INFORMATION SECURITY & PRIVACY NEWS

A Publication of the Information Security Committee
ABA Section of Science & Technology Law

SUMMER 2010 VOLUME 1 ISSUE 3

Identity Theft - Protect Yourself and Your Clients

By Mari J. Frank

Massive security breaches of sensitive personal information are on the rise, and identity theft continues to claim million of victims. It could happen to you, your firm, or your clients. When my own identity was stolen in 1996 by a woman I never met in a city four hours north of my office, I was shaken. My "evil twin" stole over $50,000 worth of credit in my name, used my good reputation and credit to buy a red convertible, totaled a rental car for which I was sued, and worse yet assumed my profession as an attorney distributing business cards with my name. There were no laws making identity theft a crime at the state or federal level (for consumer victims). As an advocate for other victims, I joined task forces, helped write legislation, testified in Congress and had discussions at the White House. *Read more*

The Ivory Tower in the Cloud

By Tanya L. Forsheit

Institutions of higher learning are often breeding grounds for experimentation and creative approaches to old problems. Thus, it is far from surprising that universities have represented some of the earliest adopters of enterprise cloud computing solutions. Cloud computing is enormously attractive to universities, for a number of reasons, especially when it comes to email. The cost of internally hosting email is particularly acute at colleges and universities: "the cost to a college of hosting e-mail accounts as an Internet Service Provider (ISP) has grown more expensive. And students, faculty and staff use e-mail differently today than they did in 1999, swapping large files and subscribing to content-heavy e-mail services." *Read more*

Developing The Security Mindset - An Evolutionary Process

By Mike Ahmadi

I did not start my life in the world of technology as a security professional. In fact, the first time I became aware of the concept of security professionals in the world of technology I was convinced that there was no possible way anyone could make a career out of it. Computer security, as far as I was concerned, was about having a good virus scanner installed and keeping it updated with virus definitions. Oddly enough, that worked (or at least seemed to work) for awhile. I did not get any computer viruses (or at least according to my virus scanner), and everything seemed to work as expected. *Read more*

2010 Information Law Updates – Cases, Statutes and Standards

By Thomas Shaw

In the first six months of 2010, there have been a number of developments in U.S. information security and data privacy statutes, cases and standards. This includes state and federal laws and regulations that have been passed pr promulgated, are being considered or coming (or not) into force. It also involves civil and criminal cases and enforcement actions brought by regulators. And it encompasses new privacy and security guidelines and standards issued by standards bodies. To describe the major developments in this broad area of law and practice, but keep it manageable, each development is presented with a brief analysis after it. Deeper analyses of these developments can be found in the *Read more*

Identity Theft – Protect Yourself and Your Clients

By Mari J. Frank

Massive security breaches of sensitive personal information are on the rise, and identity theft continues to claim million of victims. It could happen to you, your firm, or your clients. When my own identity was stolen in 1996 by a woman I never met in a city four hours north of my office, I was shaken. My "evil twin" stole over $50,000 worth of credit in my name, used my good reputation and credit to buy a red convertible, totaled a rental car for which I was sued, and worse yet assumed my profession as an attorney distributing business cards with my name. There were no laws making identity theft a crime at the state or federal level (for consumer victims). As an advocate for other victims, I joined task forces, helped write legislation, testified in Congress and had discussions at the White House.

You certainly have seen horror stories about this crime on television, and you may be concerned about this happening to you, your firm, your family, or your clients - since no one is immune. Javelin Strategy & Research issued its 2010 report on identity fraud occurrences from 2009. They found that the instances of identity theft reached record numbers in 2009 with an estimated 11.1 million adult victims of identity theft with total fraud amounting to $54 billion. Americans are worried about identity theft. According to an October 2009 Gallup Poll, identity theft was the top concern with 66 percent of respondents saying they frequently worried about identity theft.[1] My goal in this article is to help you understand your vulnerabilities, and give you tools to *minimize* your personal and professional risks.

The truth is, no matter how careful you are with your information, you, your firm and your clients are vulnerable because sensitive information is out of your control when it is in the hands of third party companies or governmental agencies. This crime has skyrocketed due to the careless information handling practices of businesses, organizations and governmental entities that collect, store, utilize, and share your personally identifiable data. Without strict guidelines and real enforcement (allowing a private right of action), the problem has grown worse.

As an attorney, you are in a distinct position to protect the sensitive records that you maintain about your staff and clients. You have a duty to report security breaches yourself. Most states have security breach notification laws such as California[2] which require all businesses and state governmental agencies that experience a security breach (an acquisition of unencrypted electronic files of sensitive information by unauthorized persons) to notify all potential victims of the breach so that they may protect themselves with a fraud alert, a security freeze or other means. Federal guidelines for financial institutions encourage safeguards and notification as well under the Gramm-Leach-Bliley Act,[3] and on August 19, 2009, the federal Department of Health and Human Services (HHS) issued the interim final

---

[1] www.gallup.com.
[2] California Civ. Code §§ 1798.29, 1798.82, and 1798.84.
[3] 15 U.S.C §§6801 – 6809.

rule regarding notification of breaches of unsecured protected health information under the privacy and security provisions of the Health Insurance Portability and Accountability Act of 1996.[4] There are numerous pending federal bills which would require alternative security breach triggers for notification which would preempt state laws. From February 15, 2005 through June 3, 2010 there was *public* reporting of the security breach of 354,568,866 records of personal identifying information.[5] It's important to remember that not all security breaches are required to be publically reported and of those that are reported, many of the incidents do not reveal the actual number of records lost or stolen. So this number of records is far below the actual number.

Before you can protect yourself, your staff, your firm and your clients from identity theft, you must understand just exactly what it is and how it happens. Simply, you become a victim of identity theft when an unauthorized person uses your personal identifiers, like your name and Social Security number, to impersonate you to commit fraud. An individual may become a victim or a business or law firm may itself become a victim. Imposters will steal identities for four main reasons — financial gain (the major reason); to avoid arrest or prosecution; revenge or jealousy; and terrorism. There is no limit to the creativity of these impostors, because whatever you can do or obtain with your identity (personal or business), your impersonator can also do as your "clone."

Financial Gain

John, Esq. and his wife were in the process of buying their first house, when John's credit reports showed that he was delinquent on payments for credit accounts that were not his. The couple's credit is flawed by outstanding bills of $35,000 for accounts from Citibank Credit Card Company, Chase, and American Express, which precluded them from purchasing their dream home.

Using your credit is an easy way for criminally minded persons to steal from innocent, good people like you. With this "faceless crime," a perpetrator doesn't have to use a gun or ever meet the victim. All he or she needs is a bit of information. Right now the key to the kingdom of identity theft is the Social Security number (SSN). In the near future it may be a fingerprint, an iris scan or another unique "piece of your body" called biometric information that is transferred electronically via the Internet, or it may even be a radio frequency identifier (RFID). The game is the same — fraud.

Not only can the thieves obtain new credit and cards using your information, but also now with tighter credit they make greater efforts to siphon money from your bank accounts, investment accounts, trust funds, college accounts and retirement plans. They can obtain life insurance in the victim's name (and make themselves the beneficiary), secure medical services, have babies using another's health insurance, get medical care, steal your disability payments or Social Security checks, receive unemployment or disability compensation, get your tax refund, or even file bankruptcy using your identity. They can create bank accounts in your firm's name and deposit fraudulent checks, and your

[4] 45 C.F.R. parts 160 and 164.
[5] For an update of current breaches please visit http://www.privacyrights.org/ar/ChronDataBreaches.htm.

firm is later on the hook.

Steve and Linda, both attorneys, had experienced what they call a living nightmare. For more than two years, an identity thief had used their names and Social Security numbers to open 30 credit accounts, making purchases totaling more than $100,000. The imposter had also purchased a Jeep Cherokee. The couple had been hounded almost daily by collection agencies. There was even a civil suit filed against them for nonpayment of a furniture bill

Indeed, identity theft is increasing at epidemic proportions and financial rewards are the leading reason for this crime. Below are examples of the top six types of financial hoaxes that fraudsters can commit using your identity:

1. Credit card fraud

George, Esq. opened his credit card billing statement and saw $2,000 worth of charges he didn't recognize — all orders for merchandise and gasoline in another state. Yet his credit card was still in his wallet. He discovered he had been skimmed. It may have happened at a restaurant when the fraudster-waitress smiled at him, took his credit card, then ran the card's metal strip through a skimmer, which copied the information imbedded in the metal stripe. All that the thief had to do was download the information and copy to fraudulent cards.

Sally, Esq. found out her debit card number was used by her secretary on the Internet to purchase Christmas presents for her family.

2. Utility theft

Laura, Esq. a Southern California resident, began to receive collection calls regarding delinquent phone accounts in Northern California. She learned several men in a California penal institution had used her SSN, not her name, to open up phone accounts. Her SSN was associated with several men's names associated with many different telephone numbers.

3. Bank swindles

Stacy, a law student, learned that her impostor deposited $8,000 worth of phony checks into her checking account, and then proceeded to make new checks using the account to buy goods and services. All of Stacy's own checks bounced and her bank refused to help her, accusing her of conspiracy.

4. Employment deception

A large top notch law firm in Southern California found out that one of its associate "lawyers" was an impersonator who had gone to law school, but couldn't pass the bar, so the impostor borrowed a similar name, the victim's SSN and the Bar number of a licensed lawyer from Northern California.

5. Counterfeit loans

The Honorable Judge Jonathon in Southern California was horrified when he went to purchase a new car. His credit report showed two new car loans for cars he didn't purchase. His credit was destroyed.

6. Newly created checks

A large law firm in Texas noticed that thousands of dollars were missing from their retainer account. What happened? A thief created new checks from an office store using the account number and routing number of the firm's checking account.

Criminal Identity Theft: Avoiding Arrest or Prosecution

Brian Esq learned that someone with similar physical features used Brian's name when he was arrested for various criminal offenses. He recently panicked when he found out that the impostor was also a sex offender and a neighbor in his office building.

Imagine this: You're sitting at your computer at work and two law enforcement officers approach you to ask for your identification. They begin to interrogate you, and then, in front of your colleagues in the firm, tell you that they have a warrant for your arrest; they handcuff you and lead you to the police station. You learn someone has used your identity to commit a crime that you know nothing about. You will need to provide fingerprints to the police, obtain the arrest and court records, make motions to clear your name and obtain a Certificate of Innocence, and rectify the public records with the data brokers and check the Internet for data re-sellers who may still report the fraudulent criminal record.

Revenge: Retaliation

Tom and one of his former client's had a falling out after a case went sour. Unbeknownst to Tom, his former client set up an e-mail account using Tom's name and sent embarrassing and degrading e-mails to the firm's staff and to the opposing firm trying to discredit Tom and his professionalism.

These are examples of Cyber Identity Theft which is a growing concern with the vastness and anonymity of the Internet.

Cloning your small firm

Stan, Esq. learned that his website was hijacked by an imposter. A blog owner set up an account in his name. An old foe was out to discredit him. It's easy to do.

Martha, PhD and expert witness in a custody case, learned that the husband of the client who hired her created a social networking profile that was meant to ruin her reputation in court.

Terrorism

Over half of the terrorists who committed the atrocious acts of 9/11 committed identity theft. All of them used false documents. They used fraudulent identities to obtain credit cards, cell phones, hotel rooms and even flying lessons. They avoided apprehension by assuming identities, and more disturbing, they stole identities for revenge against our way of life.

How Do Thieves Appropriate Your Identity?

- They steal mail from mailboxes or office mail.
- They may work in your firm or clean your office at night and steal sensitive information left on desks or stored in unlocked cabinets or in unencrypted files (prosecutors in Orange County, CA can tell me that 60 – 70 percent of all identity theft cases they handled are unscrupulous employees).
- They may pose as you and report an address change in order to divert your mail including those ubiquitous pre-approved offers of credit, to their address — or more likely, a drop box.
- They obtain in-home or in-office access to confidential documents.
- They might access your credit report fraudulently by posing as an employer, loan officer, car dealer or landlord. Or they might illicitly obtain your SSN and credit information while actually employed by a company with access to a credit bureau database.
- They scam you through e-mail, regular mail or by phone, pretending to be a legitimate agency or company asking for personal data (phishing or vishing).
- One of the most common methods is to gain insider access to a law firm, an agency or a bank, to pilfer personnel files and critical databases maintained by the company. The Gartner Group estimates that internal employees commit 70% of information intrusions, and more than 95% of intrusions that result in significant financial losses.[6]
- Impersonators also use personal information they find about you in chat rooms, e-mails, social networking websites and information brokers on the Internet.
- Electronic Security Breaches are mounting, and can be as simple as stealing disk files, backup tapes, thumb drives, and a laptop or as sophisticated as electronic hacking by unscrupulous employees, or fraudsters living in a foreign country.

A member of a notorious crime ring was employed temporarily at a large corporation. He downloaded the employee list containing SSNs and dates of birth and provided this information to members of the ring. One by one, the employees' identities were used fraudulently to obtain credit.

Consider about all the places that have your SSN and other personal identifying information - your CPA, dentist, doctors, the IRS, the State Tax Board, the credit bureaus, your creditors, your bank, your investment institutions, etc. - it is daunting. Without our ability to control access, there is no guarantee, no matter how careful you are, that you won't become a victim yourself. In your law firm you do have control to a great extent how information is collected, viewed by others, stored, secured and protected. You have a duty to safeguard information within your control and depending on what Congress or the federal appellate courts decide you may be subject to enforcement of the federal Red Flags Rule regarding identity theft described below.

[6] http://www.gartner.com/.

The Red Flags Rule Intended to Prevent Identity Theft May Apply to Lawyers

The American Bar Association (ABA) filed a three-count complaint against the Federal Trade Commission (FTC) alleging that the FTC's application of the Final Rule of the Identity Theft Red Flags Rule (the "RF Rule") under the Fair and Accurate Credit Transactions Act (FACTA) of 2003[7] to attorneys exceeds the FTC's statutory authority.[8] The complaint alleged that the FTC's actions in implementing the RF Rule as it has transgress the Administrative Procedure Act,[9] was in violation and should not apply to attorneys. On October 29, 2009, District Judge Reggie Walton of the District of Columbia held that Congress did not intend lawyers to be considered "creditors" under FACTA when he granted a partial summary judgment motion by the ABA in the declaratory judgment action. Under Walton's decision, the RF Rule developed by the FTC to impose the statute's identity-fraud-protection provisions on businesses is inapplicable to lawyers outside the financial sector.

However, on February 25, 2010, the FTC filed an appeal of the judge's decision upholding the ABA's position that the RF Rule doesn't apply to lawyers. The case is of import because it would require law firms, if the FTC prevails, to implement anti-fraud measures and it would expand federal power to regulate lawyers which many believe should be left to the states. The FTC has already delayed the deadline five times (beginning in 2008) and most recently again on June 1, 2010. Now the deadline for enforcement of the RF Rule is after Jan. 1, 2011, due to requests from several members of Congress who are working on limiting the scope of the RF Rule.

Although Congress may finally clarify that law firms are not subject to the RF Rule, we as lawyers nevertheless still have an affirmative duty to protect our clients and staff from identity theft. Indeed. If any of our clients or employees becomes victims of identity theft due to our failure to take reasonable steps to protect their sensitive data from fraudsters, we would be subject to liability. So whether or not the FTC or any other Governmental agency will be able to bring an enforcement action against you or your firm regarding the RF Rule, it's a good idea to implement the rules as they are considered " reasonable" actions to take to protect staff and clients. Being proactive will help shield us from liability if the worst happens.

The RF Rule sets out how businesses and organizations must develop, implement, and administer their Identity Theft Prevention Programs. The program must include four basic elements, which together create a framework to address the threat of identity theft as follows:

1. Your program must include reasonable policies and procedures to identify the "red flags" of identity theft you may run across in the day-to-day operation in your law firm. You and your staff can brainstorm suspicious patterns or practices, or activities, which may indicate identity theft. For example, if a client has to provide some form of identification to retain your firm, a Driver's License that looks like it might be fake would be a "red flag." Or if a new

[7] 72 Fed. Reg. 63,718 (Nov. 9, 2007).
[8] See Pub. L. No. 108-159, 117 Stat. 1952 (codified at 15 U.S.C. §§ 1681-1681x; 20 U.S.C. §§ 9701-8).
[9] 5 U.S.C. §§ 702-706 (2006).

client calls pretending to be a friend of someone on your staff and no one knows that person. Or a client may tell you that his information was stolen by someone in your office.

2. Your policies must be designed to detect the red flags you've identified. For example, if you've identified fake IDs as a red flag, you must have procedures in place to detect possible fake, forged, or altered identification.
3. Your policy must clarify what actions you'll take when you detect red flags. If you believe that a staff member has accessed a file without authority, who will be notified? You may specifically state, for example, if any suspicious identity theft activity occurs, an employee will report immediately to the privacy officer/HR person/attorney in charge/police.
4. You must address how you will re-evaluate your policies periodically to reflect new risks and you must update and train your staff as to the risks and how to respond. You need to log possible privacy and security breaches and address how to prevent them and add to your policies. Staff training is not just handing a document to read, it includes face to face training with live examples of risks and responsibilities.

You must designate a senior level person in charge or a committee to approve your first written program and policies. If you have a small office, the senior attorney should be in charge- and the person with the highest authority should be the person to approve the plan. Your written program must state who is responsible for implementing, administering, training and enforcing the policies. Fortunately, the RF Rule takes into consideration the size of your firm and risks associated with your business practices. So smaller firms will have a more intimate training and enforcement, but it should be as comprehensive as the larger firms that will institute a more formalized program.

Identity Theft Red Flags Protection Program

The following Identity Theft Precautions will help you to create your own Identity Theft Red Flags Protection Program.

<u>Collection, storing, and discarding personal information</u>

Aside from electronic breaches, ID thieves often steal hard copies of client files, employee personnel documents, loan papers, hospital records, bank documents, etc. Thieves can *use* the information so easily and quickly on the Internet, where vendors and others have no face-to-face interaction. Your impostor can make purchases from the seclusion of his bedroom, establish an e-mail account in your name without any proof of identity; or purchase authentic-looking, governmental documents on line to impersonate you for a variety of reasons. Consider these tips:

- Analyze what information you collect in your office. Don't collect more than you need. If you don't need to store it, you won't have it to lose in a security breach.
- Keep your sensitive records under lock and key

Burglars and unscrupulous employees are more interested in personal identifying information than in jewels or equipment. It's a wise investment to use locking file cabinets for your confidential

documents kept at home and in your office. Put padlocks on doors of closets that contain boxes of old client files, tax returns and financial statements. Utilize alarm systems. Secure briefcases containing private documents with a locking device and alarm in your office and locked car trunk. When using a valet, provide a key that doesn't open the trunk. For cell phones, electronic devices, laptops, iPads, etc., encrypt all sensitive data.

- Limit Access to those who need to know, and monitor audit trails

At your office set up audit trails and unique passwords for electronic access to sensitive documents. Also monitor off-line audit trails for release of keys to cabinets, storage rooms, and client files. Only allow those with a need to know to access confidential data. Change passwords every six months and whenever an employee leaves his job. Ask visitors to identify themselves and log in. Use biometric keys to access sensitive information and electronic equipment. Don't allow employees to leave cases on their desks unattended. Make sure electronic files are password protected.

- Shred confidential data at home and at your office

Purchase crosscut shredders for discarding of important papers, pre-approved offers, account statements, and confidential data of all kinds for you, employees and clients. Keep shredders at every desk and at the copier and fax machines.

Use a bonded shredding service that comes to your office and destroys sensitive documents on site. Businesses discarding sensitive documents must completely destroy them. Federal law requires complete destruction of personal information under the Fair Credit Reporting Act (FCRA).[10] The disposal rule above applies to attorneys.

- Secure faxes, printers, computers, and e-mails

Tell all persons who fax to your office or home not to send confidential information in a fax to you unless they call you first to verify the fax number and verify who will receive it and call afterwards to make sure it was received. Use designated faxes and printers for confidential data.

When disposing of electronic equipment, computers, copiers, and other electronic equipment, completely erase or destroy the hard drive. Each device that has a computer stores information. Don't give away or turn in a lease on a copier without erasing the hard drive.

- Set up privacy rules and encryption for offline electronic devices, offsite laptops, and all other electronic devices. Create a sign in and out process; consider using a biometrics entry key.
- Conduct civil and criminal background checks for all employees and vendors with access to sensitive information about staff and clients

If an impostor steals the identity of your clients or staff, you may be liable for negligent hiring or negligent supervision. Be sure to get the potential employee's prior permission in writing before obtaining a consumer report.

[10] §628; 15 U.S.C. §1681u).

- Limit use of personal identifiers like the SSN for clients and staff

For example, under California law,[11] companies may not do any of the following:

  - Post or publicly display SSNs
  - Print SSNs on identification cards or badges
  - Require people to transmit an SSN over the Internet unless the connection is secure or the number is encrypted
  - Require people to log onto a web site using an SSN without a password
  - Print SSNs on anything mailed to a customer unless required by law or the document is a form or application.

Never include the SSN or sensitive financial data in public court records. Most state and federal courts restrict the filling of such documents and you could be liable to any victim or may be hit with sanctions for careless handling of sensitive data.

- Use photo business cards, photo ID's and photo credit cards to authenticate your office
- Make sure you know who your clients are as well as your staff (authenticate them).

Credit Card Care – For Yourself and Your Clients

- Put passwords on all your financial accounts (not your mother's maiden name).
- Monitor your credit card account and bank statements online several times per month.
- Carefully review all bank statements and financial statements once per week. Make sure to have checks and balances so as not to make embezzlement tempting or easy.
- When accepting credit cards online from clients to pay bills, store only what's necessary. Don't keep credit card numbers on file. Shred faxed credit card payments immediately after processing or entering the data into the credit card machine if done manually.

Protecting Financial Transactions

- Use checks only when necessary.

You are safer using a credit card than you are using a check. Also, it's safer to do online banking. Office supply stores sell computer checks. The fraudster can copy your routing and account numbers on new checks and drain your money with the bank just by looking at your check.

- Don't print your telephone number or full name on your checks
- When you order new checks, have them delivered to your local bank branch, rather than your home or office.
- Back-up and encrypt your financial software
- Online bill pay is safe when you use a secured computer and complex passwords.

[11] California Civ. Code §1798.85.

- Always initiate online payments from your own account. Don't provide your account number to all your vendors. Your bank already has your sensitive data.

Protecting Information by Phone

Never allow family or staff to release personal information over a cell phone, a phone, in person, or on the Internet to someone you don't know who contacts you. If you are asked for information from a stranger who claims to be your bank or the IRS, be polite, get off the phone and call the number listed in the phonebook or online directory yourself to ask for that person or department.

- Check to see who is listening when sharing confidential information on a speakerphone or cell phone. When using a wireless phone in a public place, be careful to speak quietly, and move to a secluded area when speaking about sensitive information.

Secure Your iPhone, Blackberry, and iPad - encrypt confidential information

- If you are transmitting wirelessly, then ensure proper user/device authentication before transmission.
- To protect data in case the device is lost or stolen, utilize user ID and Password level security, and encrypt sensitive data.
- Find out more on how to protect yourself with wireless devices.[12]

Protecting Your Mail and Mailbox

- Don't put checks in the mail from your home or office mailbox and don't leave them in bins at work.
- Use Alternative Payments such as on-line banking with a 12-character alpha/numeric password.
- Get a post office box or a locked business and residential mailbox.
- Limit pre-approved offers by calling 1888 5 OPT OUT.

Reviewing, Accessing and Correcting Your Credit Reports.

- Order your free credit report from all three major credit reporting agencies (CRAs) at least once a year[13]
- Limit access to on-line credit reports, and background checks at your office

Monitor and restrict to those who have a permissible purpose and strictly monitor retrieval (be cautious of the FCRA.)

- Immediately correct all mistakes / fraud on credit reports in writing, return receipt requested.

If you see fraud on your credit profile, place a 90-day fraud alert on your profile (you may write for a

[12] www.firewallguide.com/index.htm.
[13] www.annualcreditreport.com or call 877 322 8228.

seven year fraud alert if you send a police report and identifying information) or consider a credit security freeze to lock up your credit with password protection.[14] In California, identity theft victims are entitled to one free credit report per month for 12 months after the first alert. Victims in other states are entitled to two free reports in the year of victimization.[15]

Protecting yourself and your office while using your computer

- Set up unique system passwords to get into your computer
- Install hardware and software firewalls and make sure staff use them and update software
- Install, use, and continually update anti-virus and antispyware software. Run live updates
- Set up automatic notices of updates for all programs, and download in a timely manner
- Back up your files daily and encrypt sensitive confidential files
- Don't share or transmit data about clients without their permission and always encrypt
- Set forth privacy policies with regard to the use of the intranet at home and taking files home either by hard copy or electronically.

Protecting Yourself on the Internet

- Don't give your password to anyone.

The secret to effective password creation of at least eight numbers and letters: Use the first or last letters of each word in a favorite line of poetry that you'll easily remember. Intersperse these letters with numbers and punctuation marks. Example: "Mary had a little lamb." M*HA2LL or Y!DAE9B. Upper and lower case can also be varied (M*ha2LL). Change your passwords every six months.

- Don't register when visiting web sites on the Internet, unless you are sure it's not a fake site. Don't provide sensitive data.
- Don't display your personal, family, or your staff's personal information on the Internet. Think twice before creating your own home personal page, family tree, or photo web site with identifying information about your family. Minimize your business website to business information.
- Shield your staff online – set forth clear rules.

Monitor chat rooms and whom they're "chatting" with in social networking sites. Set forth privacy and security policies.

- Monitor social networking and blogging sites.

Set forth policies and procedures and make sure they are followed.

- Be cautious with peer-to-peer file sharing at home and the office (p-2-p)

You may associate peer-to-peer file only sharing with sharing music (which is not legal), but people also share all types of sensitive data and other files.

---

[14] See www.consumersunion.org or www.financialprivacy.org.
[15] Learn more at www.identitytheft.org and www.FTC.gov/idtheft.

- Don't trust people you meet online, and use a nickname for your screen name.

You may find the love of your life, but you might also run into an evil-minded criminal.

- Make sure you are on the web site of the company that you really think you're doing business with.

Online fraudsters create web site names (URLs) very similar to those of legitimate companies. That's called Pharming. To check whether the site that you're on is really the legitimate company.[16]

- Only give out information that's necessary for the transaction.
- Use disposable forwarding e-mail addresses for chartrooms, purchases, public postings, and social networking.
- Never use a public computer, such as an Internet café, a library, or airport computer to access your sensitive information.
- Keep your e-mail safe by limiting personal information and encrypt sensitive attachments.
- Passwords protect and encrypt confidential attachments for clients and friends.
- Teach your clients not to send sensitive data by emails. WinZip is an easy to use free program and you can teach your clients.
- Search out your name and staff members' names on the Web to find what information is circulating on the Internet.
- Don't get hooked by a "phishing" or vishing expedition. Never respond to e-mail or voicemail asking for sensitive information.
- Advise family, staff and your clients not to put confidential or controversial information in e-mail.

Use encryption software to protect anything sensitive.[17]

- Visit an Internet safety organization such as Cyber Angels to protect your identity[18] or the Federal Trade Commission[19] for additional precautions.

<u>Other Protective Privacy Measures</u>

- Use tamperproof mailers when sending sensitive information.
- Verify that your clients, staff and vendors are who they say they are. Authenticate.
- Conduct privacy and identity theft protection audits of your on-line and off-line environment at home and at your office. Consider an outside audit by privacy professional.
- Designate a staff member to be in charge of Privacy and Identity theft protections

This staff member usually works with your IT or security consultant, but has a unique role. Security considers the systems, but privacy considers the individual. You need to designate one person to

---

[16] www.whois.net.
[17] i.e.: www.pgp.com or www.winzip.com.
[18] www.cyberangels.org.
[19] www.FTC.gov.

implement privacy policies, analyze vulnerabilities, coordinate with the technology professionals, train staff, evaluate and adjust in accordance with new state and federal laws.

- Implement Privacy and Identity Theft Policies on the Web and in your brochures.

The Online Privacy Protection Act of 2003[20] requires operators of commercial web sites or online services that collect personal information on California residents through a web site, to conspicuously post and comply with its privacy policy. The privacy policy must, among other things, identify the categories of personally identifiable information collected about site visitors and the categories of third parties with whom the operator may share the information.

- Train your family and your staff as to best practices for privacy and identity theft protection.[21] Keep apprised of current privacy and identity theft laws.[22]

As a lawyer, you must collect and utilize very private, confidential information about your clients and your employees. You have a duty to guard your clients' and staff's privacy and identity in your office and in the public courts. This daunting challenge presents legal questions, security risks, and litigation exposure. Take the opportunity to analyze and enhance your information management practices and create a proactive approach to data privacy and security. Whether or not you will be subject to the Red Flag Rule, institute a policy that is based on the model program.[23] You'll boost client trust and goodwill, and increase profits. Implement the suggestions in this article to augment your privacy environment to protect your firm and safeguard your clients' and staff's identity.

Mari J. Frank is an attorney, CIPP and creator of "The Identity Theft Survival Kit," the audiocassette series "Identity Theft Prevention and Survival," and author of "From Victim to Victor: A Step by Step Guide for Ending the Nightmare of Identity Theft," "Safeguard Your Identity: Protect Yourself with a Personal Privacy Audit," and "The Complete Idiot's Guide To Recovering From Identity Theft" (just released). Mari hosts Privacy Piracy, a weekly public affairs radio show dedicated to privacy issues. Ms. Frank has testified many times on privacy issues in the California legislature and in the US Congress and in 1999 spoke a press conference with President Clinton on Consumer Privacy. Mari's TV special, "Identity Theft: Protecting Yourself in the Information Age" aired nationwide. Mari consults for corporations and government agencies and serves as an expert witness on privacy and identity theft cases. She has served on the Identity Theft Task Force and the Task Force on Privacy. She's an Advisory Board Member of the Identity Theft Resource Center and the Privacy Rights Clearinghouse. She is also a Privacy Fellow with the Ponemon Research Institute and a law professor teaching at the University of California, Irvine. Mari has appeared on dozens of national TV programs, has been interviewed on more than 350 radio shows, has been featured in major newspapers and her many articles have been published in legal journals and numerous magazines. Learn more at: www.identitytheft.org; www.kuci.org/privacypiracy; www.MariFrank.com

[20] Online Privacy Protection Act of 2003 – California Business and Professions Code §§22575-22579.
[21] Visit www.identitytheft.org ; www.privacyrights.org; www.ftc.gov; www.idtheftcenter.org.
[22] Visit www.FTC.gov and the California Office of Privacy Protection for updated laws at www.privacy.ca.gov.
[23] For help in creating the written plan visit: www.ftc.gov/bcp/edu/microsites/redflagsrule/RedFlags_forLowRiskBusinesses.pdf.

The Ivory Tower in the Cloud

By Tanya L. Forsheit

Institutions of higher learning are often breeding grounds for experimentation and creative approaches to old problems. Thus, it is far from surprising that universities have represented some of the earliest adopters of enterprise cloud computing solutions. Cloud computing is enormously attractive to universities, for a number of reasons, especially when it comes to email. The cost of internally hosting email is particularly acute at colleges and universities: "the cost to a college of hosting e-mail accounts as an Internet Service Provider (ISP) has grown more expensive. And students, faculty and staff use e-mail differently today than they did in 1999, swapping large files and subscribing to content-heavy e-mail services."[1] Outsourcing those hosting responsibilities to a cloud provider, with all the appeal of the cloud's rapid elasticity and scalability, is likely to find many champions in the university community.

Interestingly, because many universities have been early adopters of these services, some have already reached the point of identifying real world potential downsides of the approach, particularly when it comes to information security. This article briefly explores some of the information security and privacy legal implications for higher education moving into the cloud, and then discusses some recent developments with respect to highly publicized trials of cloud computing services by universities and colleges.

Privacy and Security Legal Considerations

Universities must comply with the usual panoply of privacy and data security laws, and more. These laws may require various kinds of notices to and consent from faculty, students, and other stakeholders, plus implementation of security safeguards, and contractual imposition of similar requirements on cloud provider partners. The relevant applicable laws may include:

- dozens of non-sectoral state data security laws requiring everything from "reasonable security" to more specific safeguards, most notably Massachusetts' new data security regulations;[2]
- state encryption laws;[3]
- the Family Educational Rights and Privacy Act (FERPA),[4] discussed in more detail below;

---

[1] Seth F. Gilbertson and Joseph C. Storch, "Cloud Contracting: Outsourcing E-MAIL@YOURUNIVERSITY.EDU," NACUANOTES, Volume 8, No. 4, December16, 2009.

[2] *See, e.g.,* Ark. Code Ann. §4-110-104(b); California Civ. Code §§ 1798.81 & 1798.81.5; Colo. Rev. Stat. Ann. §6-1-713; Connecticut HB 5658; KRS §365.720 to .730; Maryland Com. Law Code Ann. § 14-3503; Massachusetts M.G.L. c. 93H and 201 CMR §§ 17.00-17.05; Nevada Rev. Stat. §§ 603A.210 and 603A.215 (SB 227); Oregon Rev. Stat. § 646A.622; Rhode Island Stat.; § 11-49.2-2; Tex. Bus. & Com. Code §§ 521.001 et seq.; Utah Code Ann. § 13-44-201; Wash. Rev. Code Ann. §19.215.020 to .030.

[3] Massachusetts M.G.L. c. 93H and 201 CMR §§ 17.00-17.05; Nevada Rev. Stat. §§ 603A.210 and 603A.215 (SB 227).

- the Health Information Portability and Accountability Act ("HIPAA") Privacy Rule[5] and Security Rule,[6] and the Health Information Technology for Economic and Clinical Health Act (the "HITECH Act")[7] – both as they apply to covered entities (e.g., university hospitals and health plans) and business associates (the more extensive higher education community that may provide services to covered entities);
- the Fair Credit Reporting Act (FCRA) and Fair and Accurate Credit Transactions Act (FACTA) amendments,[8] including the Red Flags Rule;[9]
- 46 State Breach Notification Laws;[10]
- the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act);[11]
- the EU Data Protection Directive[12] and EU member country implementing legislation;
- Canada's Personal Information Protection and Electronic Documents Act (PIPEDA);
- Mexico's newly enacted Data Protection Act;[13] and
- other foreign laws.

Cross-Border Data Transfers

A university email system that involves cross-border data transfers (with faculty and/or students who reside abroad) must also put in place compliance mechanisms such as Safe Harbor certification, standard contractual clauses, and/or binding corporate rules, and impose additional privacy and security requirements on a cloud provider and/or restrict the locations where data can be transferred (often defeating some of the benefits of using the cloud).

FERPA

FERPA is designed to safeguard the confidentiality of student "educational records," i.e., records that "contain information directly related to a student." FERPA protects such records found, among other places, in faculty and staff email. Subject to certain exceptions, FERPA requires a university to obtain consent prior to sharing the content of any education record with third parties, including outside contractors such as cloud providers.[14] One exception allows sharing with a contractor "to whom an

---

[4] 20 U.S.C. § 1232g.
[5] Standards for Privacy of Individually Identifiable Health Information, 45 C.F.R. Parts 160 and 164.
[6] Security Standards for the Protection of Electronic Health Information, 45 C.F.R. Parts 160 and 164.
[7] 42 USCA § 300jj *et seq.* and § 17901 *et seq*.
[8] 15 USCA § 1681 *et seq.*
[9] 72 Fed. Reg. 63,718.
[10] See National Conference of State Legislators, State Security Breach Notification Laws As of April 12, 2010, available at http://www.ncsl.org/Default.aspx?TabId=13489.
[11] Public Law 107-56.
[12] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.
[13] See Lina Ornelas, "Mexico passes Federal Data Protection Act," IAPP Daily Dashboard, April 30, 2010, available at https://www.privacyassociation.org/publications/2010_04_30_mexico_passes_federal_data_protection_act/.
[14] 34 C.F.R. § 99.31.

agency or institution has outsourced institutional services or functions" because such a contractor "may be considered a school official"[15] if it (1) performs an institutional service or function for which the university would otherwise use employees; (2) is under the direct control of the university with respect to the use and maintenance of education records; and (3) is subject to the requirements of the rules[16] governing the use and re-disclosure of personally identifiable information from education records.[17]

Thus, FERPA requires that additional data security obligations be imposed on cloud providers via contract.

Indemnification for Data Security Breaches

Universities across the United States have suffered data security breaches of all shapes and sizes.[18] One particularly egregious incident demonstrates the potential scope of such events. In late 2006, the University of California at Los Angeles notified more than 800,000 current and former students, faculty and staff that their names and certain personal information, including Social Security numbers in some cases, were exposed after a hacker broke into a campus computer system.[19] The media reported that, in the first half of 2006, "there were at least 29 security failures at colleges nationwide, jeopardizing the records of 845,000 people, compared to about 800,000 in the UCLA breach alone."[20]

Due to the susceptibility of universities to certain kinds of security breaches, universities might be particularly wary of relinquishing control of their network to cloud providers without adequate security assurances and broad indemnification rights in the event of a security incident caused by an act of a cloud provider (whether negligent or willful). It is imperative that universities consider these and many additional issues in negotiating cloud contracts, and that they consult with internal and/or outside counsel long before any such agreement is considered or executed, beginning at the RFP and due diligence stages.

Evidence Preservation and E-Discovery

In addition, universities, like other organizations, are subject to evidence preservation and discovery obligations. Data preservation, retention, and disposal obligations extend to data in the cloud. Information in the cloud is another form of potentially discoverable electronically stored information (ESI). Universities that may be engaged in litigation and/or subject to third party investigations and subpoenas (and that will include nearly every university) must plan ahead and discuss treatment of cloud data (a) in records retention policies; and (b) at the Rule 26 conference.

---

[15] 34 C.F.R. § 99.31(a)(1)(i)(B).
[16] 34 C.F.R. § 99.33(a).
[17] 34 C.F.R § 99.31(a)(1)(i)(B).
[18] See, e.g., http://datalossdb.org/search?org_type[]=Edu.
[19] Lloyd de Vries, "UCLA Data Breach Leaves 800K At Risk: Hacker Breaks Into Computer System, Some Social Security Numbers Obtained", CBSNEWS, December 12, 2006, available at http://www.cbsnews.com/stories/2006/12/12/tech/main2249716.shtml?source=RSSattr=HOME_2249716.
[20] *Id.*

University records retention policies and procedures must address the need to suspend routine disposal and recycling of information in the event of a litigation hold requiring the ongoing preservation of certain categories of data that may be relevant to current or future litigation. One of the unique attributes of the cloud is the ability to quickly and inexpensively replicate data for backup and disaster recovery purposes. Cloud users may not even realize how many copies of their data exist in a cloud environment, or where.

Cloud agreements should also address how the cloud user and cloud provider will cooperate in responding to party or non-party discovery requests. The agreement should address the following questions, among others: In the event of a Rule 34 request to the university, how will the cloud user access the data in the cloud? Rule 34(b)(2)(A) provides 30 days to respond in writing to a document request. How quickly will the university be able to access the data in order to review it for discovery purposes? In the event of a subpoena to a non-party cloud provider, how will the cloud provider respond? Will the cloud provider notify the university, and how quickly? Will the cloud provider seek a protective order to prevent and/or limit the disclosure of the cloud user's data? Is the cloud provider even legally required to turn over the data under the Stored Communications Act or other statutes?

Further, it is important to note that the mere processing of personal information of EU data subjects (e.g., faculty and students) for US discovery purposes could very well violate EU member country privacy laws and/or blocking statutes. Universities considering use of the cloud must evaluate whether the cost savings associated with using the cloud outweigh the costs associated with processing data for discovery purposes if and when that becomes necessary.

Campuses in the Cloud . . . or Not

In light of the complex legal landscape described above, one might expect that universities would shy away from taking flight into the cloud. To the contrary, a number of institutions have sought to become early cloud users and champions, with mixed results to date.

Some universities have been quick to make the move to the cloud. Early adopters include the University of North Carolina at Greensboro, the University of Texas at San Antonio, Hofstra University, Abilene Christian University, Arizona State University, the University of Southern California, Northwestern University, Georgetown University, and North Carolina State University.[21]

But there have been privacy and security issues, even at this early stage. In September 2009, students at several colleges were reportedly able to read each other's e-mail messages because of a software

[21] "When E-Mail is Outsourced," Inside Higher Ed, November 27, 2007, available at http://www.insidehighered.com/news/2007/11/27/email; "Forward Into the Cloud," Inside Higher Ed, September 30, 2009, available at http://www.insidehighered.com/news/2009/09/30/email; Vanessa Jo Roberts, "Above the Ivory Tower: Colleges and universities that have made a real-world move to cloud computing find it pays off," EDTECH, January-February 2010, available at http://www.edtechmag.com/higher/january-february-2010/above-the-ivory-tower.html.

bug in Google Apps.[22] At Brown University, one of the affected institutions, "some students, when logging in to their e-mail accounts, were able to see another student's entire in box, while still receiving their own mail. Other students were able to see fewer than 100 messages belonging to another student."[23]

Very recently, in early May 2010, the perceived privacy and security challenges were significant enough to convince one large university to forgo the cloud, at least for now. The University of California Davis ended its pilot (for 30,000 students and staff) of the Google Apps for Education email system due to faculty members' concerns regarding Google's ability to maintain the privacy of their correspondence.[24]

According to published reports, in a joint letter to employees, UC Davis CIO Peter Siegel, Academic Senate IT chair Niels Jensen, and Campus Council IT chair Joe Kiskis wrote that, in addition to the concerns of faculty, "outsourcing e-mail may not be in compliance with the University of California Electronic Communications Policy," which forbids the university from disclosing or examining the contents of e-mails without the account holder's consent, and from distributing e-mails to third parties. The letter reportedly stated: "Though there are different interpretations of these sections, the mere emergence of significant disagreement on these points undermines confidence in whether adopting Google's Gmail service would be consistent with the policy."[25]

As the cloud industry matures, it will be instructive to observe the successes and failures of the highly regulated higher education industry in the cloud environment.

In the meantime, it appears that many university administrators may be spending their summer vacations under cloudy skies.

Tanya L. Forsheit, a founding partner of InfoLawGroup LLP, is based in Los Angeles. Prior to founding InfoLawGroup in 2009, Forsheit was a litigator and privacy/data security counselor at Proskauer Rose, where, most recently, she was co-chair of the Privacy and Data Security group. In 2009, Forsheit was named one of the Los Angeles Daily Journal's Top 100 women litigators in California. Forsheit is certified as an information privacy professional by the IAPP and co-chairs the Cloud Computing Law Working Group of the Information Security Committee. She can be contacted at tforsheit@infolawgroup.com.

---

[22] Simmi Aujla, "Colleges' Transfer to Gmail Accounts Sends Students Mixed Messages," The Chronicle of Higher Education, September 17, 2009, available at http://chronicle.com/blogPost/Colleges-Transfer-to-Gmail/8107/.
[23] *Id.*
[24] Paul McDougall, "Exclusive: Gmail Ditched By Major University," InformationWeek, May 5, 2010, available at http://www.informationweek.com/news/windows/security/showArticle.jhtml?articleID=224700847; Zack Whittaker, "UC Davis scraps Gmail pilot: Privacy levels 'unacceptable,'" ZDNet, May 7, 2010, available at http://www.zdnet.com/blog/igeneration/uc-davis-scraps-gmail-pilot-privacy-levels-unacceptable/4958?tag=mantle_skin;content.
[25] McDougall, "Exclusive: Gmail Ditched By Major University."

Developing The Security Mindset - An Evolutionary Process

By Mike Ahmadi

I did not start my life in the world of technology as a security professional. In fact, the first time I became aware of the concept of security professionals in the world of technology I was convinced that there was no possible way anyone could make a career out of it. Computer security, as far as I was concerned, was about having a good virus scanner installed and keeping it updated with virus definitions. Oddly enough, that worked (or at least seemed to work) for awhile. I did not get any computer viruses (or at least according to my virus scanner), and everything seemed to work as expected. This was my mindset during the 1998-2000 period of my computing life.

In 2000 I took a MIS (Manager of Information Systems) job at a medium sized retail organization in the Silicon Valley area. This organization was not a technology company, but had indeed embraced technology as a way to drive profit. When I joined the organization they had already moved from a paper based customer facing system to one which was completely computerized, and the retail locations (36 at the time) all connected to a centralized system in the corporate office over the internet. While this may not seem like a big deal today, it was fairly sophisticated at the time.

It was not without its issues, however. The high speed Internet pipes were expensive and not nearly as reliable as they are today. The majority of the stores were connected to the central servers via a frame relay based system, and while pitifully slow, it was a very reliable connection. A few of our stores, however, were connected via DSL. The company had contracted with a provider of video surveillance services for the retail locations, and the service included a DSL connection, which was used to stream the video feed to the retail office. As part of our agreement with the video surveillance company we were permitted to use part of the DLS connection to connect to our retail system. This was a big win (or so it seemed) for the company, since this meant not having to pay for the DSL line (except as part of the surveillance service, of course).

The initial testing went well. It was determined that the stores on DSL could process transactions faster, and consequently brought in higher revenues. This excited our CEO and Board of Directors and we decided to move forward with connecting all stores via DSL. We soon discovered, however, that our Internet connection at the central office was incapable of handling the additional traffic. It meant having to get a “fatter pipe” at the office. This was no major issue at this point, as we had determined that the cost would be more than offset by the increased revenues. Within a few short months we quadrupled our capacity, and our stores were happily connecting at breakneck speeds.

Within a very short period of time, however, the stores began complaining that the system was getting slower. I ran some tests and discovered that this was indeed true. Further investigation revealed that

there was a massive amount of outbound traffic coming from our FTP server, which was used to upload and archive video from the stores. It made no sense that we should have ANY outbound traffic whatsoever.

What my investigation uncovered was indeed surprising. Apparently someone had logged into my FTP server, created a folder, and uploaded pirated movies into it. When I viewed the FTP server logs I discovered this happened immediately after we created the speedier connection to the Internet. The logs indicated literally hundreds of users from all over the world had been logging into the open FTP server and either uploading or downloading movies. It started out with only a few per day at first, but after a short time (approximately one week) our office became a major transportation hub for illegal file sharing.

This both annoyed me and intrigued me, so I did some more investigating and discovered that some of the same users that were now living on my network had been there before we had brought in our faster lines, but they essentially dropped by, logged in, and quickly logged off.

So what did this tell me? The slower speed Internet connection was essentially not worth bothering with, since pirates like fast Internet connections, which facilitates fast file sharing. Although they had visited many times before, they did not choose to exploit our network until it became interesting to do so. We had been lulled into a completely false sense of security simply because we had never faced the repercussions of a compromised environment.

I went to work securing things right away. I did my homework. I followed all the “best practices” guidelines available at the time.

...or did I?

Truthfully, I did not follow all the “best practices” guidelines. That was too much work and it would mean having to implement quite a few changes that would lead to a bunch of irritated co-workers. Among the best practices recommended back then:

- **Approved Software Only** – I tried this for a while, and it led to many irritated staff members. People who spend a lot of time at their computers like to personalize them. While I succeeded in stopping this for a short time, it led to a bunch of co-workers who did not like me. I later changed this rule to one where I specified specific known problematic programs (i.e. file sharing, known spyware), or programs that generated undue traffic to and from specific workstations.
- **Password Policies** – At first I tried making users change passwords frequently (every 30 days), and also forced complex password policies. This led to either lots of phone calls from users who forgot their new passwords, or users writing them down and sticking them up on their

corkboards, monitors, or wherever they found convenient. I later changed this to simply require complex passwords (numbers and letters).

- **No Remote Access** – This simply would not work, since our entire network was based on stores with remote access.
- **Hardware Firewall** – At first I tried to use settings on our network router to manage firewall settings. As the network grew this ended up being more trouble than it was worth, since it meant having to manage both internal and external firewall policies through a device that was not purpose designed for this. We eventually brought in appropriate hardware specifically for this task.
- **Strict Access Control** – When I started with the company, anyone who was allowed into the network had access to far more than their job required. It was simply much easier that way. This had to eventually change. Initially I simply gave groups of users access to large areas, but eventually narrowed this down to very compartmentalized and specific areas. While users were not happy that they could not access some parts of the network, they eventually got used to it.
- **No Outside Devices** – Back in the year 2000 outside devices where not a very big deal. Cell phones were, by and large, dumb devices. The most common "smart" device was a PDA, and I could count the number of users in my office on one hand (and that included me). This changed at an astounding pace. Over the next five years nearly everyone had a portable device of some sort that they wanted to connect to their computer, and over the next three years it seemed as if everyone had a personally owned smart device. During the early days of personal computing devices it was somewhat simple to monitor what was going on. It became nearly impossible once everyone had his or her pet devices.

I implemented what I felt was enough to keep us from being "owned" by outsiders without forcing anyone in the office to make any changes. This worked well for a little while, and then we ended up infiltrated again.

This time around the unwelcome guests were very clever about how they got in. It took me a while (several days) to figure out what was going on because they entered the network through a Windows based buffer overflow attack (one of many that the operating system seems to be susceptible to). I discovered this by literally going through every folder and file on the system and looking for anything that seemed out of place. I did a bit of web searching when I found something unusual, and that was when I discovered that one of our machines had been infiltrated during a period of time when an exploit had been discovered by enterprising young hackers and posted to the web, and the time Microsoft issued a patch to fix it. Sure, I had applied the patch, but the attacker got to me before I applied it.

What astounded me about this particular attack was what the attackers did once they got in. They used the built-in Windows FTP client to connect to their own FTP server and downloaded an

application called FireDaemon[1] and another called Serv-U.[2] The FireDaemon application allows you to run any designated application as a Windows Service, meaning that it can be allowed to run in the background every time the machine is rebooted, and without any user knowledge. The Serv-U application is a commercially available FTP server, which allows for the easy creation of a file server on any Windows machine, regardless of type. Typically if an organization chooses to run an FTP server and they have Windows servers installed, they will use IIS (Internet Information Services) on that machine, which includes an FTP server. While we did have other machines on the network running IIS, we did not have it installed on this particular machine. By installing an FTP server on this machine, the attacker created an environment that my IT staff and I overlooked entirely. Moreover, the attacker did not choose to serve files (which, incidentally, were pirated movies and software) through the common port 21 (the default FTP port), but chose a completely different available port.

…and their cleverness did not stop there. They also hid the application folder in the Recycle Bin folder. Since this was a file server, nobody bothered to empty the Recycle Bin. Why would we? We did not regularly create any digital trash on this machine.

Now this completely changed my outlook on being a system administrator. I now realized that I had to monitor "geek" websites (such as Slashdot) and always be up to speed on the latest news so I could gain awareness well in advance of the potential attack. I HAD to pro-actively take control of our network security posture before something disastrous happened.

At first this was very painful for me! It meant adding something to my daily ritual that would never go away. It also meant actively monitoring server logs for any and all activity, and then trying to find unusual patterns. It meant instituting AND ENFORCING policies that users found completely annoying. And it also meant investing in tools and hardware to reinforce our system (although this was minimal). It was an effort that required changing everyone's mindset about how to conduct oneself in an ever-growing connected world.

I quickly learned that there was no "set it and forget it" way to deal with security. Every time something new and interesting became a part of the world of technology, it presented me with a new security challenge. Every iPod, USB stick, digital camera, Smartphone, social network, or web based application meant a new avenue for an attacker to get in. I literally began looking at everything as something that could be exploited, and I would work out elaborate plans in my mind on how I could go about it. This did not make me paranoid, as it tends to make some people feel. It made me feel somewhat empowered. I felt like I was in control. I had situational awareness.

Some people I know find it very easy to adopt this mindset. Some people find it quite annoying. In order for an organization to systemically adopt this mindset the people who make up the organization

[1] http://www.firedaemon.com.
[2] http://www.serv-u.com.

need to be made aware of specific pieces of information, and much of the information tends to appear hyperbolic. If a user comes back from a conference with a free USB thumb drive from a vendor booth, or one he used at his home computer (which was infected with malware), there is a very real possibility that he could install malware (such as a key logger) on his workstation by plugging it into the USB port.[3] That nifty digital picture frame your children got you for Christmas could be infected right out of the box,[4] and while it may seem completely safe to plug it into your computer and transfer photos to it, it may contain an unwelcome visitor.

I remember showing a doctor who was so proud of his new Smartphone that could access patient information through a fairly popular web-based application that was also available through traditional desktop browsers. I asked to see his nifty new phone and immediately turned it on (no PIN protection), and went to the application he mentioned. The application was password protected, so I simply went over to his desktop computer and went to the full website, and when I got to the login page I clicked on the "Forgot Your Password" link and input his email address (which I easily found by opening his mail application on the phone). I waited several seconds and when the phone buzzed I opened the email the website had sent me and told him what his password was. He looked at me in complete amazement, and I told him to consider password protecting his phone.

As a security consultant, I find it quite helpful to both demonstrate some examples of easily accomplished exploits, and to hold occasional meetings with clients to give them an overview of what is going on in the wide world of cyber exploits. There always seems to be someone in the organization that finds cyber crime as fascinating as security experts find it, and that is the person I will spend some time coaching on how to think like an attacker, and encourage that person to spread the word to the rest of the organization.

Most users seem to eventually adapt to the need to be more vigilant. It really comes down to technological maturity. To give you a simple analogy, think back to when you were much younger, and perhaps felt it was a good idea to climb the highest tree in your yard, or floor the accelerator of your car to see how fast it can go, or discover how many beers you can put away in a night. When we are less mature, those all seem like good ideas (or at least they do not seem like bad ideas), but as we mature we discover that climbing trees could lead to falling to your death or flooring the accelerator of your car can lead to an accident. As we mature do not necessarily have to experience the negative consequences of bad decisions in order to know that they can create problems. Most of us develop a "safety first" mindset as part of the maturity process, and that mindset seems to serve those who adopt it quite well.

Those who are a bit more mature in their understanding of security truly need to be more helpful to those who are not, and remember that much like a parent who is trying to teach their children how to

[3] http://www.scmagazineus.com/ibm-distributed-infected-usb-drives-at-conference/article/170862.
[4] http://www.securityfocus.com/brief/670.

be safe, it is important to work on your approach and delivery. Being heavy handed can lead to rebellious behavior in all but the most submissive among us. Working towards a common understanding is the most effective approach. Rather than snapping at an employee who loses his access card for the third time, ask him where he normally keeps his access card after he uses it, and if there is some way to make it easier for him to remember where he left it. Perhaps you may discover that simply having this conversation makes him feel less like someone who is being "ordered" to do something and more like someone who is expected to act more responsibly. Perhaps you may learn that you should reconsider your plan for securing your environment. Getting everyone involved means that they take ownership, and you might be surprised at how much easier security becomes once that happens.

Mike Ahmadi has extensive experience in project management, information systems, mobile computing, Smart Grid and cyber security regulatory affairs, in addition to threat modeling, risk analysis, anti-cloning, anti-counterfeiting and client/server applications. He is a core voting member of the California Privacy and Security Advisory Board (CalPSAB) Security Committee, whose focus is the creation and management of health care security policies for the State of California Office of Health Information Integrity (CalOHII). He is currently assisting in the drafting of security requirements for the Smart Grid deployment of the California Public Utility Commission (CPUC). He also co-founded the RFID Security Alliance, which serves to educate stakeholders about security issues surrounding RFID solutions.

2010 Information Law Updates – Cases, Statutes and Standards

By Thomas Shaw

In the first six months of 2010, there have been a number of developments in U.S. information security and data privacy statutes, cases and standards. This includes state and federal laws and regulations that have been passed or promulgated, are being considered or coming (or not) into force. It also involves civil and criminal cases and enforcements actions brought by regulators. And it encompasses new privacy and security guidelines and standard issued by standards bodies. To describe the major developments in this broad area of law and practice, but keep it manageable, each development is presented with a brief analysis after it. Deeper analyses of these developments can be found in the other articles in this publication and in the various writings and presentations by members of the Information Security committee. While the scope of this article is the first half of 2010, some developments from late 2009 whose implementation affects 2010 are also included.

Statutes and Regulations – Federal

Privacy Bills

In May, draft privacy legislation was introduced in the House of Representatives (the "Boucher" bill). It is designed to protect the privacy of personal information, such that entities that collect such information would be required to:

- Clearly and conspicuously disclose privacy policies
- Provide privacy notices and the opportunity to opt-out before collecting, using or disclosing covered information from or about an individual
- Obtain opt-in consent from individuals before collecting sensitive information (e.g. financial or medical information) or before sharing this covered information with unaffiliated parties
- Establish, implement and maintain appropriate administrative, technical and physical safeguards to protect covered information.

In the Senate, late last year the *Personal Data Privacy and Security Act* (SB 413 or "Leahy bill") was again introduced. It has more comprehensive provisions, including the following:

- Penalties for "intentionally and willfully" concealing a security breach involving "sensitive" personally identifiable information
- Requires data brokers to disclose all personal electronic records upon request and provide procedure for making corrections and provide notice of actions taken against an individual based on this information

- Requires covered entities (except those covered by HIPAA, GLBA or public records) to implement "comprehensive" data privacy and security programs that ensure the privacy, security and confidentially of sensitive personally identifiable information
- Risk assessments must be conducted, risk management and control policies and procedures adopted, employees trained and supervised in security, and vulnerability testing and monitoring implemented
- Notification is required for any security breach allowing access to sensitive personally identifiable information.

Financial Reform Bill – Restoring American Financial Stability Act

This Senate bill (S 3217) attempts a comprehensive reform of financial regulations. Its many provisions (still under review) includes a federal consumer protection agency, regulation of derivatives, a council to monitor and respond to systemic risk, deal with non-bank institutions that are considered "too big to fail" and dealing with how credit rating agencies operate. While the reforms are far reaching, it does not appear that there will be any direct changes to information security or privacy law. But it would be expected that the consumer protection agency will impact consumer privacy rules and the interplay between federal and state privacy protections, given that this bill expressly preempts state law.

Data Accountability and Trust Act

This bill, HR 2221, requires the FTC to create and disseminate regulations requiring those who own, possess or outsource possessing electronic personal information (name, address, phone number, SSN, driver's license number, financial account number) to establish security policies and procedures, including having a person responsible for information security oversight, perform security vulnerability testing and a process for disposing of personal information. Specific rules for information brokers include the need for audits and procedures to verify accuracy, notify individuals of their data held and a means to review and correct it and an opt-in for data used for marketing purposes. There are data breach notification requirements, unless there is no reasonable risk of identity theft, fraud or unlawful conduct (data is "unusable, unreadable, or indecipherable to an unauthorized third party").

HIPPA/HITECH Regulations

The Department of Health and Human Services Office of Civil Rights (HHS OCR) has to promulgate new regulations for the *Health Information Technology for Economic and Clinical Health* (HITECH) Act, as amended by the *Health Insurance Portability and Accountability Act* (HIPAA). These include requiring business associates to implement the same level of information security (administrative, physical and technical safeguards) and privacy as covered entities, new privacy protections for personal health information (PHI) such as minimum necessary disclosure, accounting for disclosure and prohibitions on sale of PHI and breach notification provisions for unsecured (i.e. unencrypted) PHI. Even though these provisions of HITECH became effective from mid-February, extension of HIPAA privacy and security requirements to business associates and the new privacy protections may not be enforced until

specific guidance has been finalized. But the breach notifications obligations for both covered entities and business associates under the Interim Final Rule have already come into effect.

Informed P2P User Act

This bill, HR 1319, passed the House and requires file-sharing program developers / distributors to provide "conspicuous notice" before program installation and first use so that installed user is aware of the program and what files will be searched and copied and obtaining informed consent. It would also be illegal to not allow users to block or remove or disable such programs. Violations are considered unfair trade practices under the FTC Act.

Patriot Act Extension

This one-year extension of the PATRIOT Act did not include the originally proposed enhanced privacy protections. These protections included easier challenges to national security letters, protections for library records, limitations on the preservation and dissemination of surveillance records. This means that the following provisions will remain in effect: Court-approved roving wiretaps, court-approved seizures of records related to anti-terrorism and surveillance of a non-US citizen who may is engaged in terrorism outside a recognized terrorist group.

Cybersecurity Bills

In February 2010, HR 4061 the *Cybersecurity Enhancement Act of 2010* passed the House. This requires ongoing plans for research and development in cybersecurity and provides grants for research into identity management, as well as in the detection, investigation, and prosecution of cyber-crimes involving organized crime, intellectual property, and crimes against children. It also requires NIST to develop checklists of settings and options that minimize security risks associated with computer systems that are, or are likely to become, widely used within the federal government, to coordinate U.S. representation in the international development of technical standards related to cybersecurity and to implement cybersecurity awareness and education programs.

In the Senate, S 773, the *Cybersecurity Act of 2010*, was reintroduced this year. It tries to organize the federal cybersecurity efforts and to increase collaboration between the public and private sectors. It requires NIST to establish cybersecurity standards for all federal government and related critical infrastructure information systems and networks and work internationally on standards. The Secretary of Commerce is to develop professional cybersecurity certifications and to act as clearinghouse for cybersecurity threat and vulnerability information and produce annual reports on such. It requires the National Science Foundation and NIST to support research, scholarships and competitions in this area.

Federal Trade Commission

The FTC has had a number of recent announcements and actions.

- *COPPA*: A review of the *Children's Online Privacy Protection Act* will occur five years early and public comment sought on this law that prohibits websites from collecting, using or disclosing personal information from children under 13 years of age without prior parental permission. The requested input involves: the implications of interactive TV, interactive gaming and mobile communications; whether the definition of personal information should include fixed IP address, mobile geolocation data or information collected from children online; impact of centralized authentication and the availability of additional technological methods for verifiable parental consent and whether parents are using their rights therein and operators' experiences.

- *Exploring Privacy Roundtables*: Three public roundtables sessions were held by the FTC to explore the privacy challenges posed by "21st century technology and business practices" that collect and use consumer data. These include: social networking, cloud computing, online behavioral advertising, mobile marketing, and the collection and use of information by retailers, data brokers and third-party applications. The goal for these sessions was to discuss how to protect consumer privacy while supporting beneficial uses of information and technological innovation. Other privacy topics covered in the sessions included: consumer expectations and disclosures, technology and privacy; Internet architecture and privacy, health information, addressing sensitive information, lessons learned and looking forward.

- *Red Flags Rule*: In late May, the FTC again delayed enforcement of the Red Flags Rule, this time until December 31, 2010. This provides Congress time to consider the scope of entities covered by this rule. Originally developed under the Fair and Accurate Credit Transactions Act (FACTA) to have creditors (any entity that regularly extends credit) and financial institutions address the risk of identity theft with written prevention programs that indentify, detect and respond to "red flags" that could indicate potential identity theft. There are five types of listed red flags:
  - Alerts, notifications, or other warnings received from consumer reporting agencies or service providers, such as fraud detection services
  - The presentation of suspicious documents
  - The presentation of suspicious personal identifying information, such as a suspicious address change
  - The unusual use of, or other suspicious activity related to, a covered account
  - Notice from customers, victims of identity theft, law enforcement authorities, or other persons regarding possible identity theft in connection with covered accounts held by the financial institution or creditor.

- *Internet Privacy Framework*: The FTC announced its intention to create Internet privacy guidelines that would bring more transparency to what marketers do with consumer data. In particular, there is a desire to protect consumers and their data from abusive practices from search engines, social networks and location tracking services. Drivers behind this include the

recent privacy policy changes to social networking site Facebook and location tracking of mobile device users.

- *GLBA Final Model Form*: The FTC and other federal regulatory agencies released in late 2009 a final rule that amended the privacy rules under the Gramm-Leach-Bliley Act (GLBA). The Final Model Privacy Form can be used by financial institutions to describe their privacy policies and how consumers can opt out of letting their information be disseminated to unaffiliated third parties. This form is not required but its proper use will allow compliance (safe harbor) with the respective obligations for initial and annual privacy notice to the consumer on disclosure of his/her non-public personal information and for opt-out notice for how to avoid sharing their information with unaffiliated third parties. There are three versions of the model form, allowing opt-out by mail, by telephone/online or no opt-out option. The existing sample clauses are no longer the approved safe harbor for compliance after December 31, 2010. This final rule became effective on December 31, 2009.

- *Guidelines on Endorsements*: The FTC issued newly revised guidelines for advertisements on social networks, blogs, wikis, chat rooms, discussion groups, tweets, email broadcasts, virtual worlds or other Internet sites. These guidelines spell out the required transparency and disclosure of material relationships between someone endorsing a product or service and the product maker / service provider and any compensation therein. This brings this newer media into line with advertising on older media like television, print and radio.

- *Probe on Peer to Peer Networking*: A "wide-ranging" FTC probe found more than 100 public and private organizations whose data was comprised by peer-to-peer file sharing networks. The FTC sent breach notices to the effected organizations and recommended that organizations not allow such technologies and that the protection of sensitive information should be appropriate with the sensitivity of the data.

- *Copy Machine Memory*: The FTC is working with copy machine manufacturers, resellers and retailers on restricting the ability of photocopiers to store digital images on their internal hard drives. A news report showed how the copiers keep images of everything that they copy, creating a potential huge source of confidential information available to identify thieves, blackmailers and other parties in litigation. The report showed that used copy machines still had information on private medical information, sex crimes, social security numbers and paychecks. The FTC, along with these sellers, will try to educate consumers about this privacy issue.

Financial Industry Blogs and Social Networking Web Sites

In January, the Financial Industry Regulatory Authority issued *Guidance on Blogs and Social Networking Web Sites* for securities firms, investment advisors and brokers. This follows previous guidance on

interactive websites. These firms should adapt appropriate policies and procedures, supervise employees' activities on these sites, retain records of communications through these types of sites and monitor the content on their own sites. The Commodities Futures Trading Commission approved amendments on the use of social networking by its members when communicating with the public. These communications are subject to the same standards as other types of communications with the public.

Statutes and Regulations – States

Washington State - Damages for Card-related Data Breaches Law

The Washington state legislature passed HB 1149 in March to encourage reissuance of debit and credit cards when a data breach has occurred and thereby reduce the possibilities of identity theft. It also lets financial institutions who issue such cards recoup their actual financial losses from processors, businesses and certain hardware and software vendors (who are involved in the processing, storage or transmission of card data or that maintains such data not its own) who are negligent in "maintaining or transmitting card data." Only businesses that process six plus million card transactions a year are in scope. These entities can escape liability if the data was encrypted or if they were "certified compliant" with PCI DSS. It covers residents of Washington state and is effective from this July.

Maine – Marketing to Minors Law

To fix last year's *An Act To Prevent Predatory Marketing Practices Against Minors*, this year Maine's legislature passed LD 1677, *An Act to Protect Minors from Pharmaceutical Marketing Practices* that repeals the previous law and prohibits the collection and use of personal information collected on the internet from a minor child between 13 and 17 years of age for use in pharmaceutical marketing. The law is to work in synch with the federal *Children's Online Privacy Protection Act* (COPPA), although it has a few differences.

Virginia - Medical Information Data Breach Law

Virginia has enacted a data breach notice law (VC §32.1-127.1:05) for medical information. This is for any medical information that is unencrypted or not redacted and compromises its security, confidentiality or integrity. The medical information is a Virginia resident's name plus information on medical history, condition or treatment or a health insurance unique identifiers. This supplements Virginia's data breach notification law that applies to those with personal information on Virginia residents. It is effective from January 1, 2011.

California - Data Breach Revision Law

The California Senate has passed SB 1166, which attempts to modify the state's data breach notification law. The existing law requires that the entity that loses unencrypted personal information to send breach notification letters to all those affected. The new bill addresses the specific information in the notification letters, including the type of personal information lost, a description of the incident,

and when it took place, as a number of other states currently require. It also requires the letter be sent to the state's Attorney General if more than 500 people are affected.

Utah – E-commerce Law

This year Utah passed the *E-Commerce Integrity Act*. This statute prohibits "fraud and injury" through electronic communications, which is defined as phishing and "pharming" (creating a webpage that purports to be associated with a legitimate business without that business' approval). It also allows removal of domain names and online content by ISPs under certain circumstances such as use in phishing or pharming and forbids the use of spyware to change settings on an Internet PC (e.g. bookmarks), forbids collection of personally identifiable information through deceptive means, prevents blocking of such software or other deceptive practices that causes harm to the computer or its contents. There are exceptions for services providers and authorized software updates. It also prohibits the registration of domain names under certain circumstances for violating cybersquatting provisions in regards to use of famous marks. It becomes effective on July 1, 2010.

Massachusetts – Information Security Regulations

Massachusetts' information security law (*Standards for the Protection of Personal Information of Residents of the Commonwealth*) has new regulations became effective on March 1, 2010. These require businesses controlling (owning or licensing) information about Massachusetts resident to implement and maintain a comprehensive, written information security program with administrative, physical and technical security controls. The objectives of the regulations are to ensure the security and confidentiality of Massachusetts citizens' personal information, protect against anticipated threats or hazards to the integrity of that information and protect against unauthorized access to or use of such information. Among its many specific requirements are:

- Developing information security policies and designating a program leader
- Inventorying personal information and oversighting third-party service providers
- Monitoring the program and performing annual reviews
- Monitoring for unauthorized use and incident management procedures
- User authentication and access control procedures
- Encryption of transmitted records and stored data on mobile devices
- Up to date network and system protection software
- Employee security training

Nevada - Encryption and PCI Standard Law

Nevada's *Security of Personal Information Law* became effective Jan. 1, 2010. This law requires the use of the PCI DSS standard for companies doing business in Nevada and accepting card payments. It also requires the use of encryption for any electronic transmission of personal information (besides a fax) to someone outside the sender's secure system (logical and physical controls) or when moving personal information on a data storage medium outside those controls.. Nevada law also requires businesses to

destroy personal information when no longer needed, to take reasonable security measures to protect personal information from unauthorized access and to disclose data breaches.

Rhode Island – Data Destruction Law

Rhode Island's newly effective data destruction statute requires a business to take reasonable steps to destroy or make unreadable customers' personal information within its custody or control that is no longer to be retained. Each record that is "unreasonably disposed of" is considered a violation of the statute. There are exceptions for financial institutions already under GLBA, health care providers under HIPAA, consumer reporting agencies under FCRA or any business that has entered into a contractual agreement with another business for the destruction of the personal information. The statute went into effect from January 1, 2010.

New Hampshire - Health Information Privacy Law

A newly effective New Hampshire law (HB 619) requires health care providers and their business associates to obtain opt-in consent from individuals before using their protected health information for marketing purposes and the ability to opt-out of receiving fund raising communications that is based on their protected health information. A second law (HB 542) concerns electronic health data exchanges. It allows individuals to opt out of sharing their health information with these exchanges, limits access in the exchanges to health care providers for treatment purposes and requires the exchanges to maintain logs of health care providers that access patient data. This is effective from January 1, 2010.

Mississippi - Data Breach Notification Law

In April of this year, Mississippi (HB 583) became the forth-sixth (46th) state to enact a data breach notification law. This applies to businesses in Mississippi who own, license or maintain the personal information of any Mississippi resident. It requires notice to the affected individuals in the event of a security breach of unencrypted data that would affect these owners or licensors. Violation of this law is considered an unfair trade practice, which requires enforcement by the state attorney general, as there is no private right of action. It becomes effective on July 1, 2011.

Cases – Civil and Criminal

State of Connecticut v. Health Net of the Northeast, Inc. et. al.[1]

The first lawsuit under the HITECH Act was filed by the Attorney General of Connecticut in January 2010. This charges Health Net with violating its HIPAA/HITECH responsibilities in regards to the security and privacy of protected health information (PHI). This originated from the loss of a portable hard drive containing unencrypted information on close to half a million current and former enrollees of these companies. Its practices that allegedly violated its security and privacy obligations included by not encrypting the data, not keeping a log of the transfers on to this portable hard drive, no notice to

[1] *Connecticut v. Health Net of the Northeast, Inc.*, No. 3:10-CV-00057 (D. Conn. filed January, 2010).

affected individuals on discovering the breach, ineffective security procedures and failure to train and supervise its workforce. The specific alleged violations of HIPAA/HITECH include failure to:

- Ensure the confidentiality and integrity of electronic protected health information (EPHI)
- implement technical policies and procedures for electronic information systems that maintain EPHI to allow access only to those persons or software programs that have been granted access rights
- Implement policies and procedures governing the receipt and removal of hardware and electronic media that contain EPHI into and out of a facility to maintain their security
- Implement policies and procedures to prevent, detect, contain, and correct security violations
- Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity
- Protect against any reasonably anticipated threats or hazards to the security or integrity of EPHI
- Protect against any reasonably anticipated uses or disclosures of EPHI that are not permitted under the privacy rules regarding individually identifiable health information
- Ensure compliance with the HIPAA security standard rules by its workforce
- Impermissibly and improperly used and disclosed PHI that is and remains accessible to unauthorized persons
- Effectively train all members of its workforce (including independent contractors) on the policies and procedures to carry out their functions and to maintain security of PHI
- Adequately design policies and procedures establishing physical and administrative safeguards to appropriately and reasonably safeguard PHI
- Maintain an effective and appropriate sanctions policy for members of its workforce (employees and independent contractors) who failed to comply with the policies and procedures for the protection and safeguarding of PHI

Pulte Homes, Inc., vs. Laborers' International Union of North America[2]

The plaintiff brought this suit, including claims under the *Computer Fraud and Abuse Act* (CFAA). The alleged actions included filling up the company's email and phone mail systems through repeated calling and emailing, which kept the plaintiff's employees from conducting their normal functions. The CFAA requires showing that there was "unauthorized access or transmissions to a computer program." The transmissions must be knowingly caused and result in damage to the protected system but the court found that the defendants did not "intentionally" cause harm, even with continued actions after being asked to stop, because they were not informed that these actions were damaging their computers. The first prong requires proof that the defendant "intentionally accessed a protected computer without authorization and recklessly caused damage or damage and loss." The court found that as access means "the freedom and ability to make use of something," there were no such allegations of defendant gaining such freedom or abilities. Further, the court found that sending emails or leaving voicemails did not constitute access under the CFAA.

[2] *Pulte Homes, Inc., vs. Laborers' International Union of North America*, 2010 U.S. Dist. LEXIS 46416 (E.D. Mich. 2010).

In re Heartland Payment Systems, Inc. Securities Litigation[3]

In December of 2009, a lawsuit against Heartland Payment Systems for securities fraud was dismissed. This lawsuit grew out of the cybertheft of credit and debit card information from Heartland's network. Some of Heartland's shareholders filed suit after the disclosure of the data breach led to a decrease in the company's share price. The plaintiffs alleged Heartland had misrepresented the state of its computer security and had concealed a prior attack in SEC filings and other public disclosures. Because the plaintiffs were not able to demonstrate that the statements about its computer security were made with the requisite knowledge ('scienter") or that they were fraudulent within the context, the case was dismissed.

Cumis Ins. Society, Inc. v. BJ's Wholesale Club, Inc.[4]

The top state court in Massachusetts recently upheld the dismissal of claims brought against a retailer BJ's Wholesale Club in connection with a breach of debit and credit card data. After cybercriminals used the stolen cards to initiate fraudulent transactions, certain financial institutions that issued the cards sued the retailer. The court dismissed the various claims as follows. The credit unions were not third-party beneficiaries of the contract between the retailer and the processing bank due to express exclusion of third party beneficiary rights. Negligence cannot be claimed due to the lack of property damage or physical harm . The fraud and negligent misrepresentation theories were based on reliance by the financial institutions of compliance by the retailer with regulations established by the card companies, but this reliance was not justifiable.

Valdez-Marquez v. Netflix, Inc.[5]

In March of this year, a federal court dismissed a not-yet certified class action lawsuit against Netflix, due to a confidential settlement agreement between the parties. This litigation arose out of Netflix's release of anonymized subscriber data on movie ratings in support of a contest it was running. When several of its customers were identified from this released data, the class action suits followed late in 2009, alleging violations of the company's privacy policy in regards to customers' person information, a lack of consent to the release of the information and a failure to property anonymize the data.

Stengart v. Loving Care Agency, Inc.[6]

In March 2010, the New Jersey Supreme Court held that the attorney-client privilege applies to e-mails sent by an employee to her attorney though a personal, Yahoo email account. This was even though she was using an employer-provided laptop (and the emails were in preparation for litigation against her employer). These actions were in violation of the employer's policy that employees have no reasonable expectation of privacy in the communications sent using company equipment and may be monitored, reviewed and disclosed. The emails were found during a forensic examination of the

[3] *In re Heartland Payment Systems, Inc. Securities Litigation,* Civ. No. 09-1043 (D.N.J. 2009).
[4] *Cumis Ins. Society, Inc. v. BJ's Wholesale Club, Inc*., 918 N.E.2d 36 (D. Mass. 2009).
[5] *Valdez-Marquez v. Netflix, Inc*, No. 5:2009cv05903 (N.D. Cal. 2010).
[6] *Stengart v. Loving Care Agency, Inc.* 2010 WL 1189458 (D.N.J. 2010).

laptop, saved by the browser without the employee's knowledge. The court's ruling was that the employee had both subjective and objective reasonable expectations of privacy because the electronic communications policy did not specifically include web-based personal email as those that may be monitored. Also, the policy allowed for occasional personal use of email. In addition, the emails were subject to the attorney-client privilege and contained standard warnings that they may constitute attorney-client communications. It also differentiated an expectation of privacy using a company's own email system. The court also made it clear that even if the electronic communications policy gave unambiguous notice (unlike here) that an employer could retrieve and read an employee's attorney-client communications, if sent via a personal, password-protected e-mail account using the company's computer systems, it would consider this policy to be unenforceable.

Allison v. Aetna[7]

In this case, a federal court in Pennsylvania ruled that a claimed injury by an alleged data breach victim was "far too speculative." The data breach involved those persons who had applied for jobs at Aetna and subsequent phishing emails that some of these people received asked for further information (under the guise of originating from Aetna). The court ruled that data breach victims may assert that there is an increased risk of harm to satisfy the injury in fact prong for standing but that the threat must be credible rather than a mere possibility of future harm (in contrast to the *Pisciotta* case[8]). This was in part because the plaintiff could not verify that his personal information had been accessed or his email account had even been breached, as he has not received one of the phishing emails. The phishing emails searching for additional information led the court of believe that the plaintiff's data had not been compromised sufficiently to put him at risk for identity theft. The court also ruled that time and money spent on credit monitoring did not suffice to meet the injury in fact requirements for standing.

Claridge v. RockYou Inc.[9]

In California, a class action complaint was filed in late 2009 against this developer of social networking applications. The complaint alleges that developer RockYou put its more than 30 million users at risk by improperly storing their personal information in unencrypted databases therefore reasonably foreseeable it would be vulnerable to hackers. When using these applications on sites like Facebook, the users are required to register and so enter their information into RockYou's database. The complaint also asserts that the database was hacked and then not secured until days it was notified of the breach and that it waited more than ten days to notify users of the breach. The concern is that these passwords, in combination with the stolen email addresses, might be used by the users in several other accounts, such as bank accounts. The case is currently pending.

---

[7] *Allison v. Aetna*, Case 2:09-cv-02560-LDD (E.D. Penn. 2010).
[8] *Pisciotta v. Old National Bancorp,* 2007 WL 2389770 (7th Cir. 2007).
[9] *Claridge v. RockYou Inc.*, No. 3:2009cv06032 (N.D. Cal. 2009).

United States v. Ahrndt[10]

In a motion to suppress evidence in a criminal case, the defendant argued that his neighbor (and observing police) connecting to his unsecured wireless network and accessing his iTunes library violated the *Electronic Communications Privacy Act* (ECPA). The court ruled it is not unlawful under the ECPA "to intercept or access an electronic communication made through an electronic communication system configured so that such electronic communication is readily accessible to the general public." Because his wireless network broadcast beyond his house and his iTunes program was configured to share files with any computer joining that network, the court held that the wireless network was "readily accessible to the general public" and so rejected his ECPA claim. The court also found that he had no reasonable expectation of privacy in his files made available by wireless broadcast.

Lane v. Facebook[11]

A federal court in California recently approved the settlement of a class action lawsuit against Facebook for privacy violations regarding its Beacon behavioral tracking system. This system reported back to a Facebook user's friends on their Facebook the online activities (including purchases) of Facebook users, even allegedly those who were not Facebook users or had deactivated their accounts with Facebook. Started in late 2007, forty-four corporate partners agreed to supply Facebook with information about the online transactions of Facebook users. Users were not originally required to opt-in (changed after the initial reaction) and opting out meant visiting each of partner's web sites to prevent their data from going to Facebook. The net settlement funds are to be used primarily to establish a privacy foundation instead of being paid to the almost 4 million class plaintiffs. But the settlement of this suit does not end Facebook's privacy-related litigation, as several class action lawsuits have recently been filed against it and a complaint lodged against it with the FTC.[12]

City of Ontario v. Quon[13]

Recently the U.S. Supreme Court heard oral arguments in the highly publicized case involving the privacy of employee communications. The Ninth Circuit had ruled that the contents of an employee's text messages on the servers of the messaging service provider are protected from disclosure to the employer.[14] This was even though the employer was the subscriber of the text messaging service, not the employee. The appeals court held that the messaging provider was an "electronic communication service" within the *Stored Communications Act* section of the *Electronic Communications Privacy Act*. Therefore the contents of archived text messages could be disclosed only to the intended recipient of the text messages, the employee, and not to the employer subscriber. The court also ruled that although the employer's policy did not provide for an expectation of privacy when using the text

---

[10] *United States v. Ahrndt,* No. 3:08-cr-00468-KI (D. Or. 2010).
[11] *Lane et al. v. Facebook, Inc. et al.*, Case No. 5:08-CV-03845-RS (N.D. Cal. 2010).
[12] *In the Matter of* Facebook, Inc. (filed by EPIC et. al. filed May 2010); see *Gould v. Facebook, Inc*, Case No. 5:10-CV-02389-PVT (N.D. Cal. 2010).
[13] *City of Ontario v. Quon*, No. 08-1332 (U.S. cert. granted Dec. 2009).
[14] *Quon v. Arch Wireless Operating Co., Inc.* (9th Cir. June 2008).

messaging service, the reality was that the employer had led employees to believe that these messages would be reviewed by the employer only in limited circumstances.

Cases – Regulatory (FTC)

Navone[15] – This action was brought over the improper disposal of consumer report information and records. The defendant, who ran two mortgage brokerage companies, was accused of dumping confidential data. The FTC has the power under the Disposal Rule promulgated under FCRA to enforce proper disposal.[16] According to the complaint, contrary to the companies' written statements regarding security practices, they "failed to provide reasonable and appropriate security for sensitive consumer information collected, handled and/or maintained." The FTC has the power under section 5 of the FTC Act to address deceptive trade practices.[17] The defendant also kept some of the sensitive consumer information in an insecure manner in his garage and did not maintain control over third parties with access to such information. About forty boxes of consumer information, including copies of driver's licenses, credit cards and consumer reports, were found in a dumpster outside one of his former offices. The final settlement required payment of a fine, that the defendant does not engage in misrepresentation or security measures and must employ "reasonable measures" to protect credit report information during its disposal and must hire an independent, third-party security professional to review the program annually.

Dave & Buster's[18]
In March 2010, the FTC entered into a settlement with Dave & Buster's, Inc., for alleged violations of the FTC Act, and for practices, "failed to provide reasonable and appropriate security for personal information on its networks." During 2007, according to the complaint, a hacker gained access to the defendant's networks and intercepted credit and debit card information from over 100,000 consumers. Upon discovering the breach, the defendant notified law enforcement officials and credit card companies, and took steps to prevent further unauthorized access. However, the complaint alleges that the defendant had not previously taken reasonable and appropriate security measures to protect personal information. Examples included: a lack of an intrusion detection system, failure to monitor system logs, failed to use network security techniques such as using firewalls to limit access between in-store networks, isolating payment card system from the rest of the corporate network or failing to limit access through network wireless access points. As is typical in these cases, the settlement agreement requires the implementation and maintenance of "comprehensive, written data security program that contains administrative, technical and physical safeguards" protecting the security, confidentiality and integrity of personal consumer information and independent assessments from a qualified third-party.

---

[15] *Federal Trade Commission v. Gregory Navone* (D. Nev.) FTC File No. 072 3067.
[16] Disposal Rule, 16 C.F.R. Part 682.
[17] FTC Act,15 U.S.C. § 45(a).
[18] *In the Matter* of *Dave & Buster's, Inc.,* FTC File No. 082 3153.

Sears Holdings[19]

The FTC brought an enforcement action for deceptive trade practices against Sears Holdings Management Corporation. This was in regards to an agreement for installed software that did not present all required information and so was considered deceptive by the FTC. The software program kept track of almost all Internet activities and other non-Internet on consumers' computers, including those to non-Sears websites and then transmitted this information to Sears' servers. In later 2009, as a settlement, Sears Holdings agreed to not collect such information and destroy any collected to date. It also agreed to notify all the affected consumers and tell them what has occurred and how to uninstall the program. In the future, it must clearly describe all types of data collected and must now obtain express consent to the collection of this data, including a consent option box that is not pre-selected.

LifeLock[20]

In March 2010, the FTC announced it had reached a settlement with LifeLock, Inc. According to the complaint, the company marketed identify-theft services to consumers that were to prevent identity theft through placing fraud alerts on consumers' behalf. To providing this service, personal information of the consumer was collected and then stored on the company's servers. The complaint alleged that the service did not actually protect against most typical identity theft transactions that do not use credit reports and the initial fraud alert does not monitor a consumer's account. Contrary to their many advertisements, the complaint alleges a lack of reasonable and appropriate security measures, including transmitting data in the clear, lack of adequate password management, not applying security patches, lack of network penetration planning and no anti-virus programs. The settlement included several compliance measures and paying $12 million ($1 million to 35 states).

CyberSpy[21]

In June 2010, the FTC announced a settlement with CyberSpy Software, LLC. This bars the company selling the "RemoteSpy" key-logger from advertising that the spyware can be disguised and installed on someone else's computer without the owner's knowledge. It requires that the software obtain consent from these other computer owners before the software can be installed. The complaint alleges that when an email attachment is clicked on, this program installs on the recipients computer without their knowledge. Then keystrokes, passwords, screen images and website visits are recorded and sent to the defendant's website. The order requires that the defendants no longer instruct buyers how to disguise the spyware as an email attachment or do anything that would violate the law.

Standards and Guidelines

In 2010, in addition to the conclusion of the two-year review cycle for the PCI DSS standard later

---

[19] *In the Matter of Sears Holdings Management Corporation*, FTC File No. 082 3099.
[20] *Federal Trade Commission v. LifeLock, Inc* (D. Ariz.), FTC File No. 072 3069.
[21] *Federal Trade Commission v. CyberSpy Software, LLC,* et al. (M.D. Fla.) Civil Action No. 08-CV-01872, FTC File No. 082 3160.

in the year and potential new guidance documents including end-to-end encryption, NIST released documents on government system security configuration management[22] and security control assessment,[23] a glossary of InfoSec terms[24] and the following two documents.

Guide to Protecting the Confidentiality of Personally Identifiable Information (PII).[25]
In this publication, NIST is focused on protecting PII from losses of confidentiality. The impact levels of other two security objectives of integrity and availability are covered through the NIST's Risk Management Framework.[26] The protection deployed for confidentiality is based on its impact level (low, moderate or high), which in turn relates to having a limited, serious or severe/catastrophic adverse effect on operations, assets or individuals. There a number of factors to consider when determining the impact levels, such as: identifiability, quantity, sensitivity, context, protection obligations, access and location. A number of operational, privacy and security controls are suggested.

Smart Grid Cyber Security Strategy and Requirements[27]
In February, NIST put out the second draft of its Smart Grid Cyber Security Strategy and Requirements report. The report covers cyber security requirements and privacy concerns, among other topics, for the electrical power infrastructure in the U.S. Cyber security in the Smart Grid is more inclusive than in a typical IT-centric view, including both "power and cyber system technologies and processes in IT and power system operations and governance." To ensure confidentiality, integrity, and availability of the Smart Grid cyber infrastructure, other hardware must be included, such as "control systems, sensors, and actuators." In power systems, availability is considered the most important security objective and confidentiality the least important. Privacy issues can be raised by using smart meter data being combined with traditional information collected by utility companies, such as name, addresses, SSN, birth date and credit card information. Even anonymized data combined with certain patterns of use and public information could lead to re-identification. The privacy concerns listed include: fraud, determining personal behavior, remote surveillance and commercial non-grid use of the collected data.

Thomas J. Shaw, Esq. is an attorney at law, CPA, CIPP, CRISC, CISM, ERM[P], CFF, CISA and CGEIT based in Tokyo, Japan who works with corporations in Asia and the U.S. on information law (data privacy, info security, e-Discovery/litigation readiness), Internet law (e-commerce, cloud computing, intellectual property), transactional law, compliance, information governance and litigation and technology risk assessment and reduction. He is the editor of the EDDE Journal from the ABA's e-Discovery and Digital Evidence Committee. He can be reached via email at thomas@tshawlaw.com and on the web at www.tshawlaw.com.

---

[22] NIST SP 800-128, *Guide for Security Configuration Management of Information Systems* (2010).
[23] NIST SP 800-53A Revision 1, G*uide for Assessing the Security Controls in Federal Information Systems and Organizations* (2010).
[24] NIST IR 7298 (Draft) Revision 1, *Draft Glossary of Key Information Security Terms* (2010).
[25] NIST SP 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)* (2010).
[26] NIST SP 800-37, Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems* (2009).
[27] NIST IR 7628 (Draft), *Smart Grid Cyber Security Strategy and Requirements* (2010).

Committee Co-Chairs' Message

Dear ISC Members:

Happy summer to all, we hope everybody is taking some time away from work to enjoy the weather, the beach, and the barbecues. Summer is a time when things traditionally slow down, but it seems that the ISC is busier than ever. We just wanted to briefly provide an update on various ISC activities that are happening over the next couple months, just to make sure everybody is plugged in.

On the near horizon, the ISC is putting on a program in conjunction with the ABA's Annual Meeting in San Francisco. The ISC's program is happening on August 5th and 6th (the Annual Meeting goes from August 5-10). Per usual, ISC members and leadership have put together an interesting set of talks. The full agenda can be found here: http://new.abanet.org/sections/scitech/ST230002/PublicDocuments/ISC%20Meeting.pdf. We hope to see you there, and stress that these face-to-face meetings are what ultimately creates a cohesive community and makes the ISC successful and useful. Please R.S.V.P. ASAP to Kathryn Coburn at: kathryn@coburnitlaw.com.

As many of you know, the ISC is in the middle of updating its Information Security handbook. The original handbook was completed several years ago, and this second edition will update old content and cover plenty of new topics. A big thank you to Thomas Shaw for getting this effort organized and on track. If you have not volunteered already but want to, please contact Thomas at thomas@tshawlaw.com. For those that have volunteered, thank you very much. We appreciate your effort and commitment on this volunteer effort.

As we all know, sweet summertime tends to disappear quickly leading into a busy autumn. The same holds true for the ISC. The ISC will be organizing and putting on the first annual ISC Cyber Policy Institute this fall in Washington D.C. (date to be determined, but probably in early/mid October). The Cyber Policy Institute will be focused around information security and privacy policy and legislative issues (and we hope to actually make contact with some of the legislators who are proposing bills in this space). All of this is being done in conjunction with the efforts of the ISC's Legislative and Policy Working Group. Those interested should plan to join the Working Group's next conference call (which is currently set to take place on June 25, 2010 @ 1:30 p.m. Eastern; please check the list-serve for details). We encourage those interested to join the Working Group's efforts as the ISC is likely to be more focused on policy and legislative issues in the coming months and years.

That is it for now, again please have a nice summer and we look forward to seeing you in San Francisco and D.C. later this year.

David Navetta
ISC Co-Chair