need to better educate users, to warn users about what they should or should not post.

And while I agree in some circumstances that is helpful, user education can only go so far if a user has made a determination not to disclose certain types of information to certain organizations and the company in possession of that information chooses to change the rules of the game.

User might say, for example, "I don't want this information to be widely available or searchable through an Internet search engine. I only want these photos to be available to my friends or family members," and then the company says, "Well, we have a transition now in the privacy settings, and we are going to change those defaults a bit. And if you want to change them back, you are always free to do so."

The point that I am trying to make is that these changes in the privacy settings create risks for users that they really cannot control. This is the reason that we went to the Federal Trade Commission and urged the FTC to enforce the agreement that users had with Facebook and other Internet firms to respect their privacy settings.

Now, I am bringing attention to this FTC complaint because I think it has some specific implications for what this Committee might be able to do to address user concerns about online privacy in the social network space.

Because the FTC has not acted on this complaint, it means that the companies are able to continue to make these changes, and that there is no recourse for users. And what I am proposing, therefore, is that the Federal law that regulates the disclosure of information by companies such as Facebook, the Electronic Communications Privacy Act, be amended so that these disclosures to third parties could not occur without clear and affirmative consent.

In other words, if a person has chosen not to disclose personal information to an application developer that is a business partner, a Facebook or an Internet Web site that is also a business partner of Facebook, that preference should be respected. And if it is not respected, then I think it is creating a significant risk to the privacy of users online.

Looking ahead, this is going to continue to be an important concern for Internet users until we have comprehensive legislation protecting people online.

Thank you very much for the opportunity to testify. I would be pleased to answer your questions.

[The prepared statement of Mr. Rotenberg follows:]

PREPARED STATEMENT OF MARC ROTENBERG

epic.org

ELECTRONIC PRIVACY INFORMATION CENTER

Testimony and Statement for the Record of

Marc Rotenberg
President, EPIC
Adjunct Professor, Georgetown University Law Center

Hearing on

"Online Privacy, Social Networking, and Crime Victimization"

Before the

Committee on the Judiciary
Subcommittee on Crime, Terrorism, and Homeland Security
U.S. House of Representatives

July 28, 2010
2141 Rayburn House Office Building
Washington, DC

Mr. Chairman and Members of the Committee, thank you for the opportunity to testify today. My name is Marc Rotenberg, and I am the President of the Electronic Privacy Information Center. EPIC was established to focus public attention on emerging privacy and civil liberties issue. I also teach Information Privacy Law at Georgetown University Law Center. I want to thank you for holding this hearing today and also thank Chairman Conyers for his May letter to Facebook.

EPIC has a particular interest in privacy and social networking services. We filed two complaints at the Federal Trade Commission in the last year following decisions by Facebook to change its privacy policies and the privacy settings of its users. We also filed a complaint when Google introduced Buzz, its social network service, because the company essentially opted in all of its Gmail users. We believe it is vitally important to protect the privacy of users of these services, and many users agree.

To be clear, we do not object to social network services—they are enormously valuable—but we do believe that there are serious privacy risks to users resulting from the actions of Facebook that should be pursued. In some instances, we believe that laws were violated and investigations should go forward. In other areas, it may be necessary to enact new laws.

In my testimony today, I will discuss the growing importance of Facebook, the privacy risks to users, and the problems with the current approach to privacy protection. I will also point out that these concerns are widely shared among Facebook users and have been well documented by news reports, user campaigns, and survey data.

Because of the failure of the Federal Trade Commission to take meaningful action to address these problems, I will recommend that the Committee expand statutory privacy safeguards until Title 18 and specifically revise section 2701 of the Electronic Communications Privacy Act ("ECPA") to limit the ability of companies such as Facebook to disclosure user data to third parties, such as application developers and web sites without meaningful opt-in consent.

This change in law will not prevent Facebook from disclosing personal information about its users to third parties. It will simply make the company more transparent and more accountable, and it will give users greater control over the collection and use of their data.

Value of Facebook

Mr. Chairman, there is no question that Facebook is an enormously popular and successful social network service. The numbers are well known—more than

500 million users.[1] If Facebook were a country, it would be larger than the United States, Germany, and Japan combined. Also astonishing is the continued growth of the company, particularly outside of the United States. It is not unreasonable to anticipate that Facebook will, in a few years, have more than a billion members.[2]

Facebook is quickly replacing email as a primary communications tool, particularly when many people are involved. In fact, in preparing for this hearing, I posted a note on my own Facebook page and asked friends to provide ideas for this statement.[3] Many people responded – some I knew well, some hardly at all. But almost all of the suggestions were interesting and helpful. The Public Policy Director of Facebook even joined the discussion. So, there was an opportunity to those who were sending ideas to me to also share their views directly with Facebook.

In similar fashion, all across the social network service, people are organizing, gathering information, sharing ideas, and building communities. There were ways to do this before Facebook, but none as effective or as simple. Much like the telephone service, the use is as broad as the interests and needs of the users.

Of course, recognizing that Facebook is enormously successful does not answer the question of whether Congress has a role to play in protecting the public interest. We are dependent today on many popular technologies, including the telephone and email, where public law and Congressional oversight have helped encourage innovation and competition while safeguarding consumers.

Also, popularity in this context is somewhat double-edged. Although the company has many users, many are also not happy; thousands have joined groups on the service decrying its privacy policies.[4] Privacy continues to be the top concern of users and many polls give Facebook low ratings for customer satisfaction and trust.[5]

---

[1] Mark Zuckerberg, *500 Million Stories*, THE FACEBOOK BLOG, July 21, 2010, http://blog.facebook.com/blog.php?post=409753352130.

[2] *See, e.g.*, Mark Sweeney, *Mark Zuckerberg: Facebook "almost guaranteed" to Reach 1 Billion Users*, THE GUARDIAN (UK), Jun. 23, 2010, *available at* http://www.guardian.co.uk/media/2010/jun/23/mark-zuckerberg-facebook-cannes-lions.

[3] "Facehook| *Marc Rotenberg* I am testifying this week in Congress on Privacy and Facehook (or as the hearing notice says 'Online Privacy, Social Networking, and Crime Victimization.') Your thoughts? Have the changes in FB's privacy settings created serious problems for users? Examples? Thanks for your thoughts on this." *Available at* http://www.facebook.com/marc.rotenberg?v=wall&story_fbid=126089890769520&ref=mf.

[4] *See, e.g.*, Facebook, People Against the new Terms of Service (TOS), administrated by Julius Harper Jr, and Anne Kathrine Yojana Petterøe, http://www.facebook.com/group.php?gid=77069107432; Facebook, Millions Against Facebook's Privacy Policies and Layout Redesigns, administrated by Miki Perrotta and Jessica Fishbein, http://www.facehook.com/group.php?gid=27233634858; Facebook, Bring back News Feed and Wall privacy settings, administrated by Maggie Ds, http://www.facebook.com/group.php?v=wall&gid=204943119385.

[5] *See, e.g.*, ForeSee Results, *Facebook Flops in ACSI E-Business Report, available at* http://www.foreseeresults.com/news-events/press-releases/facebook-flops-in-acsi-ebusiness-

Approach to Privacy

Much of the privacy discussion with Facebook typically focuses on what users should or should not post online.[6] But in my opinion, this is a mistake. First of all most users have a good understanding about what not to post. I have never seen anyone put a credit card number or an SSN on his or her wall. People may post embarrassing photos or sharp comments, but this problem is overrated. Most Facebook users put those actions in context and don't give them much concern. And Facebook users quickly learn that they can take down photos and update profiles. Online identity is dynamic and the user experience reflects that.

But there is a problem with Facebook users who try to share information selectively—vacation photos with close friends, organizing information for an upcoming event.[7] Facebook has an elaborate system of privacy setting that the company says allows users to decide how much information to reveal to others.[8] For example: You would generally limit your "wall posts" to friends. You might share photos with certain friends. You would probably only give to third party applications, such as Farmville, the information about you that was actually necessary for the application.

In theory, this is could be a good approach. In practice, Facebook's privacy settings have not worked. They are too confusing, too elaborate, too inconsistent, and too difficult for users to make real decisions. Most Facebook users have no idea

---

report.shtml (last visited July 23, 2010); PEW INTERNET AND AMERICAN LIFE PROJECT, REPUTATION MANAGEMENT AND SOCIAL MEDIA (May 2010).

[6] *See* Alex Pham, *Internet Security 101: What not to post on Facebook*, Los Angeles Times, May 3, 2010, http://latimesblogs.latimes.com/technology/2010/05/internet-security-what-not-to-post-on-facebook.html; Donna Tapellini, *Consumer Reports Survey: Social Network Uses Post Risky Information*, CONSUMERREPORTS.ORG ELECTRONICS BLOG, May 4, 2010 *http://blogs.consumerreports.org/electronics/2010/05/social-networks-facebook-risks-privacy-risky-behavior-consumer-reports-survey-findings-online-threats-state-of-the-net-report.html*; JR Raphael, *Facebook Privacy: Secrets Unveiled*, PC WORLD, May 16, 2010, http://www.pcworld.com/article/196410/facebook_privacy_secrets_unveiled.html.

[7] *See* Kevin Bankston, *Facebook's New Privacy Improvements Are a Positive Step, But There's Still More Work to Be Done*, EFF DEEPLINKS BLOG, May 26, 2010, http://www.eff.org/deeplinks/2010/05/facebooks-new-privacy-improvements-are-positive.

[8] *See* Facebook, Choose Your Privacy Settings: Basic Directory Information, http://www.facebook.com/settings/?tab=privacy&section=basic&h=043586873d43d155919f99dfb3816a66 (last visited July 27, 2010); Facebook Privacy Guide, http://www.facebook.com/privacy/explanation.php (last visited on July 27, 2010); Robert Strohmeyer, *Facebook's Zuckerberg Answers Critics With New Privacy Controls*, PC WORLD, May 26, 2010, http://www.pcworld.com/article/197261/facebooks_zuckerberg_answers_critics_with_new_privacy_controls.html; Mark Zuckerberg, *Making Control Simple*, THE FACEBOOK BLOG, May 26, 2010, http://blog.facebook.com/blog.php?post=391922327130 (last visited July 27, 2010).

who their information goes to or for what purpose.[9] And Facebook always reserves the right to make personal information "publicly available" regardless of what the user chooses.

Several of the people who commented on my Facebook page described the problem. "Mary Mi" said she could no longer limit the availability of her profile information. Another friend pointed out that it was not easy to control comments on photos. [10] John Nagle wrote that it was basically impossible to turn off certain applications, such as Glifts and pointed out that you often have to go through many screens to set or change privacy settings.

I liked a comment from Ralph T. Castle who said that "the lack of documentation as the single biggest problem in the system." In his words:

> Proper documentation would explain the deeper ramifications of privacy settings (e.g. if you click to say that you "like" something you may receive ads for similar products). Users would then be better empowered a) to make privacy settings and b) to leave FB if they don't like it.

And then there were very extensive comments from Joanne Edwards about the complexity of the settings, the "triple-step privacy" assurances, the news feed settings, the openness of the defaults, and photo-tagging. Ms. Edwards is also an administrator for several important Facebook groups, including "Millions Against Facebook's Privacy Policies and Layout Redesigns," "Protest: Restoring The Age Of Privacy To Facebook' group," and "'Bring Back News Feed and Wall Privacy Settings' group)." The titles of these groups makes clear the concerns of users, and the groups have tens of thousands of members.

But perhaps most remarkably, I have listened to Facebook experts discuss the privacy settings who quickly became confused. I even heard Facebook founder Mark Zuckerberg describe the new changes to his company's privacy settings only to learn, unexpectedly, that some of his college photos were now available to "everyone."[11]

---

[9] *See In the Matter of Facebook, Inc.*, Complaint, Request for Investigation, Injunction, and Other Relief, Before the Federal Trade Commission 15-21 (May 5, 2010), *available at* http://epic.org/privacy/facebook/EPIC_FTC_FB_Complaint.pdf.

[10] *See* note 3, *supra.*

[11] Kashmir Hill, *Either Mark Zuckerberg Got a Whole Lot Less Private or Facebook's CEO Doesn't Understand the Company's New Privacy Settings*, TRUE/SLANT, Dec. 10, 2009, http://trueslant.com/KashmirHill/2009/12/10/either-mark-zuckerberg-got-a-whole-lot-less-private-or-facebooks-ceo-doesnt-understand-the-companys-new-privacy-settings/ (last visited July 27, 2010).

I am convinced that not even Facebook understands how its own privacy settings operate. And if Facebook cannot understand the privacy settings, how can the users?[12]

Risks to Users

The problem is serious also because these weaknesses can be exploited by criminals and others. And these data-based crimes can be very difficult to trace back to the source. For example, when a video camera is stolen from the back seat of a car, the owner knows what was taken, approximately when it was taken, and the scope of the damage. But crimes such as identity theft rarely have any of these characteristics. Information can be gathered from several sources. Delay may favor the criminal. The extent of damage is often difficult to determine.[13]

It is only in those cases where investigations are pursued that the link between a user and a sloppy business practice is likely to be established. One of the most well known examples occurred back in 2005 when the data broker Choicepoint publicly disclosed that it had sold personal information on 145,000 consumers to a criminal ring engaged in identity theft.[14] Ironically, the company also sold business verification services, but it did not bother to verify its own sale of consumer data.[15]

That case was of particular interest to EPIC because EPIC had warned the FTC prior to the incident that Choicepoint's lax security practices were placing consumers at risk.[16] The FTC ignored our complaint and one of the largest cases of identity theft occurred. It was only after the harm occurred that the FTC got involved, ultimately issuing its largest fine for a privacy violation in history.[17]

---

[12] Facebook Privacy Policy, http://www.facebook.com/policy.php (last visited on July 27, 2010) ("We cannot ensure that information you share on Facebook will not become publicly available."); *see also* Kurt Opsahl, *Facebook's Eroding Privacy Policy: A Timeline*, EFF DEEPLINKS BLOG, April 28, 2010, http://www.eff.org/deeplinks/2010/04/facebook-timeline/.

[13] FTC, CONSUMER SENTINEL NETWORK DATABOOK FOR JANUARY-DECEMBER 2009 (FTC Februrary 2010), available at http://www.ftc.gov/sentinel/reports/sentinel-annual-reports/sentinel-cy2009.pdf. *See also* FTC, *FTC Issues Report of 2009 Top Consumer Complaints*, http://www.ftc.gov/opa/2010/02/2009fraud.shtm (identity theft is top complaint of American consumers.)

[14] ChoicePoint, Securities and Exchange Commission Form 8-K, filed March 4, 2005, *available at* http://www.sec.gov/Archives/edgar/data/1040596/000095014405002087/g93611e8vk.htm (last visited July 27, 2010).

[15] *See* EPIC, *Choicepoint*, http://epic.org/privacy/choicepoint/ (last visited July 27, 2010).

[16] EPIC, *In the Matter of Choicepoint*, Request for Investigation and for Other Relief, before the Federal Trade Commission (Dec. 16, 2004), *available at* http://epic.org/privacy/choicepoint/fcraltr12.16.04.html.

[17] Federal Trade Commission, *ChoicePoint Settles Data Security Breach Charges; to Pay $10 Million in Civil Penalties*, $5 Million for Consumer Redress (Jan. 26, 2006), http://www.ftc.gov/opa/2006/01/choicepoint.shtm (last visited July 27, 2010).

Finding the tie between the cavalier attitude of social network services toward user privacy and the harms users suffered will not be easy. But reports of specific harms resulting from information made available by these services are available, including instances of domestic violence and "outing." For example, anonymous blogger "Harriet Jacobs" revealed that her abusive ex-husband gained access to her current location and workplace because of Google Buzz creating automated lists from email contacts without subscriber consent.[18] Computer science students at MIT looked at a user's Facebook friends and could predict whether the person was gay.[19] In another example, a computer science professor at the University of Texas was able to predict a Facebook user's political affiliation using details from user profiles and friend lists.[20] And researchers at the University of Maryland, College Park found that users' gender could be predicted from user profile information, membership pages, and friend lists.[21]

EPIC Facebook Complaints

Because of the many changes to the Facebook privacy policy, EPIC in collaboration with many other consumer and privacy organizations have asked the FTC to investigate.[22] To be very clear, when the company changes its privacy policies, there is really nothing the user can do. You can't even quit and walk away because Facebook makes it very difficult to permanently delete accounts. [23]

Our complaints to the FTC set out a simple theory – for a company to announce a privacy policy, to sign up a user, and then to change that privacy policy without meaningful consent is an unfair and deceptive trade and practice, or in most

---

[18] Harriet Jacobs, Fugitivus Blog Post: *Fuck You Google* (Feb. 11, 2010), http://gizmodo.com/5470696/fck-you-google.

[19] Carter Jerigan and Behram F.T. Mistree, *Gaydar: Facebook friendships expose sexual orientation*, 14 FIRST MONDAY (2009), *available at* http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/2611/2302. *See also* Carolyn Y. Johnson, *Project 'Gaydar'*, BOSTON.COM, (Sept. 20, 2009), http://www.boston.com/bostonglobe/ideas/articles/2009/09/20/project_gaydar_an_mit_experiment_raises_new_questions_about_online_privacy/; Steve Lohr, *How Privacy Vanishes Online*, NEW YORK TIMES (March 16, 2010), http://www.nytimes.com/2010/03/17/technology/17privacy.html.

[20] Jack Lindamood, et al, *Inferring private information using social network data*, Proceedings of the 18th International World Wide Web Conference, 1145 (2009), *available at* http://portal.acm.org/citation.cfm?id=1526899.

[21] *See* Carolyn Y. Johnson, *Project 'Gaydar'*, BOSTON.COM, (Sept. 20, 2009), http://www.boston.com/bostonglobe/ideas/articles/2009/09/20/project_gaydar_an_mit_experiment_raises_new_questions_about_online_privacy/.

[22] *See* EPIC et al FTC Complaint, *In the Matter of Facebook* (May 5, 2010), *available at* http://epic.org/privacy/facebook/EPIC_FTC_FB_Complaint.pdf; EPIC et al FTC Supplemental Materials, *In re Facebook* (January 15, 2010), *available at* http://www.epic.org/privacy/inrefacebook/EPIC_Facebook_Supp.pdf; EPIC et al FTC Complaint, *In re Facebook* (Dec. 17, 2009), *available at* http://epic.org/privacy/inrefacebook/EPIC-FacebookComplaint.pdf.
EPIC et al FTC Supplemental Materials, *In re Facebook* (January 15, 2010), 4, *available at* http://www.epic.org/privacy/inrefacebook/EPIC_Facebook_Supp.pdf.

simple terms, a "bait and switch."[24] That is essentially the problem that Facebook users confronted as well as users of Gmail who find that there email accounts contact information had been made publicly available so that Google could launch a social network service to compete with Facebook.

It is appropriate for the FTC to intervene in these circumstances for the obvious reason that the company is not honoring its part of the bargain but the FTC has been reluctant to do so.[25] That is a problem and has also exposed users to unnecessary risk.

Approaches to Privacy – Regulations, Self-Regulation, Bait and Switch

Congress has taken a variety of approaches to protecting privacy in new online environments. Sometimes, Congress will pass legislation as it did to protect telephone communications many years ago[26] or electronic health records more recently.[27] Congress also passed privacy legislation for email, fax machines, polygraphs, cable television, and many other new services.[28]

Other times Congress may allow industries to regulate themselves under the belief that industry will come up with effective standards that protect consumers. In the privacy world, this self-regulatory approach has always assumed that companies would still remain accountable to their users through the privacy policies that they establish.[29] This means that privacy policies, voluntarily developed by companies, must still be enforceable.[30]

But here is the problem: if the Federal Trade Commission is unwilling or unable to enforce these policies and if individual users are unlikely or unable to bring their claims, then there is no incentive for companies to honor their

---

[24] EPIC et al FTC Complaint, *In the Matter of Facebook*, 1, (May 5, 2010), *available at* http://epic.org/privacy/facebook/EPIC_FTC_FB_Complaint.pdf; EPIC et al FTC Supplemental Materials, *In re Facebook*, 1-2, (January 15, 2010), *available at* http://www.epic.org/privacy/inrefacebook/EPIC_Facebook_Supp.pdf; EPIC et al FTC Complaint, *In re Facebook*, 1, (Dec. 17, 2009), *available at* http://epic.org/privacy/inrefacebook/EPIC-FacebookComplaint.pdf.

[25] Federal Trade Commission Act § 5, 15 U.S.C. § 45 (2006).

[26] *See* the Telephone Consumer Protection Act of 1991, 47 U.S.C. § 227 (2006); the Electronic Communications Privacy Act of 1986, 18 U.S.C. § 2510, *et seq.* (2006); *see also* 47 U.S.C. § 605 (2006).

[27] *See* The Health Insurance Portability and Accountability Act of 1996, Privacy Rule, 45 CFR Parts 160 and 164, 67 FED. REG. 53182 (2002).

[28] *See generally* MARC ROTENBERG. THE PRIVACY LAW SOURCEBOOK: UNITED STATES LAW, INTERNATIONAL LAW, AND RECENT DEVELOPMENTS (EPIC 2005).

[29] In 1999, the Federal Trade Commission published a report setting forth this model. *See* FEDERAL TRADE COMMISSION, SELF-REGULATION AND PRIVACY ONLINE (1999), *available at* http://www.ftc.gov/os/1999/07/privacy99.pdf.

[30] For a detailed explanation of the need for enforceability, see Peter P. Swire, *Markets, Self-Regulation, and Government Enforcement in the Protection of Personal Information*, *in* U.S. DEPARTMENT OF COMMERCE, PRIVACY AND SELF-REGULATION IN THE INFORMATION AGE, (1997) *available at* http://ssrn.com/abstract=11472.

commitments. They may get hit with bad press, but that simply turns privacy changes into a public relations problem, which companies have learned to manage in a variety of ways. For example, companies might fund "consumer" organizations so that they are less likely to express criticism over changes in business practices.[31]

This problem is particularly acute with firms such as Facebook, which are becoming—as Mark Zuckerberg has acknowledged—"social utilities," essential services that face no meaningful competition in the marketplace.[32] But

Recommendations

Companies increasingly respond to calls for Congressional action by saying that action by Congress will stifle innovation. But much of the innovation that is being promoted today is not so much about technology, but about marketing. Companies are finding new ways to collect and disclose user data and they do this in ways that make it increasingly difficult for users to understand or control. This is the activity that the companies do not want regulated.

This is evident also in the privacy field where laws have created incentives for better business practices that promote trust and confidence in new services and reduce risks to consumers. For example, many recent privacy laws create obligations for companies offering online services to encrypt communications and stored data.[33] Others make consent meaningful through explicit opt-in requirements.[34]

For Facebook, one of the simplest and most effective ways to give users meaningful control would be to make explicit in statute the need for the company to obtain explicit, opt-in consent for any disclosure that the company makes of user data to third parties. Most notably, section 2701 of the Stored Communications Act (SCA), part of the Electronic Communications Privacy Act (ECPA)[35] should restrict more forcefully the ability of service providers such as Facebook to share user data with third parties without explicit opt-in consent from users.

It is obvious and commonsense that it is the user who should decide to whom to disclose their data. Facebook can provide many different services that allow, and even encourage users to share data, but the company should not decide for the user

---

[31] For an in-depth explanation of this problem, see EPIC, Privacy Regulation: A Decade of Disappointment, http://epic.org/reports/decadedisappoint.html.
[32] *See, e.g.*, Joshua Brustein, Facebook is to Power Company as . . . , NY TIMES, July 24, 2010, *available at* http://www.nytimes.com/2010/07/25/weekinreview/25brustein.html.
[33] *See, e.g.*, Health Information Technology for Economic and Clinical Health (HITECH) Act, 42 U.S.C. § 201 *note* (2010).
[34] *See, e.g.*, Health Insurance Portability and Accountability Act (HIPAA) of 1996, 42 U.S.C. § 201 et seq. (2010); HIPAA Administration Simplification, 45 C.F.R. § 164.508-510.
[35] 18 U.S.C. § 2701 et seq. (2010)

what information to share. Whenever that occurs, the user has lost control and has lost privacy.

Conclusion

Mr. Chairman, Facebook is a tremendous service, with the scope of email, the telephone, and even the Internet itself. It is also the source of many of the privacy concerns of users today. The critical problem is not what users post; it is that the Facebook changes the privacy settings too frequently and Facebook makes it too difficult for users to selectively post information. Self-regulation has not worked because the FTC has been reluctant to pursue investigations. So, EPIC recommends changes to ECPA in Title 18 that would give users greater control of their information and reduce risk when they go online.

GENERAL REFERENCES

Dana boyd, "Facebook's paternalistic attitudes aren't empowering," CNN Tech, June 28, 2010.

Letter from Chairman John Conyers, Jr. to Mark Zuckerberg (May 28, 2010), *available at* http://judiciary.house.gov/hearings/pdf/Conyers-Facebook100528.pdf.

Electronic Privacy Information Center (EPIC), Facebook Privacy, http://epic.org/privacy/facebook/ (last visited Jul. 27, 2010).

EPIC, Social Networking Privacy, http://epic.org/privacy/socialnet/ (last visited Jul. 27, 2010).

EPIC et al. FTC Complaint, *In re Facebook* (Dec. 17, 2009), *available at* http://epic.org/privacy/inrefacebook/EPIC-FacebookComplaint.pdf.

EPIC et al. FTC Supplemental Complaint, *In re Facebook* (Jan. 14, 2010), *available at* http://epic.org/privacy/inrefacebook/EPIC_Facebook_Supp.pdf.

EPIC et al. FTC Complaint, *In re Facebook II* (May 5, 2010), *available at* http://epic.org/privacy/facebook/EPIC_FTC_FB_Complaint.pdf

EPIC et al. FTC Complaint, *In re Google Buzz* (Feb. 16, 2010), *available at* http://epic.org/privacy/facebook/EPIC_FTC_FB_Complaint.pdf

EPIC et al. FTC Supplemental Complaint, *In re Google Buzz* (Mar. 2, 2010), *available at* http://epic.org/privacy/facebook/EPIC_FTC_FB_Complaint.pdf

Facebook, People Against the new Terms of Service (TOS), administrated by Julius Harper Jr, and Anne Kathrine Yojana Petterøe, http://www.facebook.com/group.php?gid=77069107432.

Facebook, Bring back News Feed and Wall privacy settings, administrated by Maggie Ds, http://www.facebook.com/group.php?v=wall&gid=204943119385.

Facebook, Millions Against Facebook's Privacy Policies and Layout Redesigns, administrated by Miki Perrotta and Jessica Fishbein, http://www.facebook.com/group.php?gid=27233634858.

DAVID KIRKPATRICK, THE FACEBOOK EFFECT: THE INSIDE STORY OF THE COMPANY THAT IS CONNECTING THE WORLD (2010).

BEN MEZRICH, THE ACCIDENTAL BILLIONAIRES: THE FOUNDING OF FACEBOOK, A TALE OF SEX, MONEY, GENIUS, AND BETRAYAL (2009).

JOHN PALFREY AND URS, BORN DIGITAL: UNDERSTANDING THE FIRST GENERATION OF DIGITAL NATIVES (2009)

Jeffrey Rosen, *The Web Marks the End of Forgetting,* N.Y. TIMES MAGAZINE, July 25, 2010, at 26, *available at* http://www.nytimes.com/2010/07/25/magazine/25privacy-t2.html.

Marc Rotenberg, Op-Ed, *Online friends at what price? The point of social networking is to share your personal information with the world*, SACRAMENTO BEE, July 20, 2008.

Marc Rotenberg, Constructing a Policy Framework for Social Network Services: Distinguishing the Roles and Responsibilities of the Participants, Computers, Privacy, and Data Protection Conference, Brussels, Belgium (Jan. 2009), *available at* http://www.cpdpconferences.org/L-Z/rotenberg.html

Clive Thompson, *Brave New World of Digital Intimacy*, N.Y. TIMES MAGAZINE, Sept. 5, 2008, at 42, *available at* http://www.nytimes.com/2008/09/07/magazine/07awareness-t.html.

Mr. SCOTT. Thank you.

We have been joined by the gentleman from Illinois, Mr. Quigley, so thank you for being with us.

Mr. Pasqua?

TESTIMONY OF JOE PASQUA, VICE PRESIDENT FOR RESEARCH, SYMANTEC, INC., WASHINGTON, DC

Mr. PASQUA. Mr. Chairman, Ranking Member Gohmert and Members of the Subcommittee, thank you for the opportunity to appear here today and discuss this important topic. As a global information security leader, Symantec welcomes the opportunity to provide the Committee with our insights on how to keep social network users safe online.

While social networking has provided many new benefits, it has also opened new doorways for cyber-crime. It has expanded online opportunities for the underground economy, which has discovered that social networking pays.

The infiltration of communities and the spreading of spam or malware have become a part of everyday life within social networks, and that trend is increasing. The potential abuses cyber-criminals have conceived are highly varied and range from targeted spying, spam and phishing mail distribution to exploitation of security holes within particular social networking platforms.

Attacks against both social networking sites themselves, as well as individual users of those sites, have now become standard practice for criminals. Part of the reason for this is that these sites combine two factors that make for an ideal target for online criminal activity: a massive number of users and a high level of trust among the users.

Social networks also provide a rich repository of information cyber-criminals can use to refined their phishing attacks. Many Internet users today are too blase about the information they post on the web. Social network users should always be cautious about the information they post online and how it can be used.

In a rush to embrace the advantages of sharing information on the Internet, many young people in particular have created online data sets, or "tattoos," that, much like the real thing, are difficult to remove. Posting personal information online can also leave them vulnerable to identity theft. Details such as postal codes, birthdates, mother's maiden names, can all be used by cyber-criminals to crack passwords, hijack accounts, send out spam, and distribute malware.

In addition to the direct insertion of malware or the distribution of mass mailings, cyber-criminals use social networks to lure users to primed Web sites where they can steal personal data so that they can sell it for profit. There has been a marked increase in crimeware, or software used to conduct cyber-crime, on social networks and elsewhere.

In 2009, Symantec created over 2.5 million new virus signatures and discovered more than 210 million distinct malware variants. That is a 56 and 75 percent increase, respectively, over the same period in 2008.

And to put this in perspective, Symantec created more malware signatures in the past 15 months than in the previous 18 years combined. So it is a massive, massive increase.

Attackers are now going directly after the end user and attempting to trick them into downloading malware or divulging sensitive information under the auspice that they are doing something perfectly innocent. Social engineering's popularity is at least in part spurred by the fact that the operating system that a user is using or a browser is largely irrelevant. It is the actual user that is being targeted, not necessarily vulnerabilities in the machine.

To their credit, social network sites squash most threats quickly, but it is not just targeted attacks you should be worried about. It is adapted attacks. Adapted attacks occur when bad guys take existing threats and use social networks to increase the effectiveness of the attack through social engineering. There is nothing like being surrounded by friends to get you to lower your guard, and that is what they make you think they are doing.

Given the potential for monetary gain from compromised corporate intellectual property, cyber-criminals have also turned their attention toward enterprises. Attackers are leveraging the abundance of personal information openly available on social networking sites to synthesize socially engineered attacks on key individuals within targeted companies. This can take into account position within the company, colleagues, hobbies, places they have been, pictures, etcetera.

I am just going to skip ahead a little bit and wrap up because I see I am running low on time. But I will mention that, according to a recent Symantec enterprise security survey, most organizations do not have social networking policy in place despite giving employees unfettered access to these popular Web sites. Our survey also found that 84 percent of CIOs and CISOs consider social networking sites to be a serious threat to their security.

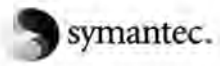
In closing, I have provided in my written testimony to the Committee a number of useful precautions that all users of social networks should consider in their use of this new medium, and we all call this to the Committee's attention.

Mr. Chairman and Members of the Committee, Symantec appreciates the opportunity to provide our input on combating cybercrime on social networks and protecting online privacy so the Internet can reach its full potential. We look forward to continuing to work with the Committee as it considers future legislation in this area.

Thank you.

[The prepared statement of Mr. Pasqua follows:]

PREPARED STATEMENT OF JOSEPH PASQUA



Prepared Testimony and Statement for the Record of

Joseph Pasqua
Vice President of Research
Symantec Corporation

Hearing on

Online Privacy, Social Networking, and Crime Victimization

Before the

House Judiciary Committee
Subcommittee on Crime, Terrorism, and Homeland Security

July 28, 2010
2141 Rayburn House Office Building

Mr. Chairman, Ranking Member Gohmert, and members of the Subcommittee, I am Joe Pasqua, Vice President of Research for Symantec Corporation[1]. I'm responsible for all activities within Symantec Research Labs, the company`s global research organization. Thank you for the opportunity to appear before you today to discuss the Committee's efforts to help ensure that consumers and businesses better understand the risks of social networking websites and the steps that one can take to reduce these risks before participating on such sites.

As the global information security industry leader, security is our top priority at Symantec. We are committed to assuring the security, availability and integrity of our customers' information. We protect more people from more online threats than anyone in the world. Our best-in-class Global Intelligence Network[2] allows us to capture worldwide security intelligence data that gives our analysts an unparalleled view of the entire Internet threat landscape including emerging cyber attack trends, malicious code activity, phishing and spam. We maintain eleven Security Response Centers globally and utilize over 240,000 attack sensors in 200 countries to track malicious activity 24 hours a day, 365 days a year. In short, if there is a class of threat on the Internet, Symantec knows about it.

Symantec strives to help educate Internet users about their exposure to online risks, and to offer advice and solutions for how they can help to keep themselves and their family and friends safe online. We welcome the opportunity to provide comments as the Committee continues its important efforts to deter social network crime victimization and further enhance cybercrime law enforcement efforts. In my testimony today, I will provide the Committee with:

- Symantec's assessment of the latest social networking cybercrime threats;
- Our Insights into the inherent privacy risks associated with social networking;
- Recommended pre-cautions for consumers and businesses alike to follow to in order to avoid being victimized by cybercriminals on social network sites; and
- Issues for the Committee to consider in order to help prevent social network cybercrime.

Social network tools have changed our personal and professional lives. Consumers and businesses alike have taken to the Internet as a medium for our most personal and sensitive activities, as search engines, social networking sites, online banking, and medical information. Web sites are becoming part of the daily lives of Americans. Social networking is everywhere. It is common to find parents, children, coworkers and even the elderly on the networks across the social media world on sites such as Twitter, MySpace, Facebook, YouTube and LinkedIn.

With social networks people across the world have access to tools and options that were previously non-existent. However, there are just as many new opportunities to connect as there are to get into potential danger. Social networking has opened up many new doorways for cyber-crime, and with all the people on social networks who are completely new to technology, it is more important than ever to educate people so they are aware of these risks.

---

[1] Symantec is a global leader in providing security; storage and systems management solutions to help consumers and organizations secure and manage their information-driven world. Our software and services protect against more risks at more points, more completely and efficiently, enabling confidence wherever information is used or stored. More information is available at www.symantec.com.

[2] Symantec has established some of the most comprehensive sources of Internet threat data in the world through the Symantec Global Intelligence Network. This network captures worldwide security intelligence data that gives Symantec analysts unparalleled sources of data to identify, analyze, deliver protection and provide informed commentary on emerging trends in attacks, malicious code activity, phishing, and spam. More than 240,000 sensors in 200+ countries monitor attack activity through a combination of Symantec products and services as well as additional third-party data sources.

The number of online U.S. households using social networks such as Facebook and MySpace has nearly doubled in the past year expanding online opportunities for criminals. The underground economy has also discovered that social networking pays. Cybercriminals have long been using the idea of these participation networks for their own purposes. The infiltration of communities, the spreading of spam or malware have in the meantime become a part of everyday life within social networks. And that trend is increasing! The potential abuses the criminals have conceived are highly varied and range from targeted spying on personal data, through spam and phishing mail distribution up to exploitation of security holes within the particular social networking platform.

Beginning in 2009, attacks against both social networking sites themselves and the users of those sites have now become standard practice for criminals. The latter half of 2009 saw attacks utilizing social networking sites increase in both frequency and sophistication. Such sites combine two factors that make for an ideal target for online criminal activity: a massive number of users and a high-level of trust among those users.

Social Networks Are a Rich Repository of Personal Information

The popularity of Facebook and other social networking sites has given hackers new ways to steal both money and information. Social networks provide a rich repository of information cybercriminals can use to refine their phishing attacks. Many Internet users are too often blasé about the information they post on the web. According to a 2009 Symantec survey, computer users under 25 years old are especially exhibiting a casual attitude to internet security with two thirds saying they aren't worried about the information they leave behind.

Nearly two thirds of computer users under 25 years old have uploaded personal photographs and private details to a social networking site. In addition, 79 percent of respondents revealed postcodes and 48 percent disclosed phone numbers on social networking sites; one in 10 has put their bank details online and one in 20 has uploaded their passport number. By comparison older internet users are more cautious about the information that they post online: under a third of 36-45 year-olds share photographs, and only two in 10 people over 46 years old share their photographs online.

People of all ages should be wary of the information that they are posting online. In a rush to embrace the advantages of sharing information on the internet, many young people have created online databanks or "tattoos" that much like a real life tattoo are difficult to remove. A "digital tattoo" is created by all the personal information web users post online and can easily be found through search engines by a potential or current employer, friends and acquaintances, or anyone who has malicious intent. Posting personal information online can also leave you vulnerable to identity theft. Details such as postcodes, birth dates or mother's maiden names can all be used by cybercriminals to crack passwords and hijack accounts to send out spam or malware to contact lists for financial gain.

Personal Data Targeted

Alongside the direct insertion of malware or the distribution of mass mailings, the cyber criminals use social networks to lure users to primed websites where they can steal personal data so that they can sell it for a profit. Targeted by the offenders are login data and classical account data, telephone numbers, email addresses and dates of birth. There's been a marked increase in "crimeware," or software used to conduct cybercrime on social networks and elsewhere. These tools fuel the black market including, botnets, keystroke loggers, spyware, backdoors, and Trojans. In 2009, Symantec created over 2.5 million new virus signatures and discovered more than 210 million distinct malware variants, a 56 percent and 75 percent increase, respectively,

over the same period in 2008[3]. To put this in prospective, Symantec created more signatures in the past 15 months than in the past 18 years combined.

According to Symantec's *Report on the Underground Economy,*[4] there continues to be a well-organized underground economy specializing in the sale of stolen confidential data, particularly credit card and bank account credentials. Today's cybercriminals thrive on obtaining unauthorized information from consumers and businesses. This active underground economy has matured into an efficient, global marketplace in which stolen goods and fraud-related services are regularly bought and sold. The underground economy is geographically diverse and generates revenue for cybercriminals who range from loose collections of individuals to organized and sophisticated groups. The geographical locations of underground economy servers constantly change to evade detection by law enforcement.

Symantec has calculated that the potential worth of all credit cards advertised in the Underground Economy at $5.3 billion. The second most common category of goods and services advertised was financial accounts at 20 percent of the total. While stolen bank account information sells for between $10 and $1,000, the average advertised stolen bank account balance is nearly $40,000. The total worth of the bank accounts advertised during this reporting period was $1.7 billion.

In addition, cybercrime attack toolkits have lowered the bar to entry for new cybercriminals, making it easy for unskilled attackers to compromise computers and steal information. One such toolkit called Zues, which can be purchased for as little as $700, automates the process of creating customized malware capable of stealing personal information. Using kits like Zeus, attackers created literally millions of new malicious code variants in an effort to evade detection by security software.

Social Engineering as the Primary Attack Vector

Attackers are now going directly after the end user and attempting to trick them into downloading malware or divulging sensitive information under the auspice that they are doing something perfectly innocent. Social engineering's popularity is at least in part spurred by the fact that what operating system and Web browser rests on a user's computer is largely irrelevant, as it is the actual user being targeted, not necessarily vulnerabilities on the machine. Social engineering is already one of the primary attack vectors used today, and Symantec estimates that the number of attempted attacks using social engineering techniques is continuing to increase in 2010.

If the social network sites are paying attention, and to their credit they usually are, most threats can be squashed pretty quickly. It's not targeted attacks you should be worried about, but *adapted* attacks. Adapted attacks occur when the bad guys take existing threats and use social networks to increase the effectiveness of the social engineering aspect of the attack. There is nothing like being surrounded by friends to get you to lower you guard.

---

[3] Symantec's Internet Security Threat Report, Volume XV, April 2010. The Symantec Internet Security Threat Report provides an annual overview and detailed analysis of Internet threat activity, malicious code, and known vulnerabilities. The report also discusses trends in phishing, spam and observed activities on underground economy servers.

[4] Symantec's Report on the Underground Economy is a survey of cybercrime activity in the underground economy. It includes a discussion of some of the more notable groups involved, as well as an examination of some of the major advertisers and the most popular goods and services available. It also includes an overview of the servers and channels that have been identified as hosts for trading, and a snapshot of software piracy using a file-sharing protocol in the public domain. This report is meant to be an analysis of certain aspects of the underground economy and is not meant to encompass a survey of Internet cybercrime as a whole. For the underground economy servers observed by Symantec, the period of observation was between July 1, 2007, and June 30, 2008.

Take the problem we are getting a lot of reports on currently—it's an advanced payment scam. This is often called a Nigerian 419 scam. But, instead of some prince in Nigeria, the scammer appears to be a friend of yours. And, instead of getting a long letter, you're contacted via a social network. What remains the same is that they both want your cash. You'll undoubtedly see endless variations on this theme, but the basic scam is that someone you are connected to via a social network posts a status message or instant messages you, or sends you an email stating that they are in trouble. They are apparently stuck somewhere -- London is currently popular -- and have gotten lost or been robbed of all their cash or both. They need you to "loan" them some money so they can get home.

Unlike helping the Prince of Nigeria, your motivation to send the cash is noble; you want to help out a friend. But, here's the thing. Whoever is contacting you is an imposter. The imposter has broken into your friend's account and having unrestricted access to all of that personal information makes it pretty easy to make convincing claims. With a stolen login and password, someone can be very convincing while pretending to be your friend.

The Proliferation of Rogue Security Software

A growing cybercrime trend is the use of misleading software programs or commonly known as RogueAV programs. Symantec's *Report on Rogue Security Software*[5], based on data obtained during the 12-month period of July 2008 to June 2009, reveals that cybercriminals are now employing increasingly persuasive online scare tactics to convince users to purchase rogue security software. Rogue security software, or "scareware," is software that pretends to be legitimate security software. These rogue applications provide little or no value and may even install malicious code or reduce the overall security of the computer.

To encourage unsuspecting users to install their rogue software, cybercriminals place deceptive website ads that prey on users' fears of security threats. These ads appear credible but typically include false claims such as "If this ad is flashing, your computer may be at risk or infected," urging the user to follow a link to scan their computer or get software to remove the threat. According to the study, 93 percent of the software installations for the top 50 rogue security software scams were intentionally downloaded by the user. As of June 2009, Symantec detected over 250 distinct rogue security software programs and had received reports of 43 million rogue security software installation attempts. Symantec blocked 4.8 million attacks of just one version of this type of malware.

Targeted Attacks on Companies

Given the potential for monetary gain from compromised corporate intellectual property (IP), cybercriminals have turned their attention toward enterprises. Symantec's Internet Security Threat Report found that attackers are leveraging the abundance of personal information openly available on social networking sites to synthesize socially engineered attacks on key individuals within targeted companies.

The information, which members of social networks divulge about themselves and their living circumstances, also permits cyber criminals to carry out targeted attacks on companies. With the information that you can collect in Xing about a particular company, targeted phishing mails can be sent to company management, sales

[5] The Symantec Report on Rogue Security Software, developed by the company's Security Technology and Response (STAR) organization, is an in-depth analysis of rogue security software programs. The report includes an overview of how these programs work and how they affect users, including their risk implications, various distribution methods, and innovative attack vectors. It includes a brief discussion of some of the more noteworthy scams as well as an analysis of the prevalence of rogue security software globally. It also includes a discussion on a number of servers that Symantec observed hosting these misleading applications. Except where otherwise noted, the period of observation for this report was from July 1, 2008 to June 30, 2009.

or accounts. This can take into account, position within the company, colleagues and hobbies. Tailor-made spyware Trojans infiltrated in this manner can ruin companies.

A Facebook message sent last fall between co-workers at a large U.S. financial firm which read: "Hey Alice, look at the pics I took of us last weekend at the picnic. Bob". The social network message rang true enough. Alice had, in fact, attended a picnic with Bob, who mentioned the outing on his Facebook profile page. So Alice clicked on the accompanying Web link, expecting to see Bob's photos. But the message had come from thieves who had hijacked Bob's Facebook account. And the link carried an infection. With a click of her mouse, Alice let the attackers usurp control of her Facebook account and company laptop. Later, they used Alice's company logon to slip deep inside the financial firm's network, where they roamed for weeks. They had managed to grab control of two servers, and were probing deeper, when they were detected.

Intrusions like this one can expose a company to theft of its most sensitive data. Such attacks illustrate a dramatic shift underway in the Internet underground. Cybercriminals are moving aggressively to take advantage of an unanticipated chink in corporate defenses: the use of social networks in workplace settings. They are taking tricks honed in the spamming world and adapting them to what's driving the growth of social networks: speed and openness of individuals communicating on the Internet.

What happened to Bob and Alice, the picnickers at the financial firm, illustrates how social networks help facilitate targeted attacks. As a rule, tech-security firms investigate breaches under non-disclosure agreements. Investigators increasingly find large botnets running inside corporate networks, where they can be particularly difficult to root out or disable. Social networks represent a vehicle to distribute malicious programs in ways that are not easily blocked.

Social networking attacks run the gamut. Earlier this year, one band of low-level cyberthieves, known in security circles as the Kneber gang, pilfered 68,000 account logons from 2,411 companies, including user names and passwords for 3,644 Facebook accounts. Active since late 2008, the Kneber gang has probably cracked into "a much higher number" of companies. Stolen credentials flow into eBay-like hacking forums where a batch of 1,000 Facebook user name and password pairs, guaranteed valid, sells for $75 to $200, depending on the number of friends tied to the accounts. On the high end, the Koobface worm, initially set loose several months ago, continues to increase in sophistication as it spreads through Facebook, Twitter, MySpace and other social networks. At its peak last August, more than 1 million Koobface-infected PCs inside North American companies were taking instructions from criminal controllers to carry out typical botnet criminal activities.

Social Networking Policies Still Scarce

Social networking is rapidly evolving into one of the biggest threats to data security out there today. But the reality is this medium is also a great way for your employees to collaborate and communicate. The challenge for many security professionals today lies in finding a balance between enabling the business while maintaining optimal security practices.

Most organizations do not have a social networking policy, despite giving employees unfettered access to the popular web sites, and according to a survey conducted by Symantec earlier this month. The survey was an attempt to gauge employee use of social media after a 2010 Symantec report on enterprise security found that enterprises view social media as a threat to security. In fact, eighty-four percent of CIOs and CISOs surveyed in

Symantec's 2010 *State of Enterprise Security Report*[6] considered social networking sites to be a serious threat to their security.

Approximately 50 percent of the 336 respondents to the survey said they access Facebook or YouTube at least once a day, with 16 percent indicating they access the sites between three and five times daily. More than half access the sites for business reasons, according to the research. Another 46 percent said the sites were accessed for personal reasons. In addition, 13 percent admit to circumventing company rules around social media. Among organizations who responded, 42 percent said their organization does not block employee access to social media sites, and has no policy in place around social media use. Only 5 percent indicated a complete blocking of the sites at work, a solution that is not really feasible in today's business environment.

Most companies will need to allow employee access to social networking sites, both for business reasons and because employees have begun to demand it. In fact, 32 percent of survey respondents indicated that being banned from social networks on the job would play a role in their decision to work for an organization.

Basic Security Measures

If you are using social networks and wish to minimize your personal security risk when doing so, you should follow some basic security tips. Symantec offers seven tips for users of a social network who want to protect their personal information. Topping this list is to (i) never share the password used to enter the site. Not even a best friend or spouse is a safe haven. Users of Facebook and other social networks should also be aware of the "digital crumbs" they leave behind. Photos, videos and comments posted on the Web are often there forever, so (ii) never post anything you wouldn't want the public, your neighbor or future employer to see. Also, (iii) never post sensitive information, such as a phone number, e-mail or birthday; and there's no need to share status updates, such as, "Off to Vegas for the weekend". Such information could be useful to criminals in your town.

Thirdly, we advise social network users to (iv) ignore links, supposedly sent from friends that have enticing titles like, "Check Out The Best Beach Bods." Chances are the link came from a hacker who broke into a friend's account. Another tip is to (v) make sure links posted to a Facebook wall are safe. While Symantec suggest the use of its Norton Safe Web software, other security vendors offer similar products. Such applications scan for links that take people to sites built by hackers to steal personal information. We also encourage people to (vi) limit their "circle of trust" on social networking sites to family and friends. Ignore requests from people you do not know, it could be a cyber-criminal. Finally, people need to (vii) stay informed of Facebook or other social networks privacy settings, which change often. In the last five years, Facebook's privacy policy has grown from about 1,000 words to today's 5,830 words.

Social Networking Rules of Engagement

Symantec encourages some basic rules to follow when engaging in social networks:

- **Don't post too much information** that could identify you or your location, including your last name, your school or business, where you live, where you spend time, your phone number or email address.

---

[6] The 2010 State of Enterprise Security report is based on input from 2100 enterprises around the world. The report finds that security IT's top concern as organizations experience frequent and increasingly effective cyber attacks. The costs of these attacks is high, and enterprise security is becoming more difficult. Symantec provides key security strategies to help security IT cope with this challenging landscape.

- **Use your site's privacy features** to limit personal posts to people you know and trust. Don't add people to your trusted list unless you know exactly who they are. Remove "friends" who post mean or untrue comments, or information that compromises your security.

- **Don't meet people you don't know**. Unless you can confirm exactly who they are, never agree to meet online friends in person. And even if you can confirm their identity, take precautions by meeting in a public, group setting.

- **Don't post suggestive pictures** or images that might give strangers clues about your identity or location. These pictures compromise your security, and they may affect how relatives, future employers, and even college admissions counselors perceive you.

- **Monitor your blog** for compromising information your friends may have added. Delete anything you don't want people to see, and consider removing offending posters from your friend list.

- **Don't lie about your age**. Acting older than you are can put you in dangerous situations. If you don't meet the age requirement, look for sites like Live Journal™, which offer lower age requirements and a safer environment.

- **Don't ever provide financial information** online without first checking with your parents, even on Web sites that appear to be legitimate. They may be fake or "phising" Web sites that exist only to steal your information.

- **What you say on a social networking site may become public** even if you post it in a private area. Don't use your account to spread rumors or disclose personal information about others. Your actions could have serious implications for you and your parents.

Conclusions

The growing danger from crimes committed against computers, or against information on computers, is beginning to claim attention by governments worldwide. Undeterred by the prospect of arrest or prosecution, cyber criminals around the world lurk online as an omnipresent menace to the financial health of businesses, to the trust of their customers, and as an emerging threat to nations' security.

Cyber crimes—harmful acts committed from or against a computer or network—differ from most terrestrial crimes in four ways. They are easy to learn how to commit; they require few resources relative to the potential damage caused; they can be committed in a jurisdiction without being physically present in it; and they are often not clearly illegal. The laws of most countries do not clearly prohibit cyber crimes. Existing terrestrial laws against physical acts of trespass or breaking and entering often do not cover their "virtual" counterparts. Web pages such as the e-commerce sites sometimes hit by widespread, distributed denial of service attacks may not be covered by outdated laws as protected forms of property. New kinds of crimes can also sometimes fall between the cracks.

Effective law enforcement is complicated by the transnational nature of cyberspace. Mechanisms of cooperation across national borders to solve and prosecute crimes are complex and slow. Cyber criminals can defy the conventional jurisdictional realms of sovereign nations, originating an attack from almost any computer in the world, passing it across multiple national boundaries, or designing attacks that appear to be originating from foreign sources. Such techniques dramatically increase both the technical and legal complexities of investigating and prosecuting cyber crimes. Clearly, law enforcement is fighting increasingly sophisticated and organized

threats; therefore, it continues to need additional resources — funding for skilled personnel and cutting-edge technology — to expand its capabilities.

Policy Recommendations

Symantec asks the Committee, as you consider new cyber crime legislation in the area of social networking or other information security issues, to take under consideration the following recommendations:

Focus on the behavior, not technology. When considering new cybercrime laws focus on a behavioral approach to public policy that focuses on punishing bad behavior versus regulating the technology. For example, laws should criminalize the act of intentionally accessing a computer without authorization, or intentionally obtaining or transmitting personal information with the intent of injuring or defrauding a person or damaging a computer, not simply outlaw programs capable of collecting or transmitting data. Those programs, like other technologies, may have many legitimate uses outside the hands of a criminal. Another example of a behavioral approach would be to criminalize activity to intentionally impair the security protections of a computer.

Increase cybercrime penalties. Stronger penalties are needed to punish and deter bad actors who seek to capture information from a user's computer without authorization. It is unconscionable that cyber crime is going unpunished to the degree that it is around the world and governments worldwide must come to grips with the escalating threats. We fully support strengthening enforcement measures to go after these increasingly emboldened bad actors. Of course, penalties in criminal law must also account for innocent, unsuspecting users whose computers are unknowingly taken over by cyber criminals and used as a platform to orchestrate cyber crime on other users' computers -- often the case in botnet herding.

Develop a model approach for use globally. Unless crimes are defined in a similar manner across jurisdictions, coordinated efforts by law enforcement officials to combat cyber crime will be complicated. A globally harmonized framework of legislation against e-crime is needed. Governments around the work need to agree on the definitions of e-crime and of phishing so that attackers from all jurisdictions can be aggressively pursued in the criminal justice system. Most countries, particularly those in the developing world, are seeking a model to follow. These countries recognize the importance of outlawing malicious computer-related acts in a timely manner in order to promote a secure environment for e-commerce. But few have the legal and technical resources necessary to address the complexities of adapting terrestrial criminal statutes to cyberspace. A coordinated, public-private partnership to produce a model approach can help eliminate the potential danger from the inadvertent creation of cyber crime havens.

Build a strong federal law enforcement and private industry partnership. Federal law enforcement needs to continue to build a strong partnership with State and local law enforcement by which we share expertise, equipment, and avoid costly duplication and fragmentation. Federal law enforcement should work in partnership with industry to address cybercrime and security. This should not be a top down approach through excessive government regulation or mandates. Rather, we need a true partnership where we can discuss challenges and develop effective solutions that do not pose a threat to individual privacy. Federal law enforcement can also take more of a leadership role in developing the means of educating our young people concerning the responsible use of the Internet.

Enact a comprehensive federal data security and breach notice law. Symantec strongly urges the enactment of a strong, federally pre-emptive national data security and breach law. While poor data security or failure to notify in the event of a breach is not itself cyber crime, common sense security and breach notice are perhaps the most important prophylactic measures that could be taken to reduce the volume of future cyber crime. In particular, we support the establishment of a presumption that there is no significant risk of harm associated

with data that has been encrypted or otherwise rendered unusable or indecipherable. This is a clear incentive for businesses to adopt proven security as a roadmap to compliance that will make a real difference in reducing cyber crime. Further, we strongly support the safe harbor for nationally and internationally recognized industry standards, such as the PCI standards and related ISO standards. These two key provisions – the safe harbor for encryption and the safe harbor for adopting widely accepted industry standards – give companies that want to help protect their customers a critically needed roadmap for compliance when protecting electronic data.

* * * *

Mr. Chairman and Members of the Committee, Symantec appreciates the opportunity to provide its input on cybercrime. We share the Committee's goals to ensure that we have a robust and effective long-term strategy for combating cybercrime on social networks, protecting our nation's critical infrastructure, enhancing information security and protecting privacy so the Internet reaches its full potential for expanding communications, facilitating commerce, and bringing countless other benefits to our society. Symantec looks forward to continuing to work with the Committee as it considers cybercrime legislation in this area. Thank you.

Mr. SCOTT. Thank you. And I want to thank all of our witnesses for their testimony. And we will now have questions, and I will recognize myself first.

Are there laws in other countries that do not apply here in terms of protecting people's privacy? Mr. Rotenberg?

Mr. ROTENBERG. Maybe I should take this.

Mr. Chairman, part of our work at EPIC is looking at different approaches to privacy protection. And I think it is fairly well known that the Europeans have I guess we could say a more comprehensive approach to privacy protection in that companies that

collect data on users have presumptive obligations to protect the privacy of that information.

Here in the United States, we tend to do it on a sectoral basis. We would legislate for a particular industry, for example, like medical records, electronic health records.

I think what is important about this approach is that it means that when companies like Facebook gather information on users in other countries, they have to be more careful about disclosure to other parties because they do run some risk of stepping over the line on those more comprehensive privacy laws.

Mr. SCOTT. I think, Mr. Rotenberg, you mentioned changing security settings.

Mr. ROTENBERG. Yes, the privacy settings.

Mr. SCOTT. And what allegation were you making there?

Mr. ROTENBERG. Well, essentially that, for a person in the United States who wants to protect their privacy on Facebook, they have to go to a series of screens provided by Facebook and make some choices. Do they want their photographs, for example, to be available to everyone, or to their friends, or friends of friends, or just a small group? And you make a lot of these decisions about a lot of different information that you put online.

Our objection is that, when the user makes those decisions, and then Facebook comes along later on and says, "Well, we want to change our approach to privacy, and maybe you had your photographs available only for family members but we are going to change that setting to everyone," that is where the problem arises. And that is actually the basis of most of the concerns we think today that Facebook users have about privacy. It is the changes in those settings.

Mr. SCOTT. Mr. Sullivan, did you want to respond to that?

Mr. SULLIVAN. Thank you, Chairman.

Our position on privacy hasn't changed. It is our belief that people who use Facebook own their information, and they have the right to share their information in the way that they want to share it. And it is our responsibility to respect their wishes.

On the subject of U.S. versus international laws, we attempt to treat all of our users by one very high standard. We don't differentiate between U.S. users and other users in terms of presenting different standards to them or treat their information with different levels of care.

Our approach has been to try and improve over time. Facebook is a relatively new technology. As a company and a product, we are 6 years old. And we are growing and learning every day.

And the number one way that we learn is through feedback from our users, and we are constantly innovating and trying to learn from our users, and every innovation that we do is driven by user feedback.

And in addition to innovating, the other thing we try and pride ourselves on is responding quickly. So when we get feedback that something isn't working right, we try and fix it very quickly.

With regard to our privacy settings, we have spent a considerable time and effort in the last year trying to make them better and trying to make them easier to understand. I feel very good about

where our privacy settings are today, and would love the opportunity to walk anyone through how those settings work today.

We have a one-page that has all of your privacy settings on it right now. We try and break it into three simple buckets—your directory information, how you share information, and how you share information with applications.

With regard to how you share information, it is literally a one-click process, where you can go on the site right now and say, "I am not sure what my settings were for each different thing that I posted, but right now I would like to make everything I have ever put on the site friends-only." One click, you can do that.

In addition, we know that people want flexibility, so we have tried to build contextual messaging into our product so that, at the time you make decisions about sharing, you can customize the setting for that particular piece of information. So if I want to share information about being in front of this Committee today, I might want to share that only at work, or maybe I want to share it with all of my friends. I have the ability, one status update at a time, to change the setting to direct it to different audiences.

Mr. SCOTT. I mean—I think, because sometimes people make those choices, and Facebook comes behind and changes the settings. Is that accurate?

Mr. SULLIVAN. No, that is not accurate.

Mr. SCOTT. Mr. Marc, do you want to make your statement?

Mr. ROTENBERG. I am kind of astounded by Mr. Sullivan's answer to your question. I mean, we have documented this in 50 pages to the Federal Trade commission, and it is discussed by hundreds of thousands of Facebook users across the Facebook platform. So maybe Mr. Sullivan would like to rethink how he answered your question.

In fact, I think he should also rethink what he said earlier in response to your question about the ability of users to selectively disclose what information to make available online. Facebook has an increasingly broad category of what it considers to be publicly available information. That is the information that the user really has no control over, even the users who would like the highest level of privacy settings.

And it is clear to just about everyone what direction that category is heading, which is to say that Facebook will simply continue to make more user information available. So I think maybe Mr. Sullivan would like to rethink that answer also.

Mr. SCOTT. Do you want to respond, Mr. Sullivan?

Mr. SULLIVAN. I am not interested in changing my answer. I stand by it.

Mr. SCOTT. Gentleman from Texas.

Mr. GOHMERT. Thank you, Mr. Chairman.

And appreciate all the witnesses being here and for the testimony.

I am curious, Mr. Sullivan, what information would you recommend not sharing on Facebook specifically?

Mr. SULLIVAN. Personally and as a company, we want people to make those decisions for themselves.

Mr. GOHMERT. Well, but I am asking you personally rather than Facebook.

Mr. SULLIVAN. Well, personally, I choose to share quite a bit of information through Facebook, and I put different levels of visibility on different types of information.

My contact information I make available to my friends on Facebook, so my friends can go on Facebook and see my e-mail address, my phone numbers, my Instant Messaging identifiers and things like that. The pages that I am a fan of, I am happy to share that with other people because I like to interact with people who are fans of the same sports teams that I am fans of, etcetera. My—information—I am sorry.

Mr. GOHMERT. Let me ask you, since our time is so limited, what problems has China indicated that they have with Facebook that would prevent them from allowing Facebook to be accessible, that is?

Mr. SULLIVAN. To be honest, I don't think we have——

Mr. GOHMERT. Well, I would prefer you be honest. Thank you.

Mr. SULLIVAN. I don't think we have received a clear answer on that. My understanding is that it relates to our refusal to moderate speech.

Mr. GOHMERT. To moderate speech? So if somebody said something unkind about China, they would want that moderated. Is that correct?

Mr. SULLIVAN. It is a very sensitive issue that we spend a good deal of time trying to make sure that we as a company respect free speech rights of our users.

Mr. GOHMERT. I will take that as a yes. Thank you.

Mr. Pasqua, I appreciate your being here. And I hadn't bought a Symantec or Norton product in probably 10 or 15 years.

But there is a perception that, once information is put into a social networking site, that it is there forever, and there is just really not anything that can be done. Since you have been in the security business with the software, is there anything that can be done to actually pull stuff out once it is in there?

Mr. PASQUA. The fact of the matter is, there really are a lot of different sites out there, and they have different capabilities. Obviously, Facebook is a major important one, but there are certain types of information on certain sites that you can remove. There are other types of information in other sites where you really have very little control over pulling back information once you have created that content.

So if you, for example, have a comment on a blog that is controlled by someone else, you can't necessarily control whether you can delete that comment, or change it or amend what you have said. It is really up to the owner of that Web site.

Mr. GOHMERT. Okay. Let me ask our Federal entities representatives.

Mr. Snow, how easy is it to pass information about questionable Internet activity to other Federal entities, whether the NSA, CIA, Secret Service? How easy is it within the FBI to do that?

Mr. SNOW. Sir, from the FBI's position, it is very easy for us to pass——

Mr. GOHMERT. Well, I understand that is your position, but from a factual standpoint, how easy is it?

Mr. SNOW. Yes, sir. We right now—and the Chairman originally discussed it somewhat—we have the National Cyber Investigative Joint Task Force that has been designated by the White House and——

Mr. GOHMERT. No, no, I understand all that, but, you know, I have enough friends that are Federal agents in all different sectors, and I keep hearing about difficulty, even since we had the big umbrella of Homeland Security, in communicating. In fact, some say that it is even created more problems in getting information from one to the other, because now it goes up before it comes down and goes lateral.

So that is what I am asking, really from a practical standpoint, how easy is it? If you see a problem, can you just send that out to friends at Secret Service, or what do you have to go through to get that done?

Mr. SNOW. Absolutely, sir. Anything that I have, I can pass, almost in real-time, depending on which systems are linked or not linked. So at——

Mr. GOHMERT. Do you need approval from anyone to do that?

Mr. SNOW. Sir, I am the approving entity and individual in the cyber division, so anything cyber-related would go through me. But I also take a very strong approach, a proactive approach, on pushing those approval processes down to my workers and my operators out at the National Cyber Investigative Joint Task Force.

Mr. GOHMERT. Great.

Mr. Merritt, how easy is the flow, from your experience?

Mr. MERRITT. Very easy, sir. I mentioned the cyber-intelligence section within our criminal investigative division.

Mr. GOHMERT. Right.

Mr. MERRITT. These are extremely talented, both agents and contractors with superior computer and linguistic capabilities who monitor, real-time, these codding portals we have talked about, the codding Web sites.

And when, in fact, an anomaly appears or a malware, for example, based on our electronic crimes task forces, we distribute that information real-time to our members. In turn, they channel it down their flow chains. To include, we have a representative on each FBI joint task force, along with our national Joint Terrorism Task Force, and we do have a member at their NCIJTF.

So the big benefit of this, sir, would be the private sector who are not seeing this. Some corporations are better suited, with their analysts, to identifying anomalies and intrusions more so than others, especially the medium to small size companies. But we do have that ability, and we do do that.

Mr. GOHMERT. Thank you.

Mr. MERRITT. Thank you.

Mr. GOHMERT. Mr. Pasqua, I didn't mean to be cryptic, but it is been back when I was a judge in the 1990's, I personally bought some Norton securityware. I had examined the boxes, all of the properties. Norton seemed to have good qualities, but they had a $20 rebate if you sent the original receipt. And I did, kept all the copies of everything I sent, said wait 6 weeks.

I waited about 10 weeks, called, and the lady said, "If you don't have proof that we received it, then you have got nothing." And I

said, "Well, I didn't send it certified because that would have eaten up the $20." And I said, "But I have got copies of everything." She said, "Too bad. We don't take copies. It said that in the rebate. We got the original."

So I have cost Symantec, because people know I am somewhat literate in the area, lots more than $20, and it is too late to send me my $20 now that I am in Congress. But anyway, that is the reason I haven't bought anything from Symantec in years, but I appreciate the time, and I yield back.

Mr. QUIGLEY [Presiding]. The gentleman yields back.

The gentlewoman from California is recognized.

Ms. LOFGREN. Thank you very much. And first, let me offer my regrets for not being here at the beginning of the hearing, because I would have liked to have given a word of welcome to two of the witnesses who represent companies located in Silicon Valley, which I represent in the House. And that is both the Facebook witness and, of course, Symantec, both companies that employ many of my constituents. So, welcome here.

As I think about the risks involved in use of technology, I think of them in at least two categories. One, there is really nothing the government can do about.

I mean, if you decide to post your home address on Facebook and not limit who sees it, and then say, "Oh, by the way, I am on vacation for a month," it is like saying, "Please come burglarize me." So that is really an education issue that the government, and I really think the companies, are not responsible for. It is a matter of Americans understanding what they are doing.

There is a second issue, which is really a technology issue, which is allowing people the opportunity to have their rights respected. And I wanted to address, really, two questions, probably three questions, to Mr. Sullivan.

It has been mentioned here by EPIC, certainly a very well regarded organization that I have supported for years, that the settings are too tough and maybe not fully implemented. And I have actually complained, most recently a few months ago, not that you couldn't do it, but that it was too complicated.

And I suggested to the Facebook people I met with that you need not the Geek Squad but the Granny Squad. I mean, design it for, you know, a grandma in the Midwest so she can understand it and make it do what she wants with very simple clicks.

Do you think you have accomplished that yet? I realize this is really still a startup. I mean, even though you are at half a billion, you know, it is 6 years, and you are still growing.

Mr. SULLIVAN. Thank you very much for that question. And I think that it is something that we spend time thinking about every day, because I think your goals and our goals are aligned on this issue. We want people to understand and be able to use the controls because they will feel good about our service. And I think that the controls that we have in place now are the best we have ever had.

And as I mentioned earlier, the controls that we launched as a result of the feedback that we received from people like you, we think that we have dramatically simplified so that you—you know, as you know, before, you had to go to five or six different screens

to cover all the different types of sharing that you could do, and now you can manage all of that on a single page.

Ms. LOFGREN. And maybe that you are not at liberty, and this may not be a fair question, but if EPIC had some further suggestions for you to consider to simplify this, would you welcome those suggestions?

Mr. SULLIVAN. We certainly would. In fact, I would like to mention that both before the large rollout that we did last fall of trying to engage users on new privacy settings, and during the spring we did reach out to a large number of organizations outside the company that asked for feedback, and we received feedback from a number of highly regarded organizations across the nonprofit and public and private sector.

Ms. LOFGREN. Let me ask you two other questions, and this is one really having to do with people who decide that Facebook is too much trouble and they wanted to delete their account.

I mean, if you post somewhere else, I realize that is on somebody else's Facebook and you can't necessarily get rid of that. But if you close your own account, is every whisper of information that you have lodged with Facebook erased with that?

Mr. SULLIVAN. Yes.

Ms. LOFGREN. And finally, I would like to make a suggestion, unless this has already been implemented. There are times when things go wrong.

For example, somebody has failed to take appropriate steps to safeguard their Facebook account, and it gets hijacked. There is nobody to call. I mean, you can send an e-mail, but it takes a long time to be sorted out. Are there plans in place to have kind of a rapid response when things of that nature occur?

Mr. SULLIVAN. Yes. It is another area where we are continuing to innovate. What we have done is we have placed "Report" buttons across our site, and you should be able to find them on basically every single page. And we have put those buttons in places where we think that you are most likely to run into a problem and would want to report something. And the "Report" button opens up a dialogue.

And like you said, I think in the old days of the Internet, companies would have a single e-mail address, and all of the issues would come into one big bucket, and then you have to have someone sort it. The way we do it now is, during the report process, we have some very easy drop-downs where a user can specify what the specific issue is. And that directs it into a prioritization queue.

And so, for example, the most serious issues we try and get to within, you know, hours, most frequent——

Ms. LOFGREN. What would a serious issue be, for example?

Mr. SULLIVAN. So, an identity theft or cyber-bullying, or a threat to life or a potential suicide discussion, or something like that.

Ms. LOFGREN. Okay. Well, that is more serious than hijacking a Facebook page. Where would that fall in your priority list? How long would it take to respond to that, do you think?

Mr. SULLIVAN. I think probably within 24 hours, but——

Ms. LOFGREN. If I told you it was 3 weeks, would you be willing to look into it?

Mr. SULLIVAN. I certainly would like to look into it.

Ms. LOFGREN. I would appreciate that.

I realize my time is just about over, but before I did, I just want to, since the Chairman didn't get his rebate, I would like to say I just bought a Symantec product that I have installed on my home computer, and it is protecting me from viruses and malware, and I appreciate it very much, and love your products.

And I yield back.

Mr. PASQUA. Thank you.

And Member Gohmert, I am sorry we lost you as a customer. I hope we can win you back. But most importantly, I hope you are using some sort of protection on your machine.

Mr. QUIGLEY. The gentlewoman's time has expired.

Mr. Goodlatte from Virginia is recognized.

Mr. GOODLATTE. Thank you, Mr. Chairman.

Folks, welcome. I missed most of your testimony because I had to go deal with another Committee and some legislation I had there. I apologize for that.

But I did want to ask Mr. Snow, with the many Federal agencies involved in some aspect of identity theft or related cyber-crimes, is there ever confusion on the part of the private industry sector as to what agency they should call for assistance or to report a breach? Do you have some kind of a clearinghouse, or——

Mr. SNOW. Yes, sir. Our most powerful clearinghouse is the agent and investigators that are in the field. So all the different agencies, federal, state and local, and our international partners are out pushing the outreach programs.

We have three very strong outreach programs—the Internet Crime Complaint Center, which is a public-private partnership; our InfraGard program, and then our computer education and development unit, which go out, along with our domain entities, as to other Federal agencies and state and local partners to let people know, if you have crime or you have crime reporting, to come and talk to us.

The clearinghouse actually takes place back in the investigative agencies along with where the different jurisdictional lines reside. So for instance, if you had a problem, an Internet breach, you could Google it. You would come up with probably about five or six places to go report.

If you were directed to the FBI Web site, FBI.gov, you would be directed back to the Internet Crime Complaint Center. It would talk to you about what that crime complaint center does, what it can provide you, and how to report. It would have a very accessible link there.

The Internet Crime Complaint Center, if you started there, would have the same issue and reporting mechanism. And then, we have an educational partnership that is called www-lookstoogoodtobetrue, and you would be able to go there, also.

An important part of the education, and I know we have talked about the education, is that all three of these sites, individuals that are suspecting that they may be subjects, or potential subjects, which everybody is, of Internet fraud or computer hacking, can sign up for informational alerts that will come to whatever piece that you have.

Mr. GOODLATTE. Thank you.

Mr. Sullivan, let me follow up on the question from Ms. Lofgren regarding the privacy issues there. Can you explain Facebook's privacy transition tool? How does this process ensure that users are considering privacy issues in evaluating their own security settings?

Mr. SULLIVAN. Certainly. So, last December, we took on I think what was probably an unprecedented event in the history of the Internet, and that is that we tried to engage every single one of our users and make them think about privacy.

And so, what we did was we put that wizard, which was a page that talked about privacy and laid out your settings and what we were recommending as settings, in front of every single user, and we simply wouldn't let you use the service again until you walked through these pages and said, "I want to do it this way."

And so, that was quite a massive undertaking, and it got quite a bit of attention, and we were pleased in both regards because we saw that users engaged with this wizard, that they made decisions, that they talked about privacy, they thought about privacy, they thought about what they put on the site before. And they have continued to use the privacy settings after that day even more than they ever did.

Mr. GOODLATTE. What is instant personalization? I know that Facebook has become a platform upon which you have invited other vendors to build various tools that they can utilize as members of Facebook. What assurances do you have that partner sites in this program have sufficient protection to safeguard Facebook users?

Mr. SULLIVAN. Sir, from the security standpoint, we focus on a number of different things. This is a beta program that—only used on a very limited number of carefully selected partner sites at the moment.

And we have done a couple of different things. We have done some external auditing of their security measures. I manage an information security team that has investigative experts who understand the different types of vulnerabilities the Web sites have. We have made suggestions. We have had dialogue with their internal experts.

And then, we also on the security side, we make suggestions for requirements to put into the written contracts about the standards that we expect those sites to live up to. So as I mentioned earlier, we are PCI level one compliant, and there are other security standards and acronyms that I won't share today, but are the types of things that we would look for.

Mr. GOODLATTE. One last thing. You indicated in your testimony that you will use legal means to go after people that are behind specific scams. Can you elaborate on this? Is it civil actions that you will pursue, or do you assist law enforcement authorities in pursuit of criminal charges, or both? What are you talking about there?

Mr. SULLIVAN. So our goal is always to prevent something bad from happening. But if it does happen our second goal is to be incredibly aggressive.

And so, I mentioned in my written testimony in a bit earlier a couple of the CAN-SPAM cases that we have brought. And so, in these two cases that have received a decent amount of attention in

the mainstream press, they have actually received even more attention in the forums where the bad guys meet.

And we spend a lot of time on my team in those forums. Like the folks at Symantec do, we spend a lot of time trying to understand what the bad guys are interested in, what they are focused on, which companies they are targeting, what their newest techniques are.

And it has been fascinating for us to take back and share with the company the impact of these spam cases. You know, we certainly aren't going to collect $700 million from Mr. Guerbuez or, you know, $800 million from Sanford Wallace, but we are going to be pursuing them for the rest of their life, and that is a heavy judgment hanging over their heads.

And you see people talking in these forums, saying, "Don't go after Facebook. That is a bad idea." So we do see a deterrent effect in that type of civil action.

Likewise, on the criminal side, we have brought a number of cases to both the FBI and the Secret Service over the last couple of years where we have identified individuals or groups that are attempting to target our users, whether through distribution of malware or through spam or other types of problems like that.

Mr. GOODLATTE. Thank you.

My time has expired. Thank you, Mr. Chairman.

Mr. QUIGLEY. Thank you.

Mr. Deutch is recognized.

Mr. DEUTCH. Thank you, Mr. Chairman.

Gentlemen, I think we need to do a better job of raising awareness among Internet users, particularly children. While most social networking activities are harmless, the fact is there are people who are out there who are going to tell a lie and hurt you.

And whether it is someone seeking easy money or a child predator, when it comes to social networking, these criminals know the game, and they are going to play it. I am deeply concerned about the risks that the predators pose to children, and I believe we need to do more to minimize the risks to children online.

Education is a critical component of crime prevention. As a parent, I am no stranger to the need to talk to children early and often about online predators. Parents must play a critical role to make them understand the risks that are out there.

Now, I applaud the efforts of the FBI, Secret Service and other law enforcement agencies to protect children, but I think everyone would agree, if even one child is victimized, we as a government need to do more. And while we can't promise our children that we are never going to let them down, we can at least commit to not deserting them and focus on what additional tools might be helpful.

To that end, as a Member of the Foreign Affairs Committee, I am particularly interested in the international component of this problem. Criminals thrive in areas where the government is too blind to see. And while this is true of traditional criminal activities, it is particularly true of Internet-based crimes.

So how do we go after criminals who know the rules and purposely set up shop in lawless areas or countries that are willing to turn a blind eye to these activities? I guess, Mr. Merritt and Mr. Snow, I would turn to you for this.

Mr. MERRITT. Sir, I think somebody referenced it earlier, some of the challenges when these crimes originate overseas and they target either U.S. citizens or corporations, and then the financial infrastructure. In addition to some countries that don't have legislation that makes this necessarily a crime in their country, there are other challenges, as well.

I mean, I think law enforcement here in the United States has been able to dispel the myth of anonymity that the computer and the Internet provide to the criminals because we have been successful in many investigations identifying these people.

But you get into lack of legislation, countries that don't have an extradition treaty with the states, the official channels that we normally go through for MLATs and letters rogatory are very cumbersome and time-consuming.

So a lot of it develops—and I will let Gordon speak for himself, but it develops on the relationship that you have with your foreign law enforcement counterparts and what you are able to successfully do with them, because we obviously have limited jurisdiction overseas.

Mr. SNOW. Yes, sir. I will—the comments of Mr. Merritt. The relationship internationally is just completely critical, and in legislation development, which, you know, we don't speak to but Department of Justice does, is also critical, the MLAT, the letter rogatories, the officer-to-officer contact that we have.

And then the private-public partnerships that develop when you talk about child exploitation is critical also. So the National Center for Missing and Exploited Children are really doing some fantastic things in their public-private partnership, along with the International Center for Missing and Exploited Children.

Mr. DEUTCH. Thank you.

Mr. Sullivan, I am looking at the statement of rights and responsibilities on Facebook, which says, very clearly, you will not use Facebook if you are under 13. I would suggest to you that there are more 60-, 70-and 80-year-old grandparents, widows and widowers, with full, rich life histories who are, in fact, 10, 11 and 12 years old on Facebook than you could even imagine.

And I wonder, since Facebook very clearly says it should not be used unless you are 13, what should we be doing? Do we pretend that the younger kids aren't doing it? Is there something Facebook can be doing to make it safer for those younger kids, which is, I think, the approach that makes the most sense to me? And have you tried to track the number of pre-teens who are actually using Facebook, since the numbers must be astounding?

Mr. SULLIVAN. Sir, you are right that our policy is very clear, that we don't want people under the age of 13 to use our service. And we have taken a multi-tiered approach to trying to make that happen. And to the extent that you are aware, or if you become aware of someone under the age of 13, or you know their parents, I would ask that you put them in touch with me or advise them not to use the service until they turn 13.

It is a topic that has received a lot of attention in recent years, how do we address teens and youth online. And the approach we have taken is kind of a three-tiered approach. I think that we do

focus on policy and we focus on education, and then we build tools to try and prevent those under 13 from using our site.

Mr. DEUTCH. I guess just if I may, Mr. Chairman, the last question is there are two approaches. You can devote considerable energy to trying to prevent 11-and 12-year-old kids from using Facebook, or you can acknowledge that there are thousands and thousands of 11 and 12 and 10, and I don't even know how young, kids who are using Facebook, and ratchet up the privacy levels or create a separate area for them. And is that even part of your thinking, or is the focus entirely on keeping them off?

Mr. SULLIVAN. Our focus right now is on keeping them off of Facebook and on making Facebook as safe as possible for that 13 to 18 group that is on the site. And so, I mentioned earlier that we don't have different rules for people in different jurisdictions around the world. We do treat people differently who are under the age of 18 in terms of what we would even allow them to do on the site or the type of information that is even made visible to them.

Mr. DEUTCH. Last question, Mr. Chairman. Do you deny access to anyone—do you scan your members to find those who are clearly describing life experiences in one way on their biography, and then have pictures of little kids, lots and lots of pictures of 10, 11 year olds on their site?

Mr. SULLIVAN. We do have some back-end tools and algorithms that we use. We also rely on a considerably passionate user community who is very happy to report other people to us. And finally, we do use technology to, you know, try and identify and make sure that those people aren't on our site.

Mr. DEUTCH. Okay. I think, finally, there is an obligation also, as you work to address all of the concerns, if you know that there are thousands of kids out there that, while the goal may be to keep them off, we should be trying, and you should be trying, to keep them safe, as well.

Mr. SULLIVAN. That is right.

Mr. QUIGLEY. Gentleman's time has expired.

I would like to thank the witnesses for their testimony today. Members may have additional written questions, which we will forward to you and ask that you answer as promptly as you can so that they may be made part of the hearing record. The record will remain open for 1 week for submission of additional material.

Without objection, the Subcommittee stands adjourned.

[Whereupon, at 3:35 p.m., the Subcommittee was adjourned.]

APPENDIX

MATERIAL SUBMITTED FOR THE HEARING RECORD

July 23, 2010

Honorable John Conyers
U.S. House of Representatives
Committee on the Judiciary
2138 Rayburn House Office Building
Washington, DC 20515-6216

Dear Chairman Conyers:

Thank you for your letter of July 22, 2010 regarding the upcoming Subcommittee on Crime, Terrorism, and Homeland Security hearing on "Online Privacy, Social Networking and Crime Victimization" on Wednesday, July 28, 2010. I appreciate your leadership on these issues, as well as the leadership of Subcommittee Chairman Bobby Scott and Ranking Member Louie Gohmert. As my colleagues in DC mentioned to your staff, I have several longstanding prior commitments on the day the hearing will take place.

Although he is scheduled to be on vacation next week, I have asked my colleague Joe Sullivan, who is Facebook's Chief Security Officer, to be prepared to attend the hearing in my absence if you would still like a Facebook representative to participate. As a former Assistant U. S. Attorney and the senior Facebook executive with day to day responsibility for the issues the hearing will likely cover, Joe is exceptionally knowledgeable, and we believe his frontline perspective would potentially be valuable to the Members of the Subcommittee. He will also be able to discuss some of the outstanding work Facebook is doing with law enforcement.

I also want to personally assure you that our entire team at Facebook appreciates the importance of the issues you are examining. Later today, my colleagues will be sending you a response to your request for more information on the privacy practices we've implemented at Facebook and I very much look forward to any feedback you have. These answers expand upon the conversations my colleagues have been having with your staff over the past few weeks.

Thank you for your understanding, and I look forward to speaking with you in person and continuing a good working relationship with you and others on the Committee. Finally, I'd like to extend an open invitation to you and any of your Committee members to visit our offices in Palo Alto so that you can learn more about our mission and efforts in the areas in which you are interested.

Sincerely,

MZ

Mark Zuckerberg

facebook

Address: [illegible]
Telephone: [illegible]
Fax: [illegible]

facebook

meaningfully engage with the concept of privacy and consider whether their settings accurately reflected their preferences, in a manner that had never occurred before, on or off the Internet.

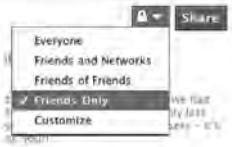
Choice and Control

Since our goal is to ensure that Facebook users understand what they are sharing and with whom, it should be no surprise that we offer users choice and control over how their personal information is shared with other users, and with developers of applications and websites through Facebook Platform. We explain our policies and practices with respect to both of these categories below, as well as our policies for advertisers, who never receive any personal information about individual users.

Users

As indicated above, whenever Facebook adds new features to the site, we also provide additional controls so users can determine what they want to share, with whom, and when. Over the years, as we introduced new features and controls, our privacy settings grew increasingly complex. As a result, early last year we started working on efforts to simplify them, while at the same time offering users enhanced and real-time control over how they share content on Facebook. These efforts culminated in significant changes to our service, including a contextual privacy control and a one-click sharing control.

Contextual Privacy Control. Our contextual privacy control allows users to control who can see each and every one of their posts at the time they share the information. We recognize that a user might want to share some information more openly (such as a comment about Haitian earthquake relief) and other information to a narrower audience (such as a photo of their grandchild). To exercise this control, a user simply clicks on the lock icon before he or she shares the information and select the intended audience:



We also designed the tool to include a warning to make sure users are aware of what it means to share their information with "Everyone." The first time they decide to share content using that setting they see the following:

facebook

One-Click Sharing Control. In recognition of the complexity associated with the number of privacy controls we introduced, Facebook deployed a new, simplified control for sharing that helps people control more than twenty categories of information with just one click, while at the same time enabling more granular controls for those users who prefer to control the information they share on Facebook in a more customized way. With this setting, users can easily restrict the information they share in the future as well as information they have shared in the past.[1]

Advertisers

Online advertising is a critical component of the economic growth that the Internet has spurred, and it enables us to offer Facebook for free. Facebook provides advertisers only with anonymous, aggregated data, such as the number of users in a particular state who clicked on a specific ad. We ask advertisers to identify the high-level characteristics of users they wish to view their ads – such as age, gender, or location. Facebook then itself automatically distributes those advertisements to the appropriate audience without ever providing any personal information about users to the advertiser.

Platform Developers

We introduced Facebook Platform in 2007 to enable developers to offer innovative and social experiences to Facebook users. Since then, it has given rise to a torrent of innovation and investment, leading Facebook to become one of the leading platforms, with over a million developers. As Facebook Platform has evolved so have the controls we offer users who want to share their information with these third-party developers:

Granular Data Permissions. In June, we became the first platform provider to require developers to obtain "granular" data permissions before being able to access information concerning a user. Developers on the Facebook Platform are now required to tell users which specific categories of information they need to provide their application and to obtain user permission for each category before the information can be accessed. This innovative permissions model provides users more control

[1] The only exception to this is information they have shared with a narrower audience using the contextual privacy control.

1601 South California Avenue, Palo Alto, California 94304
650.543.4800 - tel 650.543.4801 - fax

facebook

than they have on other leading application platforms, while allowing developers to continue the vibrant innovation that has marked the Platform economy.

Instant Personalization. Likewise, in April of this year, Facebook launched Instant Personalization, a pilot program that allows users to have a more robust and personalized experience with partner sites, currently including Yelp, Pandora, and Microsoft's docs.com. Facebook has worked diligently to ensure that these partners adopt and enforce adequate protections for personal information, and individuals receive multiple opportunities to learn about and choose to participate in Instant Personalization. When we rolled out the program, we made sure users had ample notice and an opportunity to choose not to participate, both on Facebook and on our partners' sites. Before experiencing Instant Personalization, users see a message on the top of their Facebook home page advising them of the program and giving them the opportunity to decide whether they want to experience it.

If they choose not to participate, they will not experience Instant Personalization when they visit any partner site. Similarly, when a user visits one of our pilot partner sites for the first time, they are presented with contextual notice by way of a prominent blue bar at the top of the page.[2] In addition to disclosing the program, the bar gives the user the ability to block the site from offering a personalized experience to that user. In addition, if a user chooses not to participate in Facebook's Platform entirely, this automatically blocks any participation in Instant Personalization sites. Facebook also has added a specific control that can be accessed from a user's Facebook page that blocks participation in all Instant Personalization sites.

Thank you again for the opportunity to provide you with information about how users' share information on Facebook, and the important innovations we have brought to user control. We are available to provide any additional information or assistance.

Sincerely,

Timothy Sparapani
Director, Public Policy
Facebook

[2] If a user is not logged in to Facebook or has turned off Instant Personalization, they will not experience instant personalization (or see the blue bar) on any partner site.

1601 South California Avenue, Palo Alto, California 94304
650.543.4800 - tel 650.543.4801 - fax

ONE HUNDRED ELEVENTH CONGRESS

Congress of the United States
House of Representatives
COMMITTEE ON THE JUDICIARY
2138 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515–6216
(202) 225–3951
http://www.house.gov/judiciary

May 28, 2010

Mr. Mark Zuckerberg
Chief Executive Officer
Facebook, Inc.
1601 S. California Ave.
Palo Alto, CA 94304

Dear Mr. Zuckerberg:

I write about Facebook's practices and policies concerning the sharing of personal information of its users with various third parties.

Specifically, we would appreciate a detailed explanation of the information about Facebook users that your company has provided to third parties without the knowledge of the account holders – particularly in circumstances in which the users did not expressly opt for this type of information sharing. Please explain your prior policies with respect to user consent for information sharing, and with whom any such information was shared. Also, please detail how the new policies Facebook is adopting differ from past practices, including whether the burden is on the user to opt in or opt out of the relevant privacy settings.

Thank you for assisting the Committee with our goal of enhancing the personal privacy of all Americans.

Sincerely,

John Conyers, Jr.
Chairman

cc: The Honorable Lamar Smith

CBSNEWS

Crimesider July 12, 2010 1:05 PM

Facebook Panic Button? UK Users Get Link to Child Safety Program

Posted by Edecio Martinez

(CBS/AP)

LONDON (CBS/AP) A new application was launched on Facebook on Monday by a British child protection agency. The application allows young users to report worrying or inappropriate behavior to child protection authorities.

The Child Exploitation and Online Protection Center said their application - called "ClickCEOP" - gives children between ages 13 to 18 a place to report instances of inappropriate sexual behavior and other issues.

The application is not a so-called panic button, and doesn't connect users immediately to authorities, the organization said. Rather, the application appears as a tab at the top of a user's profile once it is added, and clicking it provides links to the organization's website where bullying, sexual behavior or other online problems can be researched and, if necessary, reported.

An advertisement for the application will appear on the home pages of Facebook's British teenage users. It is aimed at kids in Britain, but spokeswoman Vicky Gillings said harassment

reported by teenagers in other countries would be passed on to law enforcement in those places.

Jim Gamble, the organization's chief executive, said the application could help reassure parents whose children use the site, because "we know from speaking to offenders that a visible deterrent could protect young people online."

Last month in the United States, Facebook - the world's largest online social network - and the National PTA announced plans to build a program to promote Internet safety through a set of tools and resources for kids, schools and parents.

What's Your Take? Shocking2Infuriating5Satisfying7Ridiculous8
Connect with CBS NewsFacebookTwitterX

The New York Times

May 2, 2010

Stolen Facebook Accounts for Sale

By RIVA RICHMOND

Researchers at VeriSign's iDefense division tracking the digital underworld say bogus and stolen accounts on the Facebook are now on sale in high volume on the black market.

During several weeks in February, iDefense tracked an effort to sell log-in data for 1.5 million Facebook accounts on several online criminal marketplaces, including one called Carder.su.

That hacker, who used the screen name "kirllos" and appears to deal only in Facebook accounts, offered to sell bundles of 1,000 accounts with 10 or fewer friends for $25 and with more than 10 friends for $45, says Rick Howard, iDefense's director of cyber intelligence.

The case points to a significant expansion in the illicit market for social networking accounts from Eastern Europe to the United States, he said.

Criminals steal log-in data for Facebook accounts, typically with "phishing" techniques that tricks users into disclosing their passwords or with malware that logs keystrokes.

They then use the accounts to send spam, distribute malicious programs and run identity and other fraud.

Facebook says it believes that the hacker's claims to control large numbers of Facebook accounts are bogus. The company attempted to purchase accounts as part of its investigation into the incident, said a spokesman, Barry Schnitt. However, "the hacker was unable to produce anything for our buyer," he said.

Facebook's investigators also discovered that "kirllos" has a reputation "for wild claims," he said.

"We would expect iDefense or anyone presenting themselves as a security expert to do this kind of verification (or any verification) rather than just reading a forum post and accepting the claims as fact and publicizing them," Mr. Schnitt said in an e-mail message.

IDefense could not be immediately reached for comment on the legitimacy of the hacker's offer. However, it previously said that it did not purchase any of the accounts as part of its study because that would violate its corporate policy.

Criminals steal log-in data for Facebook accounts, typically with "phishing" techniques that tricks users into disclosing their passwords or with malware that logs keystrokes. They then use the accounts to send spam, distribute malicious programs and run identity and other fraud.

Facebook accounts are attractive because of the higher level of trust on the site than exists in the broader Internet.

People are required to use their real names and tend to connect primarily with people they know.

As a result, they are more likely to believe a fraudulent message or click on a dubious link on a friend's wall or an e-mail message. Moreover, the accounts allow criminals to mine profiles of victims and their friends for personal information like birth dates, addresses, phone numbers, mothers' maiden names, pets' names and other tidbits that can be used in identity theft.

Last summer, Eileen Sheldon's Facebook account was hacked and used to send messages to about 20 friends claiming she was stranded in Britain without a passport and needed money. Ms. Sheldon, who lives in California, had recently been living in London, and one friend, believing the ruse, wired about $100 to the thieves.

Other friends smelled a fraud and warned Ms. Sheldon, who quickly reported the problem to Facebook. She does not know how her password was stolen.

While the accounts that were compromised and offered for sale could be legitimate ones like Ms. Sheldon's, they most likely also included bogus accounts, Mr. Howard said. IDefense did not see the accounts themselves, but the inclusion of many accounts with small numbers of friends suggests the seller could have created fake accounts, perhaps using an automated tool, and sent out blind friend requests.

Many users are eager to amass friends and accept friend requests from people they do not know, even though Facebook discourages it.

Facebook says it has sophisticated systems to defeat fake accounts, including tools for flagging them when they are created so they can be investigated. This allows Facebook to "disable them before the bad guys get very far," a spokesman, Simon Axten, said.

Facebook also monitors for unusual activity that is associated with fake accounts, like many friend requests in a short period of time and high rates of friend requests that are ignored. It also investigates reports of suspicious users .

The relatively low asking prices for the Facebook accounts points to the fact that Facebook accounts do not translate into instant profit. "The people that buy these things are going to have to do more work to make money," Mr. Axten said.

The Washington Post

Facebook's test: Building on ad revenue

By Cecilia Kang
Washington Post Staff Writer
Saturday, July 24, 2010; A08

Facebook may be growing like gangbusters, but the question clouding the storybook rise of Silicon Valley's latest phenomenon is whether it can figure out how to make money at the same pace.

And although the social-networking site gets a daily flood of new users around the globe, Facebook's long-term success might be challenged by something at the heart of its core business: sharing information.

The site, which passed 500 million users this week, says it's generating enough revenue from advertising to cover its costs. The company is privately held but has its sights on going public one day. It doesn't charge its users, and chief executive Mark Zuckerberg said this week on ABC News that it never will. (Washington Post Co. Chairman Donald E. Graham sits on Facebook's board of directors).

Facebook's lifeblood is the exchange of information -- people making more online friends and trading more pictures, news stories, music and one-line mood updates -- which also happens to be sheer gold for advertisers. Experts say the company treads

a delicate line in getting its users to share more information without alienating them through overexposure.

Federal regulators and privacy groups say the company has been testing the limits of consumer privacy online, and have suggested establishing clearer guidelines for such sites.

"Facebook is in a conundrum," said Jeremiah Owyang, an industry analyst at San Francisco-based Altimeter Group. "The promise they've made is to be closed, or restricted, on who can see what. But the more information they make available to outside networks, the more monetization they have."

Facebook, meanwhile, says its business strategy doesn't rely on selling information about its users. The company says it doesn't give user data directly to advertisers but instead places ads from its partners on the pages of users based on its own analysis of aggregated demographic information.

When the firm shifted its policy on user information in December, exposing some data about users more broadly on the Web, critics said the move was intended to generate more revenue from advertisers who want to tailor ads to specific profiles of Facebook users. But Facebook said users get more out of the social-networking site when they reveal more about themselves to others. If they don't want that, they have the option to keep information such as their sex, education, religious beliefs and social connections under wraps.

"There's a big misperception that we're making these changes for advertising," Zuckerberg said on a media call this year, when

the company announced it was dialing back some of the changes. "Anyone who knows me knows that that's crazy."

The issue of online privacy has gained more attention this past week, with two bills in motion in the House that seek for the first time to create rules for how Web sites can collect and share information about their users to advertisers and third-party marketing sites. One bill, introduced this week by Rep. Bobby L. Rush (D-Ill.), seeks to give the Federal Trade Commission the authority to create a policy on Internet privacy. The Senate Commerce Committee will hear next week from FTC and Federal Communications Commission leaders, as well as representatives from Google, Apple, Facebook and AT&T, in a hearing about privacy.

○