DuaneMorris®

ERIC SINROD

THE YEAR IN TECH LAW 2012

SAMPLING OF WEEKLY BLOGS ON FAST-BREAKING INTERNET LEGAL DEVELOPMENTS FOR FINDLAW.COM

JANUARY - DECEMBER 2012

P: 415.957.3019
ejsinrod@duanemorris.com

To receive a weekly email with a link to Mr. Sinrod's most recent blog, please send an email with "Subscribe"in the subject line to ejsinrod@duanemorris.com.

About the Author

Eric Sinrod is a partner in the San Francisco office of Duane Morris LLP (http://www.duanemorris.com) where he focuses on litigation matters of various types, including information technology and intellectual property disputes. His full Web bio is available at http://bit.ly/Sinrod and he can be reached at ejsinrod@duanemorris.com. To receive a weekly email link to Mr. Sinrod's columns, please send an email to him with Subscribe in the Subject line.

These columns are prepared and published for informational purposes only and should not be construed as legal advice. The views expressed in these columns are those of the author and do not necessarily reflect the views of the author's law firm, its individual partners or its clients.

Table of Contents

Tumblr Briefly Comes Tumbling Down During Cyberattack

December 11, 2012

Tumblr is a Website where users can share photos, music, videos, quotes and posts, all of which can be customized with different colors and themes.

On its "About" page, Tumblr boldly suggests that users "follow the world's creators." With only 128 employees, Tumblr boasts 83.7 million blogs, 37.4 billion posts and a whopping 18.1 billion monthly page views.

So, all is well and good in Tumblr land, right? Perhaps most of the time. However, last week a worm struck Tumblr and infected some of the most widely read blogs, including those of CNET, Reuters and USA Today, as reported by CNET.

A reported hacker group called GNAA took credit for the attack, and stated on its Twitter profile that 8,600 Tumblr users were impacted; however, Tumblr responded in a blog post that no accounts were actually compromised, according to CNET.

When the attack occurred, Tumblr promptly told its users to log out of browsers using Tumblr and stated that it was diligently seeking to fix things, as reported by CNET.

Tumblr was able to resolve the issue later the same day of the attack; but, according to CNET, before then, when users went to a compromised Tumblr site, they would view a nasty post with swear words that criticized the site and its users in very harsh terms.

Security provider Sophos noted in a blog post, as reported by CNET, that the worm capitalized on Tumblr's reblogging function, such that a user who was logged onto Tumblr would automatically reblog the infected post if she visited a compromised page. This caused malicious code to spread like a Web virus; mostly likely, Tumblr's filters were circumvented by the hijacking of a legitimate Tumblr maintenance message.

Tumblr obviously cured this particular problem relatively quickly. But this scenario shows why cybersecurity is a real worry for social media and other sites. Any and all technological steps that can reasonably prevent security breaches before they happen should be seriously considered and implemented when feasible.

San Francisco's Prop E Passes, Will Pay Off for Startups

November 13, 2012

Tax reform can and does happen at the ballot box. Indeed, startup companies in San Francisco should soon feel the benefit of the recent passage of the city's Proposition E.

Proposition E implements a tax on gross receipts, phasing out San Francisco's prior payroll tax. This will be very beneficial for startup companies that have paid staff but have yet to earn much revenue.

Furthermore, given that business tax trails only property tax for bringing in dollars to the city of San Francisco, by taxing gross receipts instead of payroll, there will likely be more regularity and less fluctuation in terms of dollars flowing into city coffers.

Proposition E passed with more than 70 percent of the vote, according to Business Insider -- an overwhelming victory. The proposition was backed by Ron Conway, a venture capitalist, and had broad-based, political, cross-party support.

San Francisco in recent times has become home to a new startup culture. However, when start-ups are taxed based on payroll and not gross receipts, there is a real possibility that the startups might go elsewhere. Now that the tax will focus instead on gross receipts, startups hopefully will remain in San Francisco and will pay their fair share as their revenues grow.

In the humble opinion of your faithful blogger, San Francisco voters did the right thing by passing Proposition E!

Defense Secretary Panetta: Cyberspace Is the New Battlefield

November 6, 2012

We usually think of the Internet as a place where we can obtain information, communicate with others, and engage in various business and personal activities.

However, is it also a new battlefield?

Yes, according to Defense Secretary Leon Panetta. Indeed, as reported by Reuters, he maintains that while hackers have already attacked financial institutions, they also have the capability to strike mission-critical domestic power grids and government systems.

Panetta made this comment to a business group in Virginia. One week before, he gave a policy speech to a New York business group, in which he indicated that the U.S. military has the capacity to take pre-emptive measures in the event of an imminent risk of online attacks.

Secretary Panetta stated that domestic financial institutions have been experiencing sustained attacks recently. And he noted, without indicating the countries of origin, that Washington faces thousands of attacks every day.

He indicated that the United States has made real investments in cyber forensics to address the issue of identifying the sources of cyber-attacks.

Panetta further described that Congress needs to feel more pressure to act to avoid a round of automatic budget cuts due to go into effect in January. The cuts apparently would reduce $500 billion from defense spending during the next decade, in the aftermath of almost an equal cut in projected defense spending approved a year ago.

Plainly, if the Secretary of Defense is concerned based on sensitive information available to him, the threat of cyber warfare truly needs to be explored and countered before significant harm could be caused by online attacks.

Hackers Increasingly Target Colleges, Universities

October 18, 2012

All sorts of businesses and organizations are potentially vulnerable to hackers. Educational institutions are no exception, as highlighted by a recent example involving Northwest Florida State College.

One or more hackers accessed a folder on the school's main server from May through September, according to a memo from the College's President to all employees. The folder contained multiple files.

By working between the files, the hacker(s) apparently managed to assemble sufficient information to steal the identities of 50 employees, CNET reports. Names, social security numbers, dates of birth and direct deposit account numbers were accessed. Apparently, data relating to addresses, phone numbers, and college email addresses also was compromised.

But there is more.

The President's memo indicates that current and past employees going back to 2002 who have utilized direct pay deposits potentially have been the subject of data compromise. The number of impacted employees could be as high as 2,200.

The College President opines that all of this was the result of "a professional, coordinated attack by one or more hackers." He also is concerned that student information such as birth dates and social security numbers may have been accessed, but he is not presently aware that such information has been taken.

In terms of technological solutions, the President points out that "the access pathway used to invade our main server has been sealed."

Plainly, educational institutions are not immune from hacker attacks and the potential for data security breaches. Accordingly, they would be smart now to implement needed technological measures on the front-end to prevent or mitigate possible attacks.

So, for example, if a school has some sort of access pathway to a server that could serve as an avenue for a hacker attack, that pathway needs to be addressed in order to prevent such an attack.

Switching to E-Books Would Save Our Children's Backs

October 3, 2012

It is amazing that in this day and age we still see students hauling around backpacks full of heavy school textbooks. This is true not only for college and high schools students, but also for much younger students in middle school and elementary school.

With the technology available such that many voluminous books can be loaded electronically onto an electronic book reader, a laptop, an iPad, or even a PDA, there seems no reason why kids should have to shoulder the heavy weight of books.

The electronic book readers allow for searching, highlighting, taking notes, and other features.

It is true that some people like to physically hold and read a hard copy book, and for them, actual physical books can be available. This also should be the case for students who do not have the technology available to them for e-reading. And some books are not yet in electronic form, and hard copies are the only option.

But still, schools should move in the direction of the option of electronic reading for students. Some schools already are there, but others can make further progress in this regard.

Not only do electronic books lighten the physical load for students, it also is possible the some students will read more with the ease of electronic reading - many books will come alive right at their fingertips.

The Cost of Cybercrime: 1.5 Million Victims Every Day

September 19, 2012

Make no mistake, Cybercrime is real and its impact is huge. Indeed, a recent Norton Cybercrime report by Symantec provides some fairly startling statistics.

For example, there are 1.5 million Cybercrime victims on a daily basis - that is 18 victims per second. There are 556 million such victims per year - in excess of the European Union total population.

Two-thirds of online adults already have been Cybercrime victims at some point in their lives, and 46% of online adults have been victims within the past year.

The annual cost of Cybercrime is a whopping $110 billion.

The average cost per victim is $197. Of the surveyed countries, the cost of Cybercrime is the highest in China at $46 billion, with the United States coming in second at $21 billion, and with Europe third at $16 billion.

The highest number of Cybercrime victims are found in Russia at 92%, then China at 84%, and then South Africa at 80%.

One of the greatest Cybercrime risks, according to the report, is the fact that 44% of adults access personal emails through free or unsecured Wi-Fi connections. Social networks also can present Cybercrime risks. One danger there is accepting friend requests from unknown people - as you are only as secure as your circle of network friends.

To be safe, people should change their passwords frequently, use complex passwords, delete emails from people they do not know, employ a basic antivirus solution, and they should not open attachments or links from unsolicited emails or texts.

Don't think you are immune from Cybercrime. Be smart and careful out there.

Spam Email Costs Billions But Yields Far Less

September 11, 2012

Most of us hate unsolicited commercial email - aka spam. Notwithstanding spam filters and federal and state laws prohibiting spam under various circumstances, we nonetheless continue to receive these annoying emails in our in boxes.

One might think that the spammers are making fortunes as part of their predatory practices.

But a recent study indicates that while the societal cost of spam is phenomenally high, to the tune of $20 billion, the revenue derived from spam is a fraction of that, only $200 million.

The study, titled The Economics of Spam and published by Justin Rao of Microsoft and David Reiley of Google in the Journal of Economic Perspectives, notes that American firms and consumers yearly suffer costs of about $20 billion as a result of spam. The study points out that this estimate is less than the $50 billion price tag suggested by others, but it adds that the number would be much higher without anti-spam technology that does reduce the impact of spam.

The study also finds, based on the infiltration and monitoring of spammers' conduct, that spammers globally collect revenues of $200 million. This means that ratio of external costs to internal benefits is 100:1. Thus, the harm caused to others far outweighs the benefits to the spammers.

Does this mean that spammer will stop? Of course not.

Spammers care about the benefit to them, not the harm caused to others. If this were not the case, spamming already would have ceased to a large extent.

So, hopefully spam filters will trap most spam while not blocking legitimate email. And, let's cross our fingers that federal and state anti-spam laws will help hold spammers in check. But while filters and the laws have had some success, plainly spam still reaches our in boxes. It may be a part of life for the foreseeable future.

The London Olympics: A High-Tech Success

August 22, 2012

The London 2012 Olympics games were successful, and indeed spectacular, on many levels.

Of course, there were incredible performances by phenomenal athletes, including veterans like Michael Phelps and Usain Bolt, as well as new breakout stars such as Missy Franklin and Gabby Douglas.

Great Britain also served up wonderful musical acts for entertainment purposes. Not only were we regaled by Paul McCartney, Annie Lennox, George Michael, and bits and pieces from Queen and Pink Floyd, but we also witnessed the reunion of the Spice Girls (oh my).

It was also a technologically advanced event.

Happily, there weren't any majority security incidents. And, there were nary any problems with detection of performance enhancing substances.

Not to be lost in the shuffle is the fact that this was the first truly high-tech Olympics.

Athletes real-time were tweeting with their followers, creating true interaction and really bringing the games to life at a personal level.

Also, fans had myriad ways to witness the games. As in the past, the games could be watched on television (often time-delayed); however, more viewing channels were available this time around.

Moreover, fans could gain moment-by-moment results from their smart phones.

And, video clips of highlights and specific events could be accessed from computers.

The next Olympics summer games will be in Rio. Get ready for tech carnival four years hence!

Russian Internet Bills Revive Soviet-Era Censorship Concerns

July 24, 2012

People tend to think that anything goes on the Internet. But is that true everywhere? Perhaps not. Indeed, according to a recent New York Times article, a series of controversial Russian Internet bills, approved last week by Parliament, seeks to strengthen the government's Internet controls.

The Russian Parliament's approval of the bills reportedly follows the Russian government's imposition of fines relating to unsanctioned protests and the reinstitution of criminal charges for slander.

The Russian Internet bills, approved by both the upper and lower houses of Parliament, would give the Russian government the ability to block websites that it deems inappropriate for children.

The bills would also force nonprofits to list themselves as foreign agents, to the extent any of their financing comes from beyond Russia's borders and they are deemed to be involved in political efforts.

The tightening of Internet controls, the criminalization of slander, and the foreign-agent categorization are causing public complaints in some quarters, and have many worried that Russia is reverting to Soviet-era practices.

Freedom of speech and assembly are hallmarks of democracy. The Internet provides an easy means to communicate broadly. While some nations may support such freedoms and means of communication, that is not universally true. As the Russian Internet bills seem to show, the converse can be the case in certain instances, if freedom of communication is considered threatening to a particular regime.

Twitter Transparency Reveals Government's Social Media Demands

July 18, 2012

Is the information you post via social media of potential governmental interest? Probably not, but still, it's possible.

To bring home the point, Twitter just issued its first Transparency Report. That report details the number of government demands it has received for user information in the first six months of 2012.

What do the numbers reveal?

Most of the demands for information come from the U.S. government, according to eWeek.com. Recent demands related to 948 users; Twitter has complied to some extent (or entirely) with 75% of those U.S. government requests.

Japan's government comes in second, with 98 requests to Twitter relating to 147 users. The company has only responded to 20% of those requests, Twitter's Transparency Report states.

So why is it that the government seeks social media information? The most common reason is to seek information pertaining to ongoing criminal investigations. Also, once in a while, Twitter will receive a request from a foreign government to remove content from its site; however, Twitter does not tend to comply with those requests.

Twitter does receive a fair number of copyright takedown notices. Indeed, between January and June of this year, more than 3,000 such requests were received relating to almost 6,000 accounts. Twitter reports that 38% of copyrighted material has been removed pursuant to such notices.

While the numbers in Twitter's Transparency Report may seem high, in reality they are a drop in the ocean of Twitter users and communications. Still, there is the potential that your social media communications could be of governmental interest or subject to copyright takedown notices. But, if you are far afield from criminal activity and if you are not violating any copyrights, you likely will not be bothered. So do the right thing out there and tweet responsibly.

Blog Food Fight Leaves Egg On School's Face

June 20, 2012

The Internet yields all sorts of disputes. Take the nine-year-old Scottish girl who was banned from posting photographs of school meals on her blog, which caused a firestorm of criticism.

Martha Payne, who by now has had in excess of three million hits on her blog at NeverSeconds.blogspot.com, started posting photos of her Scottish primary school lunches at the end of April. BBC News report that her "food-o-meter" rated each meal in terms of healthiness and how many mouthfuls it takes to consume the meal.

Ultimately, school officials became concerned and a school council banned Martha from posting further photos of school meals.

So, this food fight, while at times messy, has a happy ending.

But school officials likely did not anticipate the fallout from an angry social media reaction to the ban. Indeed, according to BBC News, a Scottish education secretary tweeted that he would be contacting the school council to overturn the "daft" ban. And a celebrity chef tweeted "stay strong Martha" and encouraged his more than 2 million followers to retweet his message.

In the wake of this reaction, the school council initially defended its ban and asserted that all of the attention on the blog had caused food staff at the school to be concerned about their jobs. The council also stated that the ban made sense because the photos on the blog represented only a fraction of food choices available to students.

However, and likely because of public pressure, the ban ultimately was lifted. Martha Payne likely is pleased about how this turned out. Her original goal was that her blog would help raise funds for Mary's Meals charity. Her target was 7,000 pounds. Prior to the ban controversy, her blog had raised roughly 2,000 pounds. But after all of the attention caused by the ban, she has raised in excess of 30,000 pounds.

Indeed, Martha has stated that she has raised enough funds to build a kitchen in Malawi for children who receive Mary's Meals.

Trouble In Password Paradise

June 12, 2012

Many people use the same password for all of their accounts. Why? Because it is easy to remember just one password across all accounts.

But is that a good idea? Nope. If that password were to fall into the wrong hands, it potentially could be used more pervasively to the disadvantage of the true password holder.

And this is not a hypothetical concern. Indeed, recent press reports are rife with disclosures of major password hacks/leaks.

As many of you know, LinkedIn has confirmed that many user passwords have been compromised. Some reports indicate that the number of passwords at issue could be as high as 6.5 million.

On top of that, there have been recent reports that as many as 1.5 million passwords of eHarmony users have been compromised.

And if that were not enough for one week, Last.fm, an Internet radio site, reportedly is investigating leaks of its user passwords.

Certain members of Congress do not view password threats lightly. Senator Patrick Leahy of Vermont and Representative Mary Bono Mack of California have referred to the recent password hacks as a further reason why data security legislation should be passed.

Meanwhile, users of the above-referenced sites would be smart to change their passwords for those sites. And people generally should use different passwords for their various accounts and they should change them periodically.

This may be a hassle, but an ounce of prevention in this context could be worth more far than a pound of later, potential cure.

Where Should You Store Your Digital Music?

May 22, 2012

Once upon a time, collecting music was a clunky experience, to say the least. Vinyl albums (while you might like the sound they provide) are large and take up a lot of space. And though tapes and CDs are smaller, they can add up in terms of storage needs, and none of the above are easy to navigate in terms of finding genres, artists, or songs. Moreover, of course, they cannot really be "shuffled" in a meaningful way.

Nowadays, music can be stored with hardly any storage concerns and can be searched and retrieved almost by magic. I must confess, I am a music junkie. When I open iTunes, I have tens of thousands of my songs at my fingertips. I store my songs on a 750-gigabyte external hard drive, and I can transfer and load up to 15,000 songs on my 160-gigabyte iPod. Not bad, eh?

Well, maybe. I recently visited a local Apple Store. The "Genius" there told me to be careful about relying on one hard drive to store so many songs, which in the aggregate constitutes quite a valuable music collection. As he said, all hard drives die at some point. The issue is not "if," but "when."

Great. So in one fell swoop I could lose my entire music collection. Indeed, I already have given away all of my CDs after having ripped the songs into my iTunes, and therefore the CDs no longer are available to me as security. Of course, I could have a back-up hard drive. In fact, the "Genius" said that I would be smart to have two back-up drives loaded with my songs, for a total of three drives housing my music. Thus, as they die, at least one will be still be alive, and I can keep buying and loading drives over time.

Sure, this is one way to go. Of course another way, which is not mutually exclusive from the multiple drives suggestion, is to store my music in the cloud. Presumably, music stored in the cloud would not die along with a dead drive, but instead would be maintained.

All of this begs the question as to whether I really need to even "have my own" music any longer. Perhaps buying and keeping albums and songs has become yesterday in today's world. Why do I need to own music when I have a Pandora account? I have created 100 Pandora "radio stations" and I shuffle them all together. This presents a near never-ending variety of music coming my way without me having to own or store anything. I can change up my Pandora stations whenever I like, and there are other similar music-streaming options, like Spotify.

Yes, I will do my best to preserve "my" music collection at this point. However, I may not add to it much, and I won't have a coronary if it does go missing despite my best efforts. Why? Because Pandora and other music options will follow me into the future.

Rock on.

E-Discovery is More Costly, Burdensome Than You Think

May 1, 2012

Once upon a time, it was widely believed that electronic discovery would streamline litigation, making it faster, easier, less burdensome, and less expensive. So, now that we are some years into the e-discovery experience, has the prediction come true? Sadly, not necessarily.

While it is true that it can be easier to retrieve information electronically by using search terms, rather than sending teams of associates into warehouses to rummage through boxes of documents, that is just the tip of the iceberg when considering the overall e-discovery effort. And even if vast quantities of electronic information can be brought up based on a simple search, that information had to be harvested at the front-end, and ultimately will need to be reviewed at the back-end.

The vast array of information that now is subject to discovery in the electronic age has grown exponentially. When I started out as a lawyer almost 30 years ago, the types of materials that were subject to discovery included formal memoranda, correspondence, and handwritten notes.

Now, not only are those materials still of interest, but parties also seek emails, text messages, Internet and social media posts, voicemail messages, Word documents, Excel spreadsheets, information stored on networks, backup tapes, laptops, PDAs, cell phones, and the list goes on and on.

Plainly, the scope of what must be considered within the universe of potentially discoverable information has grown significantly. And the task of rounding up such information can be Herculean. Not surprisingly, parties now not only need to pay their attorneys to spearhead e-discovery efforts, but they often need to engage specialized vendors. Moreover, companies that are subject to repeat litigation are hiring their own internal e-discovery coordinators.

On top of this, when litigation has occurred or is reasonably likely to be initiated, parties need to institute litigation holds so that discoverable information does not go missing. This too can be cumbersome for companies, given the many different ways that information is now stored electronically.

And if one side to a case believes that the other side has not properly preserved relevant electronic information, arguments of spoliation of evidence come to the surface. Indeed, spoliation fights have tended to dominate certain cases, almost pushing the merits of the litigation to the background.

It is not altogether uncommon for there to be a number of e-discovery disputes in litigation. Parties and their attorneys can fight about search terms, custodians, sources of information, methods of retrieval and production of electronic data, etc.

Also, it is important to start the e-discovery process essentially at the outset of litigation. And there are times that the price of e-discovery can actually outweigh the amount at stake in the litigation on the merits. That can "chill" the bringing of certain cases, and can heavily influence the settling of cases before e-discovery costs have escalated.

The world has gone electronic, so e-discovery obviously is here to stay. However, gone for now is the notion that e-discovery is cheap and easy.

When Should an Attorney Dump His BlackBerry for an iPhone?

April 24, 2012

I have a confession to make: I am addicted to my BlackBerry. Indeed, the term "CrackBerry" certainly applies in my case. Ever since my wireless signal was established years ago, I have been mainlining my BlackBerry on a relatively constant basis.

There was a time that BlackBerry really was the only real PDA game in town at my firm. However, more recently, we have opened up the iPhone option, and as time passes, more and more of my colleagues have been weaning themselves off the BlackBerry and migrating to the iPhone. What's more, some of my colleagues have been encouraging me (rather strenuously) to change my PDA drug of choice, turn my back on my beloved BlackBerry, and go the iPhone route myself.

So, what am I to do? At home, we are an Apple family, with MacBooks, iPads and iPods to be found all over the place. Plus, my wife and two daughters are die-hard iPhone fans and users. Thus, one would think that a switch should not be too difficult for me.

However, I am a creature of habit. And, I really like some of my BlackBerry's features and functions. For one, the BlackBerry raised keyboard really works well for me -- indeed, my thumbs just fly and I can type on my 'Berry almost as fast as on a laptop or desktop. Also, the battery life on the BlackBerry is superb. Moreover, I have saved tons of photos, songs and video clips on a rather beefy memory chip inside of my device.

But, and there always is a "but," the BlackBerry is not Nirvana either. The reception from T-Mobile where I live can be spotty. In addition, when I enter my car, the device does not automatically synchronize with the car's Bluetooth function, and at times not at all. Furthermore, there are occasions when the BlackBerry tells me that I have unreviewed messages, when that is not true. And last, but certainly not least, the viewing screen for looking at images and Internet pages is not terribly generous.

I am told that I likely would have better reception on an iPhone in my area. I also am informed that the iPhone should sync automatically with my car's Bluetooth. And I am apprised that there may be more and better functioning apps on the iPhone. Most importantly, the iPhone is an Apple product, and we know what that means: excellence in overall user ease and experience.

Habits do die hard. But I suppose if I can convince myself that I can get used to the iPhone's touchscreen keyboard, and will be able to transfer all of my media (perhaps through the cloud and back), then maybe I will make the jump. I can't tell you exactly when this might happen, but it just might be soon.

P.S. This was typed on an Apple MacBook Pro!

Online Dating Sites Vow to Protect Users from Sex Predators

March 28, 2012

According to press reports, online dating websites eHarmony, Match.com and Sparks Networks have entered into a joint statement of business principles to protect users from sexual predators and to help prevent identity theft and other scams. California Attorney General Kamala Harris followed up on this development by stating that "consumers should be able to use websites without fear of being scammed or targeted," in apparent recognition that a woman was assaulted on a date that came about through an online dating site.

The companies reportedly have agreed to use national sex-offender registries to check on subscribers, to quickly respond to reported abuses, and to give Internet safety guidance to members. The dating sites will also provide reports of suspected criminal activity to the Attorney General's office.

Apparently the statement of principles is not binding, and does not include enforcement penalties. However, members of these online dating websites likely will expect these companies to live up to their expressed safety protections.

These dating sites have a wide reach, and to the extent they can further protect the safety of their members, the better. Match.com already is in business in more than 20 countries. eHarmony operates in North America, the United Kingdom and Australia. Sparks Networks has various sites that cater to focused ethnicities and religions.

Press reports indicate that about 40 million Americans participated on online dating sites in 2011, and spent more than $1 billion for their online dating memberships. Obviously, online dating sites are popular and big business. This further underscores renewed efforts for member safety.

The woman who was assaulted was on her second date in 2010 with a man whom she had met via an online dating site. The man reportedly drove her home, followed her inside, and assaulted her. The man originally argued that the experience was consensual, but later pleaded no contest to sexual battery by restraint and received a one-year prison sentence. He apparently had a series of prior sexual battery convictions.

Perhaps some might suggest that this one publicized assault out of the millions of dates that occur via online dating sites is making a mountain out of a molehill. However, even one such assault is far too many if steps can be taken to ensure that this can be prevented. And for anyone who is assaulted, the trauma can last for a lifetime.

The joint statement of principles by the online dating sites is a positive development. Let's hope that this and other efforts can keep the online dating world a safe place for people seeking love, not violence.

Cybersquatting, Domain Name Disputes Set All-Time Record

March 13, 2012

One might think that as the Internet matures, domain name disputes might dissipate. Not so!

Indeed, an all-time record 2,764 cybersquatting cases pertaining to 4,781 domain names were filed with the WIPO Arbitration and Mediation Center (WIPO) in 2011.

These filings were made in accordance with procedures based on the Uniform Domain Name Dispute Resolution Policy (UDRP) and represent an increase of 2.5% and 9.4%, respectively, above previous record levels in 2010 and 2009.

Amazingly, since the launch of the UDRP in late 1999, WIPO has been the recipient of more than 22,500 UDRP-related cases. These cases have addressed more than 40,500 domain names.

Furthermore, as the Internet has broadened geographically, so has the country-origin of domain name disputes. In 2011, disputes filed with WIPO involved complainants and respondents from an astounding 110 countries. And these cases were handled by 323 WIPO panelists from 49 different countries in 13 languages.

For 2011, the highest sector areas of WIPO complaints related to retail, Internet and IT, biotechnology and pharmaceuticals, fashion, and banking and finance.

Interestingly, the WIPO panels found cybersquatting in 88% of the disputes. Obviously, complainants fare well with the domain name disputes filed with WIPO.

With the recent advent of the .xxx domain for pornography sites, disputes in this space already have arisen. There was quite a bit of debate within the Internet Corporation for Assigned Names and Numbers (ICANN) as to how to manage Internet pornography. Finally, the .xxx domain came into operation in December. And now that it is here, .xxx already is adding to the panoply of domain name disputes.

Plainly, the rising tide of domain name disputes continues with no sign of ebbing any time soon.

Is Your Company at Risk for a Data Security Breach?

February 14, 2012

Businesses want to know whether they are potential targets for security breaches, and if so, they seek to identify the types of electric records that may be at risk.

The Trustwave 2012 Global Security Report sheds some light on these concerns by identifying top data-security risk areas. Highlights of the report include the following findings:

- Interestingly, the food and beverage industry, for the second straight year, comprised the highest percentage of security investigations at almost 44%.
- Industries with franchise models have become the most recent cyber targets, as more than one-third of 2011 investigations related to a franchise business.
- In-transit data within victim environments are frequently targeted by data-harvesting techniques, as revealed in 62.5% of 2011 investigations.

As a heads up, the most common password implemented by global businesses is "Password1," due to its satisfaction of the default Microsoft Active Directory complexity setting.

The targeting of customer records emerged front and center in 2011, according to the Trustwave report: 89% of attacks were focused on obtaining personally identifiable information, credit-card data, and other customer data.

Plainly, businesses in the food and beverage industry, and those with franchise models, need to be aware of and take preventive measures to help thwart security breaches. But this admonition frankly applies to all businesses that operate online -- meaning, practically all businesses.

In addition, protections should be put in place with respect to in-transit and other data, true password protection procedures need to be instituted, and customer records and related personally identifiable information must be safeguarded.

There is no such thing as perfect cyber security, but businesses can and should do better.

FBI's Social Media Monitoring Plan Must Balance Privacy, Security

February 1, 2012

A few weeks ago this blog pointed out that the Department of Homeland Security's command center regularly monitors social networking sites such as Facebook and Twitter, popular sites like Hulu, controversial sites including WikiLeaks, and news and commentary sites like The Huffington Post and Drudge Report, according to a government document.

Now, there is an indication that the Federal Bureau of Investigation is developing a web application that will have the ability to monitor social media sites like Facebook and Twitter. Such an application supposedly will give the FBI intelligence about potential security threats.

The FBI's apparent social media monitoring plan has been reported on by Christina Warren at Mashable.com. She explains that the FBI's plan was inadvertently revealed by its Strategic Information and Operations Center within a social media application market research request. This revelation was uncovered by New Scientist magazine.

Privacy advocates generally are against government monitoring of social media sites.

However, it appears that the FBI's social media monitoring plan in this context is to only gain access to publicly available information.

Accordingly, the government view likely is that any information posted online for public viewing is legitimate information for it to search. Any privacy interests would be de minimis, while the policy in favor of preventing security threats and crises is strong.

The response from privacy advocates very well might be that while people may provide information on social media sites in a public fashion, they do not do so thinking that what they say and post might be monitored by the government. With such government monitoring, there could be a chilling effect on Internet speech and conduct.

Of course, the government might respond to this argument by asserting that if you are not doing anything wrong, and if you are not contributing to a security threat, you have nothing to worry about in terms of what you post on social media sites.

But privacy advocates could reply to this by arguing that even if someone is innocent of wrongdoing, his or her social media posts could potentially be misconstrued, causing that person to incorrectly fall under the government's suspicion.

This debate is coming, if it is not here already. Stay tuned to see how it evolves. Balancing on the privacy/security threat tightrope is not a simple endeavor.

Long Live Tech in 2012: But Don't Forget the 'Off' Button

January 10, 2012

Happy New Year! We're just a week into January, but 2012 seems to be firing on all tech cylinders.

The other night, I went to a shopping mall with my family. While most of the traditional retail stores were not terribly busy, the Apple store was an amazing hive of activity.

In the one room that makes up the store, I literally counted as many as 40 Apple employees who were swamped fielding questions from and helping a never-ending parade of customers. It seemed that everyone and their kid brother and sister was hunting for the latest iPad, iPod, and Apple computer.

At the same time, who doesn't spend countless hours on Facebook with our "friends"? We post our thoughts and share photos, music, and more. And, of course, it's become increasingly important to wish everyone happy holidays and to usher in the new year via social media. Many of us received holiday and New Year's wishes and photos from all over the world.

We can't forget about YouTube, where we can view and post videos of every type. We are living our lives out loud, and YouTube is proof.

There are many other ways to be entertained online these days as well. For example, you can go to Pandora and create your own customized "radio stations." If you like The Beatles, you can create a Beatles station that not only will play songs by the boys from Liverpool, but will also bring up songs by other groups that are musically similar.

No longer is the Internet confined to a desktop computer, or even a handheld device. Even automobiles now are "smart." New cars have built-in navigation systems, Bluetooth connections, and can access Pandora and music from your iPod. All you have to do is talk to your car, and it will respond.

All of this technology is fascinating, fun and exciting. But it also makes it much easier to suffer from nonstop information overload. Indeed, some research has suggested that such overload has led to greater rates of depression in our populace than previously.

So go enjoy your tech toys -- but remember the reverse of the 1960s adage: Rather than always tuning in and turning on, once in a while tune out and turn off.

With that caveat in mind, it will be interesting to see where tech takes us in 2012.