DuaneMorris®

ERIC SINROD

THE YEAR IN TECH LAW 2013

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

JANUARY – NOVEMBER 2013

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.

Table of Contents

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.

Pres. Obama's Twitter Account Hacked: Is Anyone Completely Safe?

November 5, 2013

Hacking attacks have been part of the Internet landscape, unfortunately, since the dawn of Cyberspace. Nevertheless, you might think that certain sites are sufficiently important and secure that they are immune to the effects of a hack attack.

But that is not necessarily the case. News accounts periodically report on hack attacks wreaking havoc on large commercial websites. And now even President Obama, the leader of the free world, is bearing the brunt of some recent hack attacks.

Indeed, according to AllThingsD.com, several websites affiliated with Organizing for Action, President Obama's advocacy group on nonprofit issues, were hit and compromised by hackers last week. Tweets emanating from the @BarackObama handle linked to YouTube videos hosted by the "Syrian Electronic Army"; such links were also provided via President Obama's Facebook fan page.

AllThingsD reports that the Syrian Electronic Army has been targeting a variety of high-profile people during the past year while attempting to gain support for Syrian President Bashar Al-Assad. AllThingsD reports that the SEA hacked the social-networking accounts of CNN, the Guardian, the Associated Press, and other news outlets. Notably, the AP hack in April triggered a stock market "flash crash" -- the Dow Jones Industrial Average fell 130 points within minutes after the hack.

Even though hacking still occurs on the Internet and at times causes actual harm, this does not mean that we should throw up our hands and just accept this state of affairs. Efforts must be made to continue developing the best security practices and products to try to stay ahead of the evolving ingenuity of hackers as they try to disrupt the Internet.

Effective security efforts to date have helped prevent and minimize harm caused by intended hacking attacks, and the situation would be far worse without such efforts.

Illinois' 'Amazon Tax' Law Ruled Unconstitutional

October 29, 2013

Should consumers be able to avoid paying state sales tax simply because they make purchases on the Internet?

Some legislators think not, believing that state coffers should not be deprived of sales tax revenue from online purchases. Consequently, they have enacted some laws designed to capture such revenue.

However, according to the *Chicago Tribune*, a recent law passed in the Land of Lincoln attempting to tax online purchases was just ruled unconstitutional by the Illinois Supreme Court.

Illinois Act Taxed Online Purchases

Illinois passed the Main Street Fairness Act ("the Act") in early 2011. The Act was referred to as the "Amazon tax law," reports the *Tribune*.

Prior to passage of the Act, online retailers only had to collect sales tax on purchases by Illinois residents and only if the online retailer had a "physical presence" in Illinois. Significantly, the Act gave broad meaning to "physical presence" to include affiliate companies.

Affiliates generally speaking are third-party advertisers for online stores. By including them within the ambit of the "physical presence" notion, the potential sweep of sales tax on online purchases was greatly expanded.

In response, some Internet retailers ceased doing business with affiliates in Illinois. Some Internet sellers moved out of Illinois entirely.

State Supreme Court Invalidates Act

Ultimately, this issue led to litigation, and eventually a Cook County Circuit judge ruled that the Act ran afoul of the Commerce Clause of the U.S. Constitution and that it conflicted with the Internet Tax Freedom Act, a federal law which does bar certain online taxes.

The case then worked its way up the appellate chain, and in late October, the Illinois Supreme Court affirmed the decision of the Cook County Circuit judge, reports the *Tribune*. This was in contrast to the New York high court's decision to uphold a similar state tax challenged by Amazon and Overstock.com.

The impact of the decision is not fully known yet. Perhaps Internet retailers will start doing more business with affiliates in Illinois again, and maybe they will move back into the state themselves.

Or the litigation battle may continue, as review eventually could be sought by the U.S. Supreme Court.

Other states likely are watching to see how this plays out to determine what to do on their own home turf. And it is possible that Congress might weigh in with further Internet legislation in this area.

Facebook Allowing Greater Sharing of Teen Posts

October 22, 2013

Facebook has decided to let teenagers share their posts even more broadly.

According to *The Wall Street Journal*, Facebook users between the ages of 13 and 17 will be able to set their posts as "public," meaning that they can be viewed by anyone on Facebook, not just friends and friends of friends.

This shift in policy appears designed to allow Facebook to compete even better against other social media sites that allow for teen public posts, such as Twitter, but what will it mean for teens?

Facebook Privacy Worries

While public teen posting is already commonplace on other sites, some privacy watchdogs are concerned about this policy being adopted by Facebook. This is due to Facebook's broad reach to approximately 1.2 billion members globally (five times more than Twitter), reports the *WSJ*, and because Facebook allows teenagers to post a much wider array of media online and to comment more expansively than on Twitter.

Facebook has tried to address privacy concerns -- including the new search changes -- by stating that it is implementing a pop-up feature that warns teens that anything they post as public truly is public on the Facebook network. The *WSJ* reports that Facebook also is changing its default setting for teen posts so that they are only seen by friends, not friends of friends; yet, teens will be able to change that default setting.

Facebook Restricts Ads, Respects Freedom

To further stress its efforts to try to protect teens, Facebook reports that it is limiting advertising relating to dieting, alcohol and gambling, reports the *WSJ*. Despite being under investigation by the FTC for its new privacy policies, Facebook also maintains that it is trying to uncover teens who lie about their age to circumvent teenage privacy protections and restrictions.

While Facebook expresses its desire to protect the privacy of online teens, at the same time it does not want to restrict them so much that Facebook ultimately starts losing its teenage base to competitors. By opening up the public posting option to teens, Facebook likely hopes that its teen members will remain on Facebook and not go elsewhere in terms of social media.

Time will tell as to how this plays out.

California Criminalizes 'Revenge Porn'

October 8, 2013

In my most recent blog, I reported on the phenomenon of "revenge porn," the unfortunate practice by former lovers, boyfriends, and husbands of posting nude and sexual photos and videos of women with whom they had been intimate.

Now, according to Reuters, California Gov. Jerry Brown has just signed a unique state law that criminalizes revenge porn.

California's Revenge Porn Law

The new law makes it a misdemeanor for individuals to take and then circulate without consent such images online with the intent to harass or annoy. And a conviction for violation of this law is punishable by up to six months in jail and a $1,000 fine for a first offense. The new law is immediately effective.

The new revenge porn law was preceded by a California law that already made it a crime to take sexually explicit photos of another person without his or her consent or knowledge. The new revenge porn law extends the same misdemeanor criminal status to anyone who takes nude pictures of another person with the understanding that those images are to remain private but subsequently disseminates the images without permission to cause serious emotional distress.

Criticism of New Law

Some may argue that the misdemeanor penalties of the new California revenge porn law are not severe enough. Opponents may believe that the need to prove intent to cause serious emotional distress may be too high a standard for guilt under the statute.

Moreover, critics may be disenchanted that the new law does not cover "selfies" -- meaning that the law does not criminalize the subsequent distribution of nude photos women have taken of themselves that they intended to share only with their partners. In addition, many may not like that the new law does not specifically go after operators of websites and instead only targets the people who post the damaging photos.

While such arguments can be made, the new California revenge porn law is a step in the right direction in creating criminal liability for the harm caused by public revenge porn humiliation.

Can You Really Remain Anonymous on the Internet?

September 10, 2013

In the early days of the Internet, an editorial cartoon from *The New Yorker* depicted a dog in front of a computer monitor and keyboard with a caption that read "On the Internet, nobody knows you're a dog." The point was that people could behave however they liked online without others knowing their true identity.

But is that really true? Au contraire my canine friends.

Revealing Anonymous Speech

While it is true that there is a First Amendment right to free and anonymous Internet speech, that only goes so far. For example, if someone using a pseudonym makes false statements on the Internet that cause harm to others, that can give rise to a potential defamation lawsuit.

Injured parties can then initiate legal action against "John Doe" defendants (porn companies are already adept at this) and subpoena the Internet service provider(s) to reveal the true identity of any person(s) who made the allegedly defamatory Internet statements.

At that point, the ISP likely would provide notice so that the person who engaged in the Internet speech at issue would have the opportunity to file a motion to quash the subpoena. In evaluating a motion to quash, the court would weigh the right to anonymous Internet speech against the need of a truly harmed party to recover damages for harmed caused. Likely, the court would require there to be a prima facie initial showing of tangible harm before actually unmasking the Internet speaker's true identity.

Anonymity Slipping

In addition to the foregoing, practically 60 percent of Internet users recently polled by the Pew Research Center (PRC) do not believe it possible to operate completely anonymously on the Internet, reports CNET. But PRC's report revealed 59 percent of those polled feel that they should be able to communicate anonymously on the Internet. And in excess of 85 percent of these Internet users have made efforts to conceal their identities secret on the Internet.

Users seeking anonymity not only avoid using their real names, but they also encrypt email, remove cookies, and attempt to hide their IP addresses. Modern Internet consumers are presumably taking matters into their own hands, and according to the PRC study, 66 percent believe existing privacy laws provide insufficient protections.

So, if you speak (or bark) on the Internet, others may truly know or find out that you are a dog.

NSA Seeks to Come Clean on Surveillance Practices

August 20, 2013

With potential reforms in the wind with respect to government surveillance practices, the National Security Agency (NSA) has issued a seven-page report that seeks to explain and justify its conduct.

The report, titled "The National Security Agency: Missions, Authorities, Oversight and Partnerships," begins with a quote from President Obama that calls for "reviewing the authorities of law enforcement, so we can intercept new types of communication, but also build in privacy protection to prevent abuse."

NSA Report Justifies Surveillance

In its prologue, the NSA report claims that when the 9/11 attacks occurred, the NSA did not have the tools or the database to allow it to search and identify certain information connections and share them with the FBI.

Due to this blind spot in intelligence, the report explained that the government's agencies needed "to connect the dots of information available to the intelligence community and to strengthen the coordination between foreign intelligence and domestic law enforcement agencies."

Likely in reaction to concerns about governmental review of the private communications of law-abiding citizens, the NSA states that while the Internet transmits 1,826 petabytes of information daily, the NSA "touches about 1.6% of that." And, of this 1.6% of data, "only 0.025% is actually selected for review."

Accordingly, "the net effect is that NSA analysts look at 0.00004% of the world's traffic in conducting their mission." Doing the math, the NSA says that amounts to "less than one part in a million." As such, "NSA's total collection would be represented by an area smaller than a dime on [a] basketball court."

Remaining NSA Worries

While this metaphor may satisfy some critics, the actual amount of communications reviewed by the agency is fairly substantial when considered standing alone. Rather than focusing on the sheer amount of information, more interesting questions lie in what types of information are collected are what is done with that information after it has been reviewed.

Plainly, the NSA has important missions, including preventing terrorism, and as the NSA points out in its report, there are various legal bases and authorities supporting its practices. Still, as President Obama recognizes, we need to "build in privacy protections to prevent abuse."

The NSA attempts to provide further comfort by explaining that while it partners with more than 30 other countries as part of its foreign intelligence efforts, the "NSA does not and will not use a relationship with a foreign intelligence service to ask that service to do what NSA is itself prohibited by law from doing." The NSA states, for example, that its combined efforts with other countries has saved allied lives in Iraq and Afghanistan.

Striking the appropriate balance between governmental surveillance for foreign intelligence purposes and protecting privacy interests is not an easy matter. The NSA in this instance should be applauded for issuing its recent report. While the report does seek to justify the conduct of the NSA, at least the NSA does explain some of its practices to shed some light for public consideration.

Vacation Should Mean Vacation in the Tech Era

August 6, 2013

We live in the always-on age. Around the clock we can log in and communicate electronically in many ways.

While this often is advantageous and convenient in the working world, this dynamic can create challenges and even risks when it comes to vacations.

'Vacation' Means Taking a Break

We are rewarded with vacation for a reason. It gives us the opportunity to take a break from the workplace, relax, and rejuvenate ourselves with down time and leisure activities.

However, we have grown increasing accustomed to reaching for our smartphones, tablets and laptops so that we can keep in touch and stay on top of work developments, even when we are supposed to be "off."

Digital burnout has become such a problem that there are now specific getaways premised on disconnecting people from their devices, like Camp Grounded in California, *The New York Times* reports.

Over time, this unhealthy connection to our data streams can take its toll. There is greater likelihood of mental burnout and lower productivity when one returns to the workplace without a genuine break from the buzz of the working world.

Risk to Employers

Aside from the deleterious effects a working vacation can have on personal well-being, companies are growing increasingly concerned about the risks presented from personnel working remotely while on vacation.

One potential risk facing any company is the possible leak of sensitive company information while an employee is using a smartphone in a public place. By the same token, there can be less security when vacationing employees forward private company communications to their personal email accounts.

Company information also can be pirated when employees use Wi-Fi hot spots while on vacation. And, of course, many smartphones and other devices are lost each year when employees are traveling, which can lead to misappropriation of confidential information.

Because of these risks, some companies now are not allowing employees to work remotely on vacation, or if they do, they provide strict guidelines that are to be followed. Hopefully, these employers also are compassionate, wanting their employees to refresh themselves by taking true vacations, not working vacations.

Part of the onus, naturally, has to be on the employee too. Even if working vacations are permissible, that employee would be well served to opt-out of checking email, enjoy the fresh air and sunshine, and leave work to another non-vacation day.

American Universities Under Siege by Cyberattacks

July 23, 2013

American universities are being bombarded by cyberattacks, according to a recent *New York Times* article.

These universities are being hit with millions of hacking attempts per week, and some of those attempts have succeeded in obtaining personal and other data.

Unfortunately, at times these data compromises are not discovered until long after the fact, if at all.

Cyberattacks Present Real Threat

Undoubtedly, information held by universities can be sensitive and valuable. Not only do universities have identifiable personal information relating to students, faculty and others, but they also house important intellectual property, as universities are on the cutting edge of patent development in many areas.

In terms of volume, some universities report that the number of cyberattacks they experience are doubling every few years, and the University of Wisconsin reported hacking attempts on the institution up to 100,000 times per day from China.

The New York Times reports that most of the hacking attempts on American universities emanate from China, yet hackers are adept at covering their tracks by routing their attacks across various computers and, at times, multiple countries.

Therefore, while it appears that China is the critical source of many of these attacks, it is very difficult to pin the attacks on specific organizations or individuals.

Securing University Data

In the wake of increasing cyberattacks, some universities are beefing up their computer security systems, while others are preventing their professors from taking laptops to certain countries.

Universities' systems characteristically can be difficult to secure, as a great number of students, faculty and staff have the ability to sign in from their own computers. As a result, some universities are keeping the "external shells" of their systems relatively open, while locking down more sensitive information within "smaller vaults" with encryption.

Given the current state of affairs, American universities should do everything they reasonably can to protect vital information.

FTC Updates Advertising Disclosure Guidance for Search Engines

July 2, 2013

Back at the dawn of the commercial Internet era in 2002, the Federal Trade Commission provided guidance to search engines in terms of differentiating between true search results and advertisements. However, over the past 11 years, the FTC has determined that search results and advertisements have become less distinguishable from each other.

Accordingly, in correspondence recently sent to major search engines such as Google, Bing, Yahoo and AOL, the FTC has updated its 2002 guidance.

In its correspondence, the FTC explains that "consumers ordinarily expect that natural search results are included and ranked based on relevance to a search query, not based on payment from a third party." And, to prevent confusion or even deception, "consumers should be able to easily distinguish a natural search result from advertising that a search engine delivers."

The FTC tells the search engines in its correspondence that "clarity and prominence of advertising disclosure are key."

Visual cues and text labels are suggested by the FTC.

As to the former, the FTC recommends that in differentiating top advertisements or other advertising results integrated into natural search results, there should be **more prominent shading** that contains a clear outline, **a prominent border** that distinctly sets off advertising from natural search results, or both.

With respect to the latter, search engines should use a text label that:

- Explicitly and clearly states **that a search result is advertising**,
- Is sufficiently **large and visible** for notice by consumers, and
- Is **located near the search results** that it qualifies.

The FTC also explains that the need to plainly differentiate search results from advertisements applies even in the context of new search platforms, like mobile apps, voice search and social media.

The FTC thanks the search engines for their anticipated cooperation. And cooperation is expected. Indeed, the correspondence closes by seeking "cooperation in *ensuring* your business practices conform to the supplemental guidance provided in this letter." (Emphasis added.)

DDoS Attacks, 'Zombie' Sites On the Rise

June 11, 2013

Distributed denial-of-service (DDoS) attacks are not hypothetical possibilities. Indeed, they have been bringing down websites for quite some time.

Most recently, two men in Britain have been sent to prison for their DDoS attacks perpetrated on PayPal and other sites, according to *InformationWeek*.

The *InformationWeek* article notes that six people were arrested in connection with these DDoS attacks. Three of them ultimately were charged under the United Kingdom's Computer Misuse Act of 1990. Of these three, the head of the group received a prison sentence of 18 months, another was sentenced to seven months in jail, and the third was sentenced to six months in jail which was suspended for two years while he was ordered to serve 100 hours of community service.

This reportedly marks the first instance in which DDoS perpetrators actually have been sentenced to imprisonment in Britain. DDoS attacks can wreak havoc on commercial websites. Indeed, InformationWeek notes that PayPal had informed the court that it had suffered $5.5 million in damages for just these attacks. Likely, others will go to jail for such violations.

However, it is not always easy to track down the DDoS attackers. The attacks, which bombard websites with numerous packets of information to the point of shutting down the sites, can be launched directly; but they also can be routed through innocent "zombie" sites, making it more difficult to ferret out the originating sources of the attacks.

We no longer live in an era in which there is little knowledge about the possibility of DDoS attacks. Companies and other entities should take protective measures to do their best to secure their websites from DDoS attacks. They also should try to safeguard their sites from being used as "zombie" launching pads for attacks on other sites.

We live in a new world where the Internet reigns supreme, but where new risks have emerged that must be addressed.

New WTO Information Technology Agreement May Do Away With Duties

June 4, 2013

The imposition of duties on the global trade of technology products is significant from a monetary standpoint.

However, Reuters reports that a potential agreement among the United States, China, the European Union and almost two dozen other countries that could eliminate billions of dollars of such duties might be achieved as soon as within in the next two months.

At issue is the negotiation of a possible expansion of the World Trade Organization's Information Technology Agreement. The Agreement is a pact from the late 1990s that ended duties on a wide array of technology products. These products include laptops, computers, telephones, fax machines, software, semi-conductors and some office machines.

The Agreement's original membership has expanded to 75 nations over time, including the various nations of the European Union. Still, that is not even 50% of the World Trade Organization's 159 members. However, it does account for roughly 97% percent of worldwide trade in subject technology products.

The pact encompasses in the range of $4 trillion in current trade. It is reported that an expanded Agreement could cover $800 billion in additional trade. That is real money, obviously.

Additionally, U.S. companies are anxious to see the Agreement augmented to cover flat-screen displays for computer monitors and televisions. The European Union, has been reluctant in this regard, because it has a 14% tariff on flat-screens and likely is concerned that this could cause U.S. and Asian manufacturers currently based in Eastern Europe to move elsewhere.

Other products like speakers, headsets, and other electronic components also are sought to be included by the United States.

A number of members of the present Agreement, such as major nations India and Indonesia, have not entered into the fray with respect to the potential expansion of the pact.

It will be worthwhile to monitor developments in this area to see what unfolds.

From CrackBerry Addict to iPhone Junkie: A Lawyer's Tale

May 21, 2013

Up until recently, and for years, I was a lawyer addicted to his BlackBerry. My BlackBerry always was on my hip, ready for immediate use. I became so proficient that I literally could type as fast with two thumbs on the device as I could with all of my fingers on my desktop keyboard at work. But other attorneys kept whispering in my ear, "Try the iPhone -- once you do, you will never go back to the BlackBerry."

So, over the New Year holiday, I tried my daughter's iPhone. I must say, I was most intrigued by Siri and the voice-recognition feature, not to mention the much larger screen.

I nevertheless did procrastinate -- change is hard. Ultimately, a couple months later, I ordered the most current version of the iPhone, and with 64 gigs of memory to boot. But, at least for a couple weeks, the iPhone stayed in its box and I kept on using my BlackBerry. I had a mortal fear that I would not handle the iPhone well (especially the touchscreen typing) and that my work would grind to a halt. Thus, I kept reading and learning about the iPhone without actually taking the plunge.

Finally, on a trip to the Big Apple a month ago, I freed the iPhone from its box. I dove into the device like a madman, trying to master its functions while downloading and using many apps. I overlapped with the BlackBerry for a couple weeks -- just in case.

Ultimately, I was confident enough to part ways with my BlackBerry, though I did suffer some withdrawal. I still miss the tactile keys for typing on the BlackBerry, as well as the little red light that indicates that messages are waiting for retrieval. The BlackBerry's battery life also is remarkably good.

However, for me at least, the iPhone wins when it comes to everything else. The larger screen size really does afford better viewing of all sorts of content. I really do use Siri and voice-recognition with ease and speed (the latter helps because I still am not too fast at typing on the touchscreen). The camera and video functions certainly are more than adequate. And the wide array of apps for the iPhone is fantastic.

My favorites include Flipboard; CNN and NPR for news; Downcast for podcasts; Pandora for music; Audible for audiobooks; Flashlight; AroundMe for restaurants, gas stations, hotels, movie theaters and other nearby attractions; Google Maps; Google Translate for foreign languages; Fastcase for legal research; and ESPN's ScoreCenter. I have downloaded, and use, dozens of other apps too.

Also, my iPhone really syncs with my car via Bluetooth; while that was supposed to be true for my Blackberry, it was not the case. I appreciate very much being able to speak hands-free on

the phone in the car. And I can get Pandora going in my car via my iPhone, whereas that did not work with my BlackBerry.

All in all, I now am an iPhone junkie. However, once in a while I still do jones for the BlackBerry keyboard.

Workers' Firings Over Facebook Complaints Were Improper: NLRB

May 7, 2013

In the case *Design Tech. Grp. LLC d/b/a Bettie Page Clothing*, the National Labor Relations Board (NLRB) has ruled that employees of a clothing company were improperly terminated based on comments they made on Facebook complaining about their supervisor and expressing their workplace concerns.

According to the administrative law judge's ruling, which was appealed to the NLRB, workers at Bettie Page Clothing engaged in the following exchange on Facebook:

> Holli Thomas: needs a new job. I'm physically and mentally sickened.
>
> Vanessa Morris: It's pretty obvious that my manager is as immature as a person can be and she proved that this evening even more so. I'm am [sic] unbelievably stressed out and I can't believe NO ONE is doing anything about it! The way she treats us in [sic] NOT okay but no one cares because everytime we try to solve conflicts NOTHING GETS DONE!!
>
> Holli Thomas: bettie page would roll over in her grave.
>
> Vanessa Morris: She already is girl!
>
> Holli Thomas: 800 miles away yet she's still continues our lives miserable. Phenomenal!
>
> Vanessa Morris: And no one's doing anything about it! Big surprise!
>
> Brittany [Johnson]: "bettie page would roll over in her grave." I've been thinking the same thing for quite some time.
>
> Vanessa Morris: hey dudes it's totally cool, tomorrow I'm bringing a California Worker's Rights book to work. My mom works for a law firm that specializes in labor law and BOY will you be surprised by all the crap that's going on that's in violation 8) see you tomorrow!

The NLRB found that the administrative law judge (ALJ) had correctly determined that the employer had violated the National Labor Relations Act and that the employees had been engaged in protected concerted activity under the Act.

Furthermore, the NLRB ruled that the ALJ was right in rejecting the employer's defense that the employees supposedly had schemed to "entrap" the company into terminating them.

The online comments at issue involved complaints that a store manager had been overbearing and unfair, as well as concerns about safety when the stored closed. Ultimately, the store manager was shown the Facebook postings, and thereafter the employees were fired.

While it is one thing for companies to control closely content posted on their own Facebook and social media pages, it is another matter entirely for them to terminate employees based protected speech on the employees' Facebook pages.

Cybersecurity Bill Passes the House, But What's Next?

April 23, 2013

The House has approved the Cyber Intelligence Sharing and Protection Act (CISPA, H.R. 624). CISPA allows private companies and the federal government to exchange information relating to cybersecurity threats.

The bill was passed in the face of some concerns that it might provide private consumer information to the government. According to Reuters, President Obama has threatened to veto the bill on the basis that it supposedly does not mandate that companies take the greatest efforts to remove personal information before providing it to the government.

CISPA specifically states that it would amend the National Security Act of 1947 by adding a new section titled "Cyber Threat Intelligence and Information Sharing."

That section provides that the Director of National Intelligence is to establish procedures to allow elements of the intelligence community to share cyber threat intelligence with private entities and utilities.

As such, classified cyber threat intelligence may only be shared by an element of the intelligence community with a certified entity, a person with appropriate security clearance, and shared consistent with the need to protect the national security of the United States.

Cyber threat information is to be shared only pursuant to restrictions placed on the information by the protected entity authorizing such sharing, and may not be used to gain any unfair competitive advantage to the detriment of a protected entity authorizing the information-sharing.

Information shared is to be exempt from disclosure under the Freedom of Information Act. Furthermore, there is to be no civil or criminal liability based on a protected entity sharing cyber threat information in good faith.

Shared cyber threat information may be used by the federal government for cybersecurity purposes, for the investigation and prosecution of cybersecurity crimes, for the protection of individuals from danger of death or serious bodily harm, and for the protection of minors from child pornography, sexual exploitation and physical safety.

CISPA also provides that the Director of National Intelligence shall establish policies and procedures that, among other things, "minimize the impact on privacy and civil liberties" and "protect the confidentiality of cyber threat information associated with specific persons to the greatest extent practicable."

The devil always is in the details. And while the bill likely is positively motivated and calls for policies and procedures to be created protect privacy, civil liberties and confidentiality, it very well may be that such policies and procedures will need to be specifically outlined in advance before this type of legislation actually can become law

.

Apps Gone Wild: Is There Anything They Can't Do?

April 2, 2013

Once upon a time, I was known as Inspector Gadget. Why? Because I wore on my belt three different devices — a mobile phone, an iPod, and a Palm Pilot. The phone was only good for calls, the iPod could only play music, and the non-wireless Palm Pilot was simply a calendaring assistant.

I wondered then whether there could ever be convergence, such that at some point I only would need to carry around one device. Of course, that did happen, but the convergence occurred beyond my wildest dreams.

Sure, on one device the size of a deck of cards, I can make calls, play music, and I can organize my calendar. But that is just the tip of the iceberg.

I can exchange emails and texts, I can take and receive photos and videos, I can watch television shows and movies, I can search the Internet, I can talk to my daughter while seeing her live in Europe by videoconferencing, I can work on documents, I can engage in social networking, I can perform financial calculations, and more.

Indeed, there now are hundreds of all sorts of apps that can be downloaded and implemented on a smart phone. Some of the apps are very useful, others are extremely creative, and some are just plain fun.

There are apps for flashlights, GPS mapping/tracking, weather forecasting, and all sorts of games. There are also apps for a wide variety of business, education, entertainment, finance, health and fitness, news, traffic and many other functions. The list just goes on and on. Indeed, there are even apps for the current NCAA March Madness basketball tournament.

I truly have the world at my fingertips within a small handheld device. Amazingly, a tiny smartphone has much more functionality than the massive yet ancient computers I tried to handle decades ago while in college in the library's basement computer room. Remember computer punch cards?

The phenomenal capabilities of smartphones now are so alluring and still developing that the main challenge is to look up once in a while and stay present in the real world.

Google Transparency Reveals FBI's Use of National Security Letters

March 12, 2013

Google has posted a "Transparency Report" that provides a range of how many National Security Letters (NSLs) it has received and a range of how many users/accounts were specified in these NSLs each year since 2009. Of course, your first question may be: What is an NSL?

An NSL is a special search vehicle by which the FBI has the authority to demand the disclosure of customer records maintained by banks, Internet Service Providers, telephone companies and other entities. When this happens, these entities are prohibited from revealing to others their receipt of an NSL. There have been reports that the issuance of NSLs has expanded significantly since the Patriot Act increased the FBI's power to issue them.

Getting back to Google, its Transparency Report details that for each of the years 2009, 2010, 2011, and 2012, it received between 0 and 999 NSLs. And for the years 2009, 2011, and 2012, these NSLs specified between 1,000 and 1,999 users/accounts, while the range was between 2,000 and 2,999 for the year 2010.

Google only was able to reveal these numerical ranges after it had engaged in negotiations with government officials.

Because NSLs are generally handled in secret, understanding their use and frequency has been difficult. Also, there has been little oversight when it comes to NSLs, which makes them controversial.

According to the *San Francisco Chronicle*, Google has stated that the NSLs can be used to compel companies to identify the name, address, length of service and local and long-distance toll billing records of a customer -- but not Gmail content, search queries, YouTube videos or user IP addresses. The FBI has issued an average of nearly 50,000 NSLs per year for the time period 2003 to 2006, The Washington Post has reported.

NSLs are supposed to address national security investigations. They are not designed to focus on usual criminal, civil, or administrative matters.

The foregoing numbers seem to suggest a fairly broad use of NSLs. We must hope that they have been used as intended. Without much oversight, it is not easy to know for sure if that indeed has been the case.

The Legal Ethics of Social Media and the Cloud

February 5, 2013

Social media no longer is the province of only those who are college-aged or younger. Indeed, businesses of all types now seek to capitalize on social media connections, and law firms are no exception. Many firms now have their own Facebook pages, for example, and many lawyers are seeking to attract attention through a variety of other social media sites such as LinkedIn and Twitter. Also, more and more, information is being stored in the cloud.

Notwithstanding this gravitational pull toward clouds and social media, lawyers need to remain mindful of ethical and practical constraints, so that they do not feel more pain than joy in this context.

Targeted Advertising by Lawyers

There are numerous potential issues, two of which are touched on here. The first is best illustrated by a hypothetical: Suppose a person posts on Facebook that she was recently injured in an automobile accident. Shortly thereafter, Facebook pushes an ad to her from a personal injury law firm. Is there a problem?

As far back as the 1970s, the U.S. Supreme Court held that it was permissible for law firms to advertise generally. But this hypothetical represents targeted, not general, advertising.

In the non-legal context, the FTC has weighed in and has recommended certain principles that should apply when it comes to targeted (or behavioral) advertising. In a nutshell, the FTC suggests that websites should be transparent so users are informed as to how they may be tracked and targeted, and that choice should be provided so users can opt out of this process.

Back to the legal context, ethical rules provide that a solicitation from a lawyer to a potential client cannot contain untrue statements, cannot confuse or be deceptive, and cannot intrude. When it comes to our hypothetical, the advertisement of the personal injury law firm to the injured Facebook user could potentially be considered deceptive and/or intrusive, as the injured user does not understand or know why she has received the advertisement in response to her injury.

Thus, the hypothetical targeted advertising probably is not a good practice, unless people somehow could choose to receive such ads -- but it is difficult to imagine how that would unfold in this precise setting, as people do not know in advance that they will be injured. Moreover, recent studies show that while social media might be good for branding generally, it does not necessarily translate into true revenue from direct advertising.

So while a law firm's Facebook page may be good image building, the hypothetical targeted advertising, whether proper or not, might not lead to legal work anyway. Additionally, other studies indicate that the public views targeted advertising in a dim light, and this may be yet another reason not to engage in the targeted advertising suggested by the hypothetical.

Legal Issues in the Cloud

The cloud presents another area where thorny issues can emerge for lawyers. It is not uncommon for lawyers now to consider to engage a cloud provider for storage of client and other data. The ABA Commission on Ethics 20/20 recently highlighted some real cloud issues that need to be addressed.

Those cloud issues include:

- The potential unauthorized access to client confidential data in the cloud;
- The possible failure properly to back up data stored in the cloud;
- The storage of information in countries where there are less legal protections than in the United States;
- A lawyer's potential inability to access data if the relationship with the cloud provider changes or ends;
- The possible lack of clarity in terms of who owns the data stored in the cloud;
- The prospect of inadequate encryption;
- The extent of consent needed from clients before lawyers engage cloud providers to store data; and
- Policies as to cloud data destruction when data no longer is needed.

And, of course, there are other issues, such as the need to comply with regulatory requirements, like HIPAA requirements for sensitive medical information.

While social media and the cloud present new ways to communicate and store information, the ethical responsibilities of lawyers remain intact. Lawyers therefore must be educated and mindful as they move forward in the new high-tech world.

High Tech Replacing Familiar Favorites, But Low Tech Will Live On

January 22, 2013

Technology is advancing at warp speed, and the way we live is changing constantly. Indeed, what was once lifestyle bedrock is now going the way of the dinosaurs.

For example, when I backpacked in Europe more than three decades ago, I kept in touch with my family by way of aerogrammes and postcards. Those days are gone. My daughter just started her study abroad program in Copenhagen, and within hours of hitting Danish soil, I heard from her by way of Facebook messages and mobile telephone calls via Skype.

On top of this example, I recently read an email that is spreading across the Internet that suggests the imminent disappearance of certain aspects of life that we have been accustomed to for a very, very long time.

The first email suggestion is that the **U.S. Postal Service** will not survive. Email, text messages, social media communications, FedEx and UPS all will wipe out any marginal remaining post office viability. It is true that the postal service has been impacted greatly, and we will see if it remains in force, at least to some extent. There may be some continuing utility, but perhaps in a much decreased role.

The next email prediction is that in short order we no longer will make payments with **hard-copy checks**. Plastic cards and online payments already are rendering checks as quite a secondary payment method. While check writing may have decreased, checks may not disappear completely as a means of payment.

Also soon to be extinct is **the traditional newspaper**, according to the email. People now are getting their news on their laptops, their mobile devices and their e-readers. Plus, it is suggested that the current younger generation does not even consider the newspaper as an option. And while news will be obtained online, it is predicted that in the near future we will have to pay for such access. This all could be true, certainly to a large extent.

And what about **the old-fashioned book**? Won't there still be instances when people want a hard copy in their hands so they can experience actually reading from and turning pages? Not according to the email prediction: People will prefer the storage, ease and cost-effectiveness of reading on gadgets. While reading will continue to go the electronic route, it is difficult to imagine hard-copy books no longer on the scene at all.

Not too surprisingly, it is suggested in the email that **the landline telephone** will fade into history. People use their mobile phones constantly for many purposes, not just phone calls. And there is no true reason to have a landline phone other than habit, and there is no valid reason to pay for such a phone in addition to a mobile phone. This could come to pass, at least for the vast majority of people.

The email also decries the death of **innovative music**. The argument is that a good portion of the music purchased today is that created by established artists. However, the Internet has allowed some previously unknown artists to be discovered and to make it big.

The demise of **traditional network television** also is suggested by the email. It is true that people have many more ways now to entertain themselves in the past. There are so many forms and means of entertainment in the new electronic age. So, yes, the dominance of traditional television programming has waned.

The email also predicts the end of **"things that you own."** The point is that rather than owning your music on CDs, for example, you will have access to your music in the cloud. This also will be true for photographs, movies, documents, etc. Yes, there is a good deal of truth here, although we still will want real possession of some aspects of our personal lives.

Finally, the email proclaims the death of **privacy**. Certainly, the world is a smaller, fishbowl place than it used to be. There are cameras practically everywhere tracing our moves. GPS technology maps out our exact locations, and where we go online leaves digital footprints. But still, human dignity requires privacy in certain spheres, and the laws are developing to protect privacy. Privacy is like oxygen: It is not really noticed until it is gone, so there must be protection on the front end where it counts.

It is a brave new world; fasten your seatbelts, and enjoy the ride.

Get Your eDiscovery Together, Or It Could Cost You in Court

January 15, 2013

Once upon a time, the production of information in civil litigation primarily consisted of the exchange of hard-copy, paper records. Those days are long gone.

We now are in the electronic age, and productions feature all sorts of electronic data. It is important to get it right when it comes to eDiscovery, as the downside consequences for getting it wrong can be severe.

As soon as litigation happens or is reasonably believed to be on the horizon, it is imperative to implement a "legal hold" to preserve potentially relevant data. In this way, relevant data will not be destroyed. The failure to preserve relevant data can lead to charges of spoliation of evidence. Actual spoliation can lead to court orders excluding evidence, creating negative evidentiary inferences, leading to the dismissal of claims or defenses, awarding significant monetary sanctions, and/or entering judgment against the spoliating party.

Potentially relevant data must be collected for use and production in litigation. There can be many sources of data. These include information on networks, hard drives, and hand-held devices, and can include electronic documents, emails, text messages, social media communications, and even voicemail messages. Older information stored on back-up tapes at times may have to be retrieved. Where possible, it is advantageous to reach agreements with opposing counsel in terms of sources of data, custodians of data, and search terms.

The processing of electronic data for discovery purposes can involve a number of steps. One issue to consider is whether text and metadata should be removed from native files.

Prior to production to opposing counsel, a review phase should be implemented to ensure that privileged information is not produced, and to produce only information that is responsive to discovery requests. At times, sensitive, confidential and/or trade secret information will need to be treated with different levels of protection. It is wise to negotiate a mutually acceptable protective order with opposing counsel. There are different types of tools that can be utilized to help in the review process.

The production itself likely should be based on agreed-upon specifications with opposing counsel. Frequently, the production is loaded onto a document review platform.

There are many other issues and nuances when it comes to electronic discovery. A suitable New Year's resolution for companies is to get their eDiscovery houses in order. They should consult with counsel skilled in this area to move forward, if they have not done so already.