

THE CIP REPORT

Privacy

| | |
|--------------------------------------|----|
| DHS Privacy Advisory Cmte . | 2 |
| Spyware | 3 |
| Spyware Legislation | 4 |
| Federal Privacy Officers | 5 |
| Privacy in the Government .. | 5 |
| Legal Insights | 6 |
| P2P, E-Filing, and Identity Theft .. | 7 |
| Online Privacy Fraud | 8 |
| Tips from the IFCC | 8 |
| Security vs. Liberty | 9 |
| Privacy Oversight Board | 12 |
| CSIA / CIPP Symposium | 13 |

Newsletter Editorial Staff

John McCarthy, *Director / Principal Investigator*

Jessica M. Milloy, *Special Assistant to the Director*

Amy Cobb, *Senior Project Associate*

Jeanne Geers, *CIP Report Editor*

Ken Newbold, *JMU Outreach Coordinator / JMU CIP Program Liaison*

Contact: cipp01@gmu.edu
703.993.4840

If you would like to subscribe to *The CIP Report* please click [here](#).

Director's Message

How much privacy can we and should we really expect? If we left our doors and windows wide open, or gave our house keys to strangers, would we expect any more privacy than when we engage in high risk behaviors online? As our expectations and online consumption of ever increasing services and possibilities continue to expand, the price we pay for convenience is also growing. As new legislation, consumer education campaigns and media coverage race to keep pace with the spread of new phishing schemes, hacking attempts and disclosures of consumer or employee information, how vulnerable have we become?

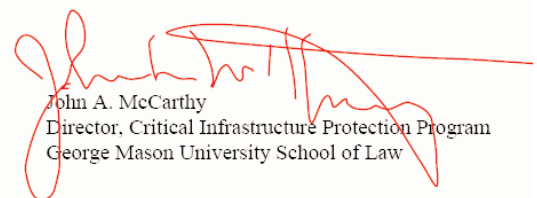
Despite the realities of the vulnerabilities we face, rarely do we as individuals consider ourselves a likely victim. However, the recent security breaches at SAIC and here at George Mason University exposed confidential employee information, rather than consumer information we knowingly gave to online vendors. Although we have all heard stories of identity theft and online fraud, each new incident comes as an unpleasant surprise and a reminder that with each new technological innovation comes responsibilities and vulnerabilities that require additional diligence. Being concerned about privacy doesn't mean that we stop using the Internet as an access point for financial transactions or information sharing; rather it requires that

we reexamine the legal protections, forensic capabilities in targeting criminal activities, as well as our own potentially high risk behaviors.

This issue of *The CIP Report* provides some insight into privacy concerns and the legal, social and policy discussions surrounding the protection of our personal information. Many of our current privacy laws were created to deal with the physical, not cyber world, and while they have clear applications, they do need further development. We have highlighted proposed legislation to combat spyware and those that seek unauthorized access to personal data, while examining the application of HIPAA and Sarbanes-Oxley, which place responsibility on those that fail to protect the data they hold.

To further this conversation, the CIP Program and the Cyber Security Industry Alliance are holding a three part symposium on the emerging landscape of cyber security legislation and compliance, beginning in late March. These three events, focused on state, federal, and international levels, will convene thought leaders and practitioners to explore the complex legal and technology compliance requirements. If you are interested in joining this discussion, registration information is provided within this issue.




John A. McCarthy
Director, Critical Infrastructure Protection Program
George Mason University School of Law

DHS Announces Data Privacy and Integrity Advisory Committee

The Department of Homeland Security (DHS) recently announced the appointment of twenty members to the Data Privacy and Integrity Advisory Committee (DHS Privacy Advisory Committee). This newest federal advisory committee to DHS was established to provide external expert advice to the Secretary and the Chief Privacy Officer on programmatic, policy, operational, and technological issues that affect privacy, data integrity, and data interoperability in DHS programs.

"This Committee will provide the Department with important recommendations on how to further the Department's mission while protecting the privacy of personally identifiable information of citizens and visitors of the United States," said Nuala O'Connor Kelly, the Chief Privacy Officer of the Department of Homeland Security. "The diversity of experi-

ence and perspectives represented by this Committee will play an important role in advancing the national discourse on privacy and homeland security."

The members of this Advisory Committee have diverse expertise in privacy, security, and emerging technology, and come from large and small companies, the academic community, and the non-profit sector. The members also reflect a depth of knowledge on issues of data protection, openness, technology, and national security. Members for the first term will serve staggered terms of two years, three years, or four years and all subsequent members will serve for a period of four years.

Critics say that the panel is missing representation from some of the most active privacy rights groups, including the Center for Democracy

Nuala O'Connor Kelly is the Chief Privacy Officer for DHS. She has served in this office since April 2003. Her position was the first statutorily created Privacy Officer in the federal government.



and Technology and EPIC, the Electronic Privacy Information Center. EPIC's executive director did not apply for membership on the panel, while CDT's president did apply but was rejected.¹

The first Privacy Advisory Committee meeting will be held on April 6, 2005 in Washington, DC. Additional information on upcoming events will be posted on the DHS Privacy Office website, www.dhs.gov/privacy. ❖

¹ Starks, Tim. "New DHS Privacy Panel Has Everything-Except the Loudest Privacy Advocates." *CQ Homeland Security*, 23 Feb 2005.

Members appointed for the inaugural term of the DHS Privacy Advisory Committee are:

Joseph Alhadeff, Vice President and Chief Privacy Officer, Oracle Corporation, Washington, DC

Ramon Barquin, President, Barquin International, Bethesda, MD

J. Howard Beales, Associate Professor, The George Washington University, Arlington, VA

D. Reed Freeman, Chief Privacy Officer and Vice President, Claria Corporation, Arlington, VA

James W. Harper, Editor/Executive Director, Privacilla.org & Director of Information Policy Studies, Cato Institute, Washington, DC

Kirk Herath, Chief Privacy Officer & Associate General Counsel, Nationwide, Columbus, OH

David A. Hoffman, Group Counsel and Director of Privacy, Intel Corporation, Hillsboro, OR

Lance Hoffman, Distinguished Research Professor, The George Washington University, Washington, DC

Tara Lemmey, Chief Executive Officer, Lens Ventures, San Francisco, CA

Joseph Leo, Vice President, SAIC, Vienna, VA

John Marsh, Distinguished Professor of Law, George Mason University School of Law, Winchester, VA

Joanne McNabb, Chief, Office of Privacy Protection, California Department of Consumer Affairs, Sacramento, CA (Continued, Page 10)

Spyware: Good Business Cents or Trespassing?

Bryan Day

Faculty Research Associate, School of Public Policy
George Mason University

Where privacy, economics and technology intersect, the debate about spyware begins - that frustrating software annoyance that has infiltrated the computers of 80 percent of Internet users, according to a 2004 America Online survey. State and federal legislators have taken notice and since mid-February, more than a dozen states and the U.S. Congress have proposed legislation to stem the tide of these online headaches. At the federal level, Representative Mary Bono (R-CA) introduced the Securely Protect Yourself Against Cyber Trespass Act (SPY ACT/H.R. 29) which gives computer users the opportunity to give consent before spyware purveyors can install their product, requires that spyware be easily removable, and gives enforcement power to the Federal Trade Commission. The act recently passed the House Trade and Consumer Subcommittee. A competing bill is the Internet Spyware Prevention Act (I-SPY Act of 2005/H.R. 744) introduced by Representative Bob Goodlatte (R-VA). This bill makes criminal the installation of spyware on non-consenting Internet users. Violators face fines and even jail time.

A major challenge to any legislative effort is that spyware is not easily defined, even by those

within the industry. Generally, most lawmakers define spyware as any software that is downloaded onto a person's computer without their knowledge or consent. However, even this definition may be too broad to be effective.

Today's Internet is a public good; most websites are non-excludable and have non-rivals in consumption. Web surfers have become accustomed to accessing an endless supply of information without charge. However, as any good business person knows, "there is no such thing as a free lunch." So who is paying for this modern day public good? The truth might surprise you - you are - through files and programs that enter your computer without your permission and store certain information that is useful to web-based businesses. Companies pay top-dollar for this information, and herein we find the Internet's main source of revenue - its dollars and cents.

At one end of the spectrum are 'cookies,' the poorly understood files left behind on one's computer after visiting a website. Cookies make navigating the Internet easier and faster by retaining important data about you which creates the incentive for businesses to offer their website information at no cost. The

information gathered is often no more than the number and nature of visitors to a website. This informa-



tion is critical data for businesses that pay for their website operations through the sale of advertising. Some cookies, however, store more information than is needed and are considered by some to be an invasion of privacy. Any legislative effort to protect Americans against spyware that prohibits all cookies would run into tremendous opposition from business interests and would have a profound effect on cyber commerce.

Adware is another class of passively installed computer technology. It is a benign type of spyware, and often confused with programs that exist solely for the purpose of identity theft. Adware monitors a user's internet travels and manipulates pop-up advertising to appeal to the user's interests based on past website visits. This information is very appealing to businesses and plays a critical *(Continued, Page 4)*

Spyware Legislation Active in the House

On March 9, Representative Mary Bono's (R-CA) spyware legislation passed in the House Energy and Commerce Committee. H.R. 29, the Securely Protect Yourself Against Cyber Trespass Act (SPY ACT), aims to protect individuals from unknowingly downloading and activating spyware by requiring that consumers receive a clear and conspicuous notice prior to the transmission of spyware programs. The bill includes provisions to prohibit unfair or deceptive behavior such as keystroke logging, computer hijacking and the display of advertisements that cannot be closed, according to Bono.

An amendment was offered in subcommittee to H.R. 29 to, among other technical changes, clarify that cookies (passive text files), including tracking cookies, are not subject to the provisions of the bill. The bill directs the

Federal Trade Commission (FTC) to issue a report regarding cookies, including third-party cookies, that studies the behavior of cookies as technology advances. Another amendment in committee steps up enforcement against phishing schemes.

The technology industry says the bill could restrict important security programs and might constrain legitimate businesses that rely on programs that may be considered "spyware" by some definitions. Last summer, the Information Technology Association of America sent a letter to the Committee, warning that the legislation (then H.R. 2929) could "generate a veritable blizzard of legally mandated pop-up notices that only a lawyer would love. The proposed legislation goes beyond addressing the problem of Spyware to create a new Federal regulatory regime at

the Federal Trade Commission for online software distribution."

Meanwhile, Representative Bob Goodlatte (R-VA) recently reintroduced competing legislation, the Internet Spyware (I-SPY) Prevention Act of 2005. H.R. 744 would impose criminal penalties for tapping into computers to steal personal information or damage hardware. The legislation also authorizes \$10 million to the Department of Justice to combat spyware and phishing scams. "Phishing" scams typically involve the use of fake e-mail messages and websites to lure consumers into providing bank account information, credit card numbers and other personal information. These fake e-mail messages and websites are often indistinguishable from the real ones and often request account information from consumers. ❖

Spyware (Cont. from Page 3) role in e-commerce.

At the other end of the spectrum are the most pernicious of spywares. These programs track a user's every keystroke and transmit each move back to strangers, perhaps revealing pass codes and other very sensitive information. In addition to the tremendous invasion of privacy these programs represent, they are also a significant drain on computer speed and memory often causing machines to stop functioning entirely - all without prior consent from the owner.

When legislators discuss remedies to curb passive computer intrusions such as spyware, they find the phenomenon hard to understand. One serious concern is to ensure any legislative efforts to ban spyware do not have the potential to preclude legitimate programs that underwrite the Internet. Such examples would be the automatic updating of Windows XP and most anti-virus software. Would Microsoft need to seek advance permission from all of its product users before making available a patch to fix problems in its ubiquitous Window's operating system or the

popular Internet navigational software, Explorer? Would anti-virus software companies need to notify customers and have their approval each time an auto-update of their program was to occur?

Some in the legal community have suggested that we already have protections against spyware - the laws against trespass and nuisance. Trespass is the wrongful injury or interference with another's property. Nuisance is the interference with the enjoyment of (Continued, Page 14)

The History of Chief Privacy Officers in the Federal Government

Excerpted from the statement of James X. Dempsey, Executive Director, Center for Democracy and Technology, before the House Judiciary Cmte Subcommittee on Commercial and Admin Law, 2004

For years, many federal agencies have had "Privacy Act Officers." In some agencies, this has actually been a part-time job. Privacy Act Officers often spend much of their time not on privacy issues per se, but in dealing with requests from individuals who want to see their government records under the access provisions of the Privacy Act. In addition, these officers usually are also responsible for the other major records disclosure law, the Freedom of Information Act. Privacy Act Officers, despite their title, have no statutory basis in the Privacy Act. There is no mechanism for including them in internal deliberations on matters affecting privacy. They are often mid-level career officials and do not have the ability to intervene at a policy level even when a major privacy issue comes to their attention. They are often brought into discussions about a program only at the last minute to draft a notice required under the Privacy Act when the government creates or changes a "system of records," but that notice generally serves no role in shaping policy.

Realizing that this system was not effective, the Clinton Administration in 1998 required all agencies to "designate a senior official within the agency to assume primary responsibility for (Continued, Page 10)

Privacy in the Federal Government

Privacy Officers

The fiscal 2005 omnibus appropriations bill requires all agencies to appoint chief privacy officers. The provision says that the officers must create privacy policy and data protection rules that assure that technology does not "erode privacy protections relating to the use, collection and disclosure of information."

The privacy officers are required to conduct privacy impact assessments, prepare annual reports to Congress on anything that affects privacy, including complaints of violations of the Privacy Act, and help design training programs for agency employees. The bill gives agencies one year to implement comprehensive privacy and data protection strategies.

Congress and the administration have disagreed over the role of privacy officers for several years. The White House successfully had a privacy officer requirement removed from the 9/11 Intelligence Reform bill. And administration lawyers are examining whether the omnibus appropriations language is applicable to the entire federal government. The language was placed in Title V of the act, which generally applies to the appropriated agencies, while Title VI applies governmentwide.

Meanwhile, OMB issued a memorandum to executive agency heads in February asking for the designation of a "senior official

who has the overall agency-wide responsibility for information privacy issues." The memo states that the agency's Chief Information Officer may perform this role. Perhaps in response to past criticism that privacy officers are rarely senior enough to champion privacy issues in the policy development stage, the OMB guidance calls for "senior agency officials" who have a "central policy-making role in the agency's development and evaluation of legislative, regulatory and other policy proposals which implicate information privacy issues, including those relating to the agency's collection, use, sharing, and disclosure of personal information."

Back on the Hill, Representative Tom Davis (R-VA) has introduced bills to repeal the chief privacy officer language in the omnibus appropriations or to make the officers report to agency CIO's. According to Davis, the language "merely creates a layer of bureaucracy that contradicts existing federal information policy currently executed by the CIOs... Furthermore, the section attempts to address information security concerns that are already addressed in the Federal Information Security Management Act, the Clinger-Cohen Act, the E-Government Act and the Paperwork Reduction Act."

Privacy Impact Assessments

The E-Government Act of 2002 requires agencies to submit Privacy (Continued, Page 14)

Protecting Privacy in a Networked World

by Randy Jackson, J.D.

Senior Legal Researcher, CIP Program

Privacy in the cyber world continues to be of crucial importance to anyone using the Internet and/or computer-based data storage and maintenance. For many people the ability to protect their privacy while still taking advantage of the many commercial and personal opportunities presented by online interactions has become a task made ever more difficult by the increasing sophistication of those attempting to penetrate information sources. Perhaps the leading player in the anti-privacy theatre is Spyware and its various manifestations. Congress is concerned with this situation and has moved to quickly pass anti-Spyware legislation. H.R. 29, known as the "Securely Protect Yourself Against Cyber Trespass Act" (SPY ACT), sponsored by Mary Bono (R-CA), was reintroduced on January 4, 2005, after having been passed last year in the House as H.R. 2929. This bill imposes civil penalties for the transmission through Spyware of data that may be used to personally identify an individual.

Similarly, in 2004 Congress passed H.R. 4661, the Internet Spyware (I-SPY) Prevention Act of 2004, sponsored by Robert Goodlatte (R-VA) which enacts criminal penalties for "[i]llicit indirect use of protected computers,"

but does not specifically mention data leading to the personal identification of an individual.

Both of these pieces of legislation reflect Congress's awareness and desire to address the expanding threat of the invasion of privacy through Internet Spyware. With identity theft growing throughout the US economy (through elec-

With the tremendous dependence of the US economy on electronic systems both as a means of commercial transactions as well as the main repository for data held by individuals and public and private institutions, the government will be expected to create a legal regime under which those who try to undermine the system... are effectively stopped.

tronic as well as more traditional means), it has become increasingly urgent for the legal system to create recourse for those trying to escape the danger presented by Spyware and other "illicit indirect use of protected computers." With the tremendous dependence of the US economy on electronic systems both as a means of commercial transactions as well as the main repository

for data held by individuals and public and private institutions, the government will be expected to create a legal regime under which those who try to undermine the system, through methods like Spyware, are effectively stopped.

From the other direction, legislation relevant to this area includes HIPAA and Sarbanes-Oxley in terms of the transmission, processing and compilation of data in a secure fashion; and California's passage of Senate Bill 1386 which places the burden on businesses, no matter where they are based or where they process information, to take "adequate measures" to protect the personal information of California residents. Each of these creates legal consequences for those who fail to adequately protect their private data as opposed to the Spyware legislation which is aimed at punishing the perpetrators themselves.

Interestingly, in the case of HIPAA and Sarbanes-Oxley, neither bill was written with cyber security or the protection of electronic privacy explicitly in mind. Yet as is often the case, the ever accelerating forward march of the e-world has overtaken previous action and is now shouting for a response to new threats to privacy and the system underlying it. ❖

Stop, Thief!: How Peer-to-Peer and Electronic Tax Filing Cause Identity Theft

By John Edgell



It's tax-filing season, that dreaded time of the year where forms, figures and finances converge in one headache-inducing exercise

meant to keep the American government's lights on.

This year, the IRS and state governments are again touting electronic filing as the means to reduce their end of the headache: the management of a mountain of nearly 120 million tax filings. Enticed with the incentive of faster tax withholding rebates, the American taxpayer's responding: it's estimated that more than half of all American households will file their tax forms with the click of a mouse this year.

In a short span of ten years, life's certainties of death and taxes will have evolved to death and e-filing.

But for untold millions of unsuspecting e-filers, particularly those with computer-literate, music-loving children, there's perhaps a third guarantee: identity theft victim. Make that death, e-filing, and credit card fraud.

The last six years' virtual explosion – from two million to over 10 million – in estimated identity

theft victims is not limited to better dumpster-divers, more pick-pockets, or inventive ChoicePoint cons. It's related to computers, spawned by electronic commerce, obviously, coupled with computer users' ignorance and the cunning of computer criminals. Such fraud cost American banks nearly \$50 billion last year, which of course was simply passed along to consumers in the form of higher loan and credit card rates.

It's the tech world's most commonly-accepted secret: the recent explosion in identity theft, credit card fraud, and bank fraud is made possible by the convergence of exceedingly popular peer-to-peer (P2P) music and gaming file-sharing programs, electronic tax filing programs, and a sophisticated, computer-savvy international identity theft cartel. Oh, and there's the unsuspecting American public too.

Simply put, P2P programs, such as KaZaa, Morpheus, and Grokster, installed on the same home computer with popular electronic tax-filing programs, such as TurboTax and Quicken, create an open access by computer criminals to your most sensitive financial and personal information.

Without as much of a trace, thanks to P2P's design, identity thieves can reach into your com-

puter's files and retrieve a copy of your most important private financial information, namely your annual tax filing. When any 14-year old comes home from school, turns on the computer to download the latest 'cool' poker game, the download most likely comes with spyware or malware aimed at capturing the 40-something parent's tax return, credit card or bank records.

You may as well spray-paint your social security number, your date of birth, and your home address on a sidewalk in Estonia, one of the world's identity-theft havens.

Amazingly, nearly 70 percent of all household computers lack the basic necessary protections of firewalls, anti-virus, and anti-spyware programs. But even for those P2P users with such security programs – even those with updated versions – computer-savvy identity-theft criminals can access any P2P user's personal financial information with relative ease by bypassing and disabling these programs, since P2Ps operate behind a computer's firewall.

Operating behind a firewall and the ability to disable anti-virus programs permits the transmission of viruses and malware, which then provides access to any file in an end user's file directory, including personal tax returns, money management programs or *(Continued, Page 11)*

Battling Online Privacy Fraud

Amy Cobb, Senior Project Associate
CIP Program

Identity theft, which the Federal Trade Commission ranks as the "number one fraud-related complaint," is exponentially rising each month. Most of this is due in part to Phishing scams and break-ins to netted computers containing personal information.

In the recent past, SAIC, ChoicePoint Inc. and George Mason University have all been targeted by hackers breaking into data systems containing social security numbers, photos and other private information for hundreds of thousands of people. Each day, VISA, eBay and other online service providers are struggling against Phishing scams, in which the identities of their consumers are put in jeopardy by emails or web page links that are mimics of their popular websites. As attack sophistication continues to intensify, companies will need to be progressively more alert and obligated to supply updated security services.

This daunting task cannot be accomplished alone. Large companies, institutions and ISPs have started to work together in the unremitting fight against online fraud. A hacker's ability to cause significant financial losses and a major downturn in consumer confidence has necessitated the establishment of the "Phish Report Network." Companies such as VISA and eBay report confirmed Phishing

sites to a central database operated by WholeSecurity. Other companies and ISPs obtain these lists and can incorporate the "known" Phishers into their protective services. All the groups that participate must meet basic qualifying criteria prior to admittance to the Phish Network. The more participants in this network, the better a tool this will become in the fight against online privacy fraud.

State and federal governments have contributed to the fight against identity scams. California's 2003 Notification of Risk to Personal Data Act reflects a growing trend of states' interests in establishing greater privacy security by forcing companies to disclose break-ins to its affected residents. The Fair and Accurate Credit Transactions Act, signed by President Bush in December 2003, assists consumers who may have fallen prey to identity theft with a free 90 day fraud alert on their credit reports. These regulations are not a fail proof fix, but, as part of an ever growing concern across industry and government, they provide forward momentum towards winning the battle.

Financial, e-commerce and ISP companies and the government are beginning to fight these security breaches, but we cannot allow responsibility for e-security to lie solely in *(Continued, Page 14)*

Tips from the FBI's Internet Fraud Complaint Center on Identity Theft

Prevention tips:

- Check your credit reports once a year from all three of the credit reporting agencies (Experian, Transunion, and Equifax)
- Guard your Social Security number. When possible, don't carry your Social Security card with you.
- Don't put your Social Security Number or driver's license number on your checks.
- Guard your personal information. You should never give your Social Security number to anyone unless they have a good reason for needing it.
- Carefully destroy papers you discard, especially those with sensitive or identifying information.
- Be suspicious of telephone solicitors. Never provide information unless you have initiated the call.
- Delete any suspicious e-mail requests without replying.

Steps to take if victimized:

1. Contact the fraud departments of each of the three major credit bureaus and report that your identity has been stolen.
2. Get a "fraud alert" placed on your file so that no new credit will be granted without your approval.
3. Contact the security departments of the appropriate creditors and/or financial institutions for any accounts that may have been fraudulently accessed. Close these accounts. Create new passwords on any new accounts that you open
4. File a report with your local police and/or the police where the identity theft took place.
5. Retain a copy of the report because it may be needed by the bank, credit card company, or other businesses to prove your innocence.

Security vs. Liberty

The following is excerpted from a speech that the Honorable John O. Marsh, Jr. presented at JMU on Madison Day in 2003.

On the 17th of September 1787 George Washington as President of the Constitutional Convention signed a resolution of the Convention transmitting a draft of the Constitution to the Continental Congress for their consideration. It is quite likely this resolution had been drafted by James Madison. Washington described the difficult task the Convention had trying to balance "Security" versus "Liberty." He used these words in the resolution: "Individuals entering society must give up a share of Liberty to preserve the rest."

These words reflect the thoughts of the great seventeenth century philosopher John Locke, whose views on the role and structure of government had enormous impact on the Constitutional framers, especially Madison.

Locke was a foremost proponent of the concept of checks and balances in government as a safeguard of individual freedom. For Locke it was only a theory. A cen-

tury later Madison made Locke's theory a reality.

Madison was not only a superb political theorist, but he was a hands on political practitioner,

Liberty is a favorable, pervasive condition, which affects all areas of American life. If there is no liberty, there can be no right to privacy. For privacy to exist, liberty must flourish.

and a political realist. He observed: "if men were angels, no government would be necessary." However, he always remained a political visionary. The Constitution, which is a document of extraordinary flexibility, was the product of his vision, and his intellectual genius....

The impact of the Cyber Revolution has been global. It functions through the Internet, the cell phone, e-mail, and computers. More than 75% of these cyber resources, and activities, are in the private sector. This circumstance alone becomes a major factor that impacts on oversight, or governance. It complicates both.

The Cyber Revolution

has moved so swiftly it has resulted in generation skipping in the field of communications. Lesser developed areas of the world have not had to go through the poles and copper wire stage to achieve an effective communications infrastructure with global linkages. Unfortunately, it has given terrorist organizations communication resources that have become a central nervous system for their worldwide operations.

Computers, and the Internet, have been the source of much mischief. Some of it is extremely serious, and difficult to handle. There has been the adventure-some hacker, and the hacker with malice. There are Trojan Horses, and viruses that can disable systems on a global scale. Hostile intrusions have shut down electrical power grids, and cut off airport lights causing diversion of air traffic in the Northeast corridor. Bank accounts have been penetrated, and pilfered. There have been identity thefts, and the compromise of medical records. Remedies at law to address these problems are often woefully inadequate. This poses an enormous challenge to lawmakers, the courts, and the Bar.

Personal privacy is eroding rapidly – voluntarily and involuntarily. Massive data banks can profile a purchaser's habits, and can tell whether a customer prefers black or green olives, or likes crunchy peanut butter better than smooth. (Continued, Page 12)



The Honorable John O. Marsh is a Senior Fellow at the CIP Program and a Distinguished Adjunct Professor at the GMU School of Law.

History of the Privacy Officer

(Cont. from Page 5) privacy policy.¹ The Clinton Administration used these "privacy leaders" to review Privacy Act compliance within each agency. The next year, Peter Swire was named Chief Privacy Counselor for the Administration within the Office of Management and Budget. Mr. Swire worked on both commercial and government privacy issues and had a voice in deliberations concerning agencies across the government. Among his accomplishments was requiring all government Web sites to include privacy notices.

At the same time, many companies in the private sector began to hire or promote employees to be "Chief Privacy Officers." The CPO position is now very common in the e-commerce, banking and health care industries. Several membership organizations of CPOs have formed. The largest of these, the International Association of Privacy Professionals (IAPP), now meets twice yearly and includes a wide

range of industry and government representatives from around the world.

In 2001, many of the privacy leaders within federal agencies—mostly political appointees—left government service with the change in administrations. Despite urging from privacy advocates,² the Bush Administration did not hire a new Chief Privacy Counselor and only a few agencies kept their privacy leaders. Some of these privacy leaders thrived in new full time roles as Chief Privacy Officers. In fact, a few of the federal government Chief Privacy Officers have been among the most innovative in the

James X. Dempsey is Executive Director of the Center for Democracy and Technology. In addition to day-to-day management responsibilities, he works on privacy and electronic surveillance issues and heads the Global Internet Policy



Initiative. The Center for Democracy and Technology works to promote democratic values and constitutional liberties in the digital age. With expertise in law, technology, and policy, CDT seeks practical solutions to enhance free expression and privacy in global communications technologies. CDT is dedicated to building consensus among all parties interested in the future of the Internet and other new communications media.

world, in either the public or private sectors. ❖

¹ William J. Clinton, "Memorandum for the Heads of Executive Departments and Agencies," May 14, 1998, <http://www.cdt.org/privacy/survey/pres-memo.html>.

² Several privacy groups and academics including CDT wrote to OMB Director Mitch Daniels urging him to continue the position <http://www.cdt.org/privacy/010416omb.shtml>.

DHS Privacy Advisory Committee Members (Cont. from Page 2)

Charles Palmer, Department Group Manager, Security, Networking & Privacy, IBM Corporation, Yorktown Heights, NY

Richard Purcell, Chief Executive Officer, Corporate Privacy Group, Nordland, WA

Paul Samuel Rosenzweig, Senior Legal Research Fellow, The Heritage Foundation, Washington, DC

John Thomas Sabo, Manager, Security, Privacy, and Trust Initiatives, Computer Associates, Herndon, VA

James Sheehan, General Counsel, Milton Hershey School, Hershey, PA

Lisa Sotto, Partner, Head of Regulatory Privacy & Information Management Practice Group, Hunton & Williams, New York, NY

Michael Turner, President and Senior Scholar, Information Policy Institute, New York, NY

Samuel Wright, Senior Vice President, Government Relations, Cendant Corporation, Washington, DC

P2P Identity Theft (Cont. from Page 7) bank records.

Moreover, P2Ps' file sharing of text-based downloads – think computer games or word documents – permit installation of hard-to-detect, nefarious 'keylogger' programs which allow the monitoring of keystrokes from remote locations. Most recent email-based viruses have keylogger variants embedded in their attachments.

After acquiring the end user's personal financial information, the identity thief is able to reinstall the anti-virus programs and then delete any malware, leaving virtually no trace of the criminal activity. By the time you finish reading this article, the TurboTax filing on the P2P-user's computer in Easton has been emailed to Estonia, without a trace.

This all happens in a matter of minutes. The combination of P2P, keylogger and the disabling viruses make computer-related identity theft all too convenient and frightfully effective.

Those charged with either preventing or pursuing computer crimes offer little solace. Security programs – McAfee, Norton, and Microsoft – face tracking and responding to a daily onslaught of viruses and their mutations. To confront them is an overwhelming, monumental task, made impossible by the combination of P2P and inventive computer-savvy identity thieves. By their own admission, these top firms cannot keep up

with the the deluge of malware variants. There is no "Good Housekeeping Seal of Approval" for combatting computer viruses.

Law enforcement's pursuit of international identity theft rings is made all the more difficult since most ISPs maintain records of only incoming, but not outgoing, emails. For all the relative advances the FBI and Secret

The identity thief has the keys to the bank vault, and the P2P download is the getaway car.

Service have made in recent years in the pursuit of computer crimes, it's impossible to investigate – let alone convict – a suspect without a paper trail.

And since most computer users would never suspect that a teenager's afternoon's online poker game led to the misery of dealing with credit card fraud, perhaps years later, there's little that law enforcement can do.

Parents do not understand that their child's downloading habits – gaming and music – exposes their most personal financial records to credit card and bank fraud.

Of course the scrutiny of the hidden embedded content will always remain with the end user, only now the masses aren't even aware of the vulnerability, as evi-

denced by P2P's and electronic tax filing's continual surge in popularity. With P2P programs installed on an estimated 30 million home computers, and perhaps as many as 60 million electronic tax filings expected this year, chances are either you or someone you know is made quite vulnerable by the convergence of computerization, convenience, and criminal computer cartels.

A full understanding or higher profile of how P2P causes identity theft would likely prompt millions of parents to remove those programs from their home computers. But who would lead such an effort? It's not going to be Microsoft's Bill Gates or H&R Block's CEO Mark Ernst – they're already complicit in their silence.

And don't look to the government either. The FTC has the knowledge but lacks the will; the Congress and White House has the platform but not the understanding; the FBI and Secret Service have the jurisdiction but are distracted (for more obvious reasons – terrorism); and the IRS, free from the paper deluge, is drinking Kool-Aid.

Perhaps the two industries most likely to benefit from P2P's demise, the music and film industries, have adopted strategies that require suing your customers. This may get you headlines, but it hasn't stopped P2P downloads.

The combination of growth in online retail, the popularity of file sharing (*Continued, Page 12*)

Security vs. Liberty (Cont. from Page 9) Your tastes in toothpaste and paper towels is information you authorize to be collected when you use your super-market saving card.

Privacy is not an enumerated right in the Constitution. However, it is clearly implied in the Bill of Rights. Outrage about computer insecurity has become a public issue. This is often framed as "security vs. privacy," and how much privacy must we give up to have security?

The issue should really be presented as the Constitutional framers addressed it: Security vs. Liberty. Liberty is a stronger word than privacy. Liberty is a favorable, pervasive condition, which affects all areas of American life. If there is no liberty, there can be no right to privacy. For privacy to exist, liberty

must flourish. We are dealing with a fundamental issue of human freedom. One to which James Madison dedicated his life.

What is to be Done?

First, I think we have to revisit the world of James Madison. We must find some way to bring together several key interests: Governmental (Federal and State); non-governmental (commercial and institutional); and individual users. All of whom must search for common ground to establish new organizational structures, or modalities for the effective oversight, and governance of the information technology infrastructure of this Country. This must be accomplished in a way that we maximize the great advantages of information technology, but minimize encroachments on

individual liberty and citizens' privacy. It is my view the best workshop to address this task could be the university campus. I believe our Constitution has the flexibility for such an approach.

It is a task James Madison would have relished, and met head on effectively. I am confident he would see the important role played by science and technology, and its vital linkage to other studies. I believe in seeking solutions he would draw heavily on History and Philosophy. History can teach us what will, or won't work; and Philosophy can teach us what is right, and what is wrong. They are cornerstones of learning. Madison's leadership in framing the Constitution was grounded in years of intense study, and research in History and Philosophy. ❖

Legislation Calls for Creation of Oversight Board

The privacy panel at DHS will not be alone in advocating for privacy and civil liberties at the federal level. The Intelligence Reform and Terrorism Prevention Act of 2004 created a **Privacy and Civil Liberties Oversight Board**. This five-member body will reside in the Executive Office of the President and will provide advice and counsel on the development and implementation of policy. The Board is specifically charged with reviewing proposed regulations and executive branch policies related to efforts to protect the Nation from terrorism while ensuring that privacy and civil liberties are appropriately considered in the development of such regulations and polices. The members of this board have not yet been nominated by the President.

P2P Identity Theft (Cont. from Page 11) and a reliance on online tax filing and online banking has converged to make identity theft convenient, efficient and extremely profitable, now with little chance of the thief getting caught.

For identity thieves, the sun,

moon and earth are all in alignment, and tragically Americans are blind to this vulnerability. Meanwhile their government and key industry sectors have all the reason to keep them in the dark.

The identity thief has the keys to the bank vault, and the P2P

download is the getaway car. ❖

John Edgell is a Washington, D.C.-based legislative/public affairs consultant and entrepreneur. He will file his taxes by snail mail this year.

Cyber Security and the Law: Addressing Compliance, Complexity, and Confusion

The Cyber Security Industry Alliance and The Critical Infrastructure Protection Program at George Mason University School of Law present a three-part symposium on the emerging landscape of cyber security legislation and compliance. The frequency and complexity of legislation surrounding cyber security has exploded in the past two years. As our lives and commerce become increasingly dependent on IT systems, the interaction of existing laws and proposed legislation becomes more and more complex. This symposium series explores the complex emerging framework of multi-level legal and technology compliance requirements.

SAVE THE DATES:

March 22 (State Level) **April 26** (Federal Level) **May 26** (International Level)

The symposium series will be held at 6:15 pm on March 22 and April 26 at the GMU Law School Main Atrium, conveniently located on the Metro Orange line at Virginia Square; the final session of this three-part series will be held May 26 near Capitol Hill. A keynote speaker or panel will focus on a specific legislative and compliance arena each evening, with a wine and cheese discussion and reception to follow.

State-Level Cyber Security Compliance
Tuesday, March 22 (GMU Law School Main Atrium)
6:15-8:00 pm

California's passage of Senate Bill 1386 places the burden on businesses, no matter where they are based or where they process information, to take "adequate measures" to protect the personal information of California residents. The national impact of this requirement could be profound. Similarly, a recent scan of a legislative tracking service showed that over twenty five state legislatures have proposed legislation that touches upon "spyware," each with potentially different definitions and exceptions. This session will hone in on state-level developments that may develop in conflict with other states and that may impact clients in various ways across state lines.

Invited speakers include...

David Albo and David Oblon of Albo & Oblon LLP. David Albo proposed Virginia's anti-spam law; David Oblon defended one of the first cases prosecuted under the law. Hear the two partners provide perspective on both sides of the issue, as well as the outline of other emerging state-level compliance issues from across the nation.

More information to follow for the April 26 event.

Space is limited
RSVP now to Amy Cobb, 703-993-8193 or acobb1@gmu.edu

CLE credit may be available.

Spyware (Cont. from Page 4) the life or property of another. The complexity here is that these torts operate in a world where humans live and walk on land, not where individuals exist in cyber space.

Additionally, the Internet is truly a global public good whose services cut across international borders where any U.S. legislation could be rendered futile. Already U.S.

officials have discovered the 2003 anti-spam legislation lacked any real teeth in lessening spam in America - it just relocated many spam operations overseas.

With the progression of unimaginable technology and an ever-more global economy, how can we protect the rights of individuals against problems that lack the clear boundaries of yesterday? Justice Oliver Wendell

Holmes once wrote that the answer for bad speech is the competition of good speech in a "marketplace of ideas." Perhaps the fix for bad programs, such as spyware, may be good programs that stay one technological step ahead. We may well have reached a place where traditional fixes, such as legislation, are entirely inadequate to address certain modern societal ills. Spyware may be one such ill. ❖

Online Fraud (Cont. from Page 8) their hands. Consumer ignorance about identity theft, vulnerability in today's cyber world and the need for self protection is parallel to not locking one's doors to reduce the probability of being burglarized. Current regulations and safeguards can help deter hackers and Phishers but they cannot guarantee online security or the future capabilities of these criminals. Steadfast monitoring of our own cyber activities, influencing service providers through purchasing power to make online activities safer, and pressuring government to compel disclosure of break-ins across all fifty states is our own responsibility. ❖

Privacy in the Federal Gov't (Cont. from Page 5) Impact Assessments (PIAs) to OMB for major systems that collect new information and for any new system that will collect personal information.

A PIA is an analysis of an agency's handling of personally identifiable information describing for a specific system how the agency ensures compliance with law and policy. Agencies have been conducting

PIAs pursuant to this requirement since the third quarter of FY 2003, submitting them to OMB in support of their information technology investment requests and making them publicly available as required by the Act.

OMB issued a PIA "how-to" guide in September of last year, and was reportedly pleased with the over 300 assessments agencies completed for fiscal 2005 budget submissions. ❖

The CIP Program is directed by John A. McCarthy, a member of the faculty at George Mason University School of Law. The CIP Program works in conjunction with James Madison University and seeks to fully integrate the disciplines of law, policy, and technology for enhancing the security of cyber-networks, physical systems and economic processes supporting the nation's critical infrastructures. The CIP Program is funded by a grant from The National Institute of Standards and Technology (NIST).

The CIP Report is published by Zeichner Risk Analytics, LLC on behalf of the CIP Program. ZRA is the leading provider of risk and security governance knowledge for senior business and government professionals. ZRA's vision is to be a consistent and reliable source of strategic and operational intelligence to support core business processes, functions, and assurance goals.

If you would like to be added to the distribution list for *The CIP Report*, please click on this link: http://techcenter.gmu.edu/programs/cipp/cip_report.html.