DuaneMorris®

www.duanemorris.com

ERIC SINROD'S SAMPLING OF WEEKLY BLOGS ON FAST-BREAKING INTERNET LEGAL DEVELOPMENTS FOR FINDLAW.COM

JANUARY 1, 2010 - PRESENT

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.

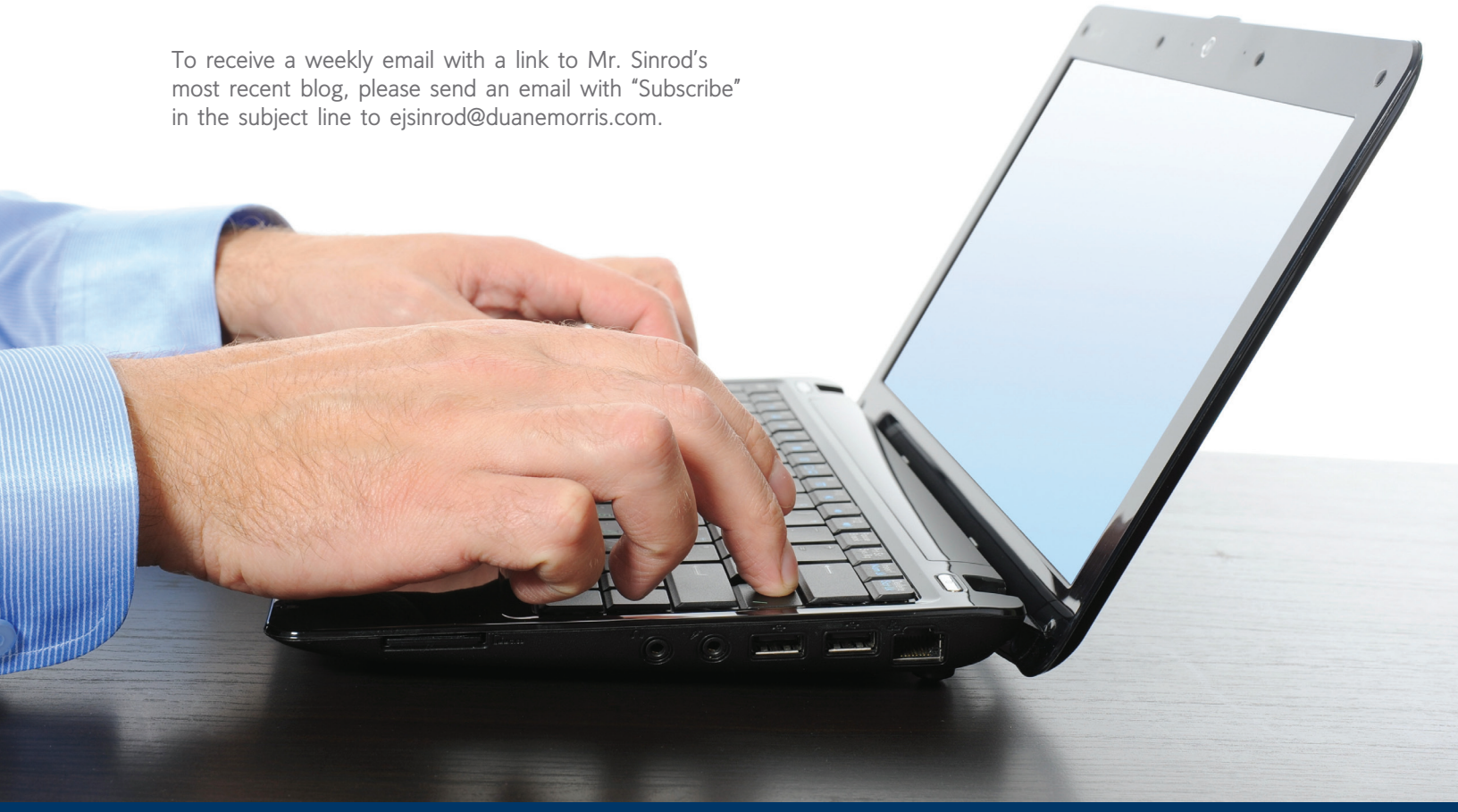

Table of Contents

(link)

Google Buzz Settlement: Privacy Audits For 20 Years

April 5, 2011

Google has entered into a settlement with the Federal Trade Commission (FTC) to address perceived privacy violations relating to the social network, Google Buzz.

The Google Buzz settlement requires Google to implement a comprehensive privacy program and to be subject to independent privacy audits for the next 20 years.

Why could this end up being a big deal?

Google found itself in the cross-hairs of the FTC with respect to alleged deceptive tactics and violations of Google's privacy practices having to do with Google Buzz.

According to the FTC, Google had given its Gmail email users the impression that they could choose if they wanted to join the network, while the options for declining Buzz actually were ineffective.

In addition, the FTC asserted that Google's controls for limiting the sharing of personal information were confusing and difficult to implement. For example, Buzz contained a feature that allowed it to publicly list a user's frequent email contacts; while this feature could be turned off, the default setting was to leave it on.

The Google Buzz settlement does serve notice to other companies that the FTC is watching and checking to ascertain whether privacy promises in policies actually are adhered to in practice.

However, the penalty as to Google is not too severe. Yes. Google needs to develop a comprehensive privacy policy, and it will be subject to independent privacy auditing for 20 years. But it is in Google's best interests anyway to have sound privacy policies and practices.

Creating an atmosphere of security and safety for the personal information of customers equates to good business. Users will tend to gravitate over time to places on the Internet where they know that their private information will not be compromised.

(link)

Porn Websites Get Go Ahead for .xxx Domain Suffix

March 29, 2011

Pornography web sites have finally been given the green light to establish the .xxx suffix for their domain names, according to the Internet Corporation for Assigned Names and Names (ICAAN) .

Thumbs up? Thumbs down?

Well, not surprisingly, the reception has been mixed.

While, on the one hand, one might think that the pornography industry would be in favor of the .xxx suffix as an easy way to categorize and find their sites, there actually has been some backlash. Indeed, industry members have expressed concern in the media that by being grouped within the .xxx domain suffix, those sites potentially could be on the receiving end of censorship from certain governments and other types of regulation.

They also have voiced that they now may have to register .xxx domains to protect their names and trademarks contained within their current .com domain names so as not to allow others to register their names and marks using the .xxx suffix.

Some opponents of pornography also have expressed discontent. They worry that the .xxx suffix makes it even easier for people to seek out and find "smut" on the Internet.

But, of course, there are people in favor of the .xxx suffix. Their argument is that it is good to provide an easy to understand suffix that makes plain that a site with the .xxx suffix contains adult content. While that naturally makes it easy for people who want that content to find it, the opposite also is true – people who do not want to view pornography can avoid and even filter out .xxx Web sites.

And, of course, there is money to be made.

Over 200,000 .xxx domain names reportedly have been registered already, with each such registration costing $60 annually. ICM Registry will oversee the .xxx domain process, and certainly is not complaining about recent developments.

It will be interesting to see whether sites that truly are not related to adult content will also seek to register .xxx domains, perhaps to try to spice up their image or gain greater traffic or attention.

(link)

Distributed Denial Of Service Attacks Are Still Cause For Concern

March 8, 2011

Distributed denial of service (DDOS) attacks are not creatures of the past. Indeed, they still are with us, as exemplified by the recent DDOS attack on WordPress, a blogging site.

According to recent press reports, this attack impacted connectivity for a large number of the 25 million WordPress bloggers.

The press reports indicate that the magnitude of this distributed denial of service attack was multiple gigabits and tens of millions of packets of information per second, impacting data centers in Chicago, San Antonio and Dallas. While WordPress reportedly is seeking to grapple with the attack, it is having some difficulty based on the sheer size of the attack.

A DDOS attack, in essence, and for the sake of simplicity, is the bombardment of so much data to a Web site that the site is overloaded and shuts down. Obviously, when a commercial Web site is not operational, there is an interruption in business and operational revenue. Thus, DDOS attacks can represent a real threat to the commercial viability of a site.

Naturally, to the extent possible, defensive technical measures should be taken to prevent the intrusion of DDOS attacks. And, where such measures are not successful, legal remedies are available.

However, the perpetrators of the attacks may not be sufficiently solvent to make a legal recovery meaningful. Moreover, at times it is difficult to track down and ascertain who actually launched a given DDOS attack. This is because at times as such an attack can be routed through various "zombies" sites, making it difficult to track the attack back to its original source.

So, why are DDOS attacks with us? It is not always easy to peer into the minds of those who are bent on destruction. The motivation in a given instance could have to do with simple mischief, or it could relate to efforts to harm a commercial competitor, or it could be politically inspired.

Whatever the case, DDOS attacks remain on the Cyber scene and must be addressed.

(link)

On The Internet, People Can Find Out If You Are A Dog

February 15, 2011

Long ago and far away, back when the Internet first started gaining traction as a public communications medium, a cartoon depicted a dog logging onto a computer with a caption that read: "On the Internet, nobody knows you are a dog." The clear implication was that the Internet was a new playground where communications could be free and anonymous. But is that really the case as the Internet has matured? Not necessarily.

It is true that people have a constitutional right of free speech. Indeed, that right has been interpreted by courts to allow for free online anonymous speech – but to a point.
While people can say what they want on the Internet without providing their true identities, perhaps operating under pseudonyms, their identities can be unmasked under certain circumstances.

The right to free online anonymous speech potentially ends when that speech is defamatory. If what is posted online and is false, and causes harm the true identity of the online communicator can be unmasked.

For example, let's say hypothetically that a person with the true name John Smith sets up a Web site and on that site under the pseudonym "Consumer Crusader" he proclaims that a well-known fast-food chain serves rat instead of chicken as represented in its fried food offerings. Continuing with the hypothetical, let's assume that as a result of the hysteria whipped by this site, there is a large drop off in the number of customers that go eat at the chain's restaurants and that the share price of the chain plummets. Can John Smith's anonymous free speech rights protect him from being unmasked as the person behind the Consumer Crusader and associated Web site?

Well, first the fast-food chain likely would file a defamation lawsuit against a "john Doe" defendant – the person behind the Consumer Crusader whose identity is not yet known. The idea would be to substitute in the true name of this defendant (John Smith) in the lawsuit once his identity is ascertained.

Next, the fast-food chain would subpoena the ISP that hosts the Consumer Crusader's Web site for his identity. The ISP then would give John Smith notice that his identity will be revealed pursuant to the legal process of the subpoena unless John Smith timely files a motion to quash.

If John Smith files such a motion, he would argue that his online anonymous free speech rights trump any interest in obtaining his true identity. Obviously, while making this motion to the court, he still would be operating under a fictitious name. The fast-food chain would counter this argument by setting forth the falsity of the online statements made and the harm suffered.

Ultimately, if the court finds that the fast-food chain has made out a prima facie case of falsity and harm, John Smith's identity would be unmasked and his name would be added as the true defendant in the defamation lawsuit, and he then would have to defend the case. Of course, if his identity is not unmasked, the lawsuit essentially would end, as there would be no true defendant to go after.

In this particular hypothetical, it is highly likely that John Smith's identity would be unmasked, and if he were a dog, that would come out, contrary to what was suggested in the cartoon.

The lesson learned is that people should not take comfort that they can say whatever they want without implication on the Internet, even if they do have some rights of anonymous online speech.

(link)

Harvesting Electronic Discovery

February 1, 2011

Since the Federal Rules of Civil Procedure were amended at the end of 2006 to specifically embrace electronic discovery, parties to litigation and their counsel have been scrambling to figure out the best and most economical ways to comply with their obligations in this area. And while the rules were amended with the goal of reducing litigation expense, ironically electronic discovery costs actually may have increased as a consequence.

For example, while the amended rules are supposed to provide early structure, uniformity and predictability, parties now within the first 120 days of a case must evaluate whether their counsel and their IT teams where they stand in terms of the electronic discovery. And this undertaking can be fairly enormous. The scope of potential electronic discovery is practically limitless. Relevant data may be located on live on networks or on various servers. It also can be found on hard drives, laptops, PDAs, backup tapes and even voicemail messages, and instant messages.

And ascertaining the logistics of eDiscovery a party may intend to produce in a case may help determine the electronic discovery to demand from the opposing party. Clearly, a party should not expect to demand a category of electronic discovery that it is not willing to produce.

Recent history in cases is showing that electronic discovery can be very burdensome and expensive. At times, and perhaps as a result, cases are resolved before the parties, counsel and IT vendors have invested time, effort and expense of carrying out electronic discovery search retrieval and production procedures. By telescoping these processes early in cases by way of the federal amendments, opposing sides in a case have no choice but to move forward with electronic discovery unless a settlement can be achieved relatively immediately.

There have been battles in cases over the appropriate reach of electronic discovery. Courts are called upon to weigh the potential probative value of the information requested versus the burden and expense of production. At times, where appropriate, there can be cost-shifting, such that the party demanding production has to pay the freight of electronic discovery.

Given the broad scope of electronic discovery in some cases, the amended federal rules do allow parties to retrieve inadvertently produced privileged information. The vast amount of data produced in some instances does not allow for perfection in screening out all privileged information in advance of production. Parties need to be very careful not to allow for the deletion or destruction of relevant data once they know of the actuality or potentiality of litigation.

While parties may not be sanctioned when electronic information has been deleted as a result of the good faith, normal data retention policies, once a lawsuit is on the horizon, a litigation hold must be put in place to preserve relevant data. Not surprisingly, electronic discovery has become a growth industry in its own right. Electronic discovery vendors constantly are coming out of the woodwork offering all sorts of "solutions."

Parties need to work actively with their counsel in selecting the best electronic discovery vendors and technology for their cases. Counsel also need to try to reach across the table to establish protocols and agreements with opposing counsel that will help define electronic discovery parameters that are mutually acceptable. For example, counsel can agree on search terms, custodians as to whose records will be searched, and locations to be searched. With proper thought and planning, electronic discovery can become more manageable.

(link)

Transparency When It Comes To Online Security Breaches

January 25, 2011

The hacking of commercial websites can have real world consequences. Case in point: http://www.lush.co.uk

The United Kingdom website for Lush, a cosmetics retailer, voluntarily was shut down after having been hacked recently. According to an announcement posted on the website, ongoing monitoring demonstrated that the site continues to be targeted for further hacking entry attempts.

Thus, in order not to put its customers "at risk," the website will remain closed. Meanwhile, Lush plans to set up an independent website soon that will be able to take orders for Lush products and will accepts payments via PayPal.

Notwithstanding the hacking and subsequent site shut down, Lush has emphasized that orders can be placed in its stores and over the telephone. That is well and good, but of course, Lush would prefer not to have lost the revenue stream from its UK website. Plainly, hacking causes business interruption and decreased revenue flow for companies that are victims of such activities. And one of the reasons for such interruption and decreased revenues is the potential responsibilities owed by companies to their customers.

Companies will be looked to by their customers and possibly by regulators to be transparent in terms of online security breaches and to protect the private data of customers. Indeed, according to Internet legal expert Jonathan Armstrong, the UK has adopted new rules on online advertising and the Office of Fair Trading there recently instituted a campaign on online fairness.

In a best case scenario, hackers will not be successful in penetrating and disrupting websites. But when they do succeed, remedial actions and openness make abundant sense.

(link)

YouPorn Sued For "History-Sniffing"

December 14, 2010

The Internet certainly serves up interesting legal cases. A recent one involves a lawsuit filed against an adult Web site called YouPorn for allegedly running afoul of computer crime and consumer protection laws by virtue of a data collection practice referred to as "history sniffing." Two California residents, in their Los Angeles federal lawsuit, claim that YouPorn, via history sniffing, improperly has been harvesting information about Web sites that the residents and others have visited.

History sniffing, according to published reports, depends on Internet browsers that show Web links in different colors if users have visited the links previously or not. And by implementing certain code within users' Web browsers, a company such as YouPorn can determine if certain sites have been visited. As a result, a profile of sites visited by a particular user can be created without the user's knowledge.

The plaintiffs in the YouPorn case seek class action status on behalf of others similarly situated, damages and injunctive relief.

David Vladeck, the Director of the Federal Trade Commission's bureau of consumer protection, reportedly took issue with the practice of history sniffing in a recent speech, stating that it deliberately bypasses the technique of deleting cookies – the most common technique used by Internet users to thwart tracking of them. Mr. Vladeck reportedly has strongly suggested to Web browser providers that they should come up with technical remedies in this area. Apparently, certain browsers are more vulnerable than others.

As much as people may want to roam free and unwatched on the Internet, the YouPorn case and history sniffing show that we leave our footprints in the digital sand as we move from site to site. If technical measures cannot solve the problem of tracking without consent, greater regulation and increasing lawsuits could follow.

(link)

Valuable Corporate Data Walking Out The Door With Departing Employees

November 30, 2010

Do companies have legitimate concerns that departing employees may take critical corporate information with them when they leave? You bet, according to recent survey statistics. Indeed, as many of 70% of workers revealed that they would have "clear plans to take something with them upon actually leaving," according to a survey of London company employees by Imperva, a data security company.

The survey results demonstrated that 72% of the respondents confessed to having taken corporate information from prior companies. In that context, the most frequent types of materials taken were human resource materials, marketing information, and customer records. Looking forward, as many as 27% intend to take materials containing intellectual property and 17% plan to take customer information. Interestingly, many respondents believe that they "own" the information they have access to, and thus think that they may not be doing anything wrong when they take company data with them.

The survey results also confirm the obvious. Namely, that easy access to information makes walking away with it all the more possible. Of the respondents, 85% maintain corporate information on their mobile devices or home computers, much of which includes customer records and intellectual property.

Very troubling is the survey indication that more than half of the respondents gained access to information that was supposed to be off-limits to them. In fact, 73% reported that access controls are "very easy" to skirt.

Bottom line: companies need to be very proactive to ensure that valuable corporate data – often times the corporate crown jewel – does not leave with departing employees. Protecting corporate data may be easier said than done. Employees need to be educated in terms of what they can and cannot do upon departure, and they need to execute agreements that spell out proper steps to be taken when it comes to protected company data. Companies also need to have appropriate technical measures in place to help ensure that devices and computers of departing employees are wiped clean of corporate information and that the departing employees no longer have access to company networks and systems.

(link)

Down With Spam!

November 23, 2010

Levels of unsolicited commercial email, aka spam, have dropped by a staggering 47% in the past several months, according to statistics assembled by Symantec. This certainly is welcome news, as spam still accounts for 81% of all email traffic on the Internet.

Once upon a time at the dawn of the Internet age, spam frankly was a bigger problem than it is now, as filtering technology was not terribly advanced. Thus, email in boxes were flooded with unwelcome messages.

It was in that context that a number of states enacted their own laws to grapple with the spam problem. Indeed, more than half of the states stepped in to fill the void left by Congress failing to act. Of course, state regulation of spam had its own limitations, given that the Internet does not know state boundaries. When messages are sent to email addresses, it is not known in advance in which states the recipients are located.

Ultimately, Congress did pass the Can-Spam Act of 2003 in an effort to regulate unsolicited commercial email on a national basis and to help achieve some uniformity. But did that stop spam? No! Even with a legal framework in place, offshore and hard to track spammers continued to send their messages with abandon.

So, while the legal solution was not terribly effective in a big picture sense, spam filters were developed and improved to help save the day. As a result of such filters, email in boxes now are not nearly as flooded with spam as they once were. However, filters are not perfect. They can filter out legitimate and desired emails, and they also can fail to trap some spam message. As a result, filtered emails do need to be checked.

So, why have spam levels dropped off significantly in the past several months? It appears that intelligence work has led to the shutting down of major spam-sending botnets. Hopefully, such work will continue and spam levels will continue to decrease.

(link)

Keeping Jurors From Straying Electronically

November 16, 2010

Jurors routinely are admonished by judges only to consider the evidence presented to them at trial and not to consider outside information. How is that working in this electronic age? Not so well. There have been a number of reports of jurors going online to learn about and communicate regarding the cases on which they are serving.

Once upon a time, when jurors were given this admonition, perhaps it was much easier to follow. They readily could understand that they were not to visit the scene of an accident, for example. And even going to visit that location may have been too much trouble anyway. However, these days all types of information is immediately available to jurors fingertips electronically. A simple Google search on a Blackberry can provide all sorts of information about the parties and circumstances of a case within seconds.

We now live in a culture of instant information access and influencing a jury becomes much easier. People are use to electronically searching for and sharing information constantly. Thus, when a judge tells jurors not to consider outside information, while they may not visit the scene of a particular incident, some of them still may have a reflexive instinct to find out more. And their internal motivation may not seem devious to them; they may simply feel that they are given incomplete information at trial, and they want the full context. Of course, what they do not appreciate in that scenario is that the rules of evidence are in place for a reason – to make sure that only reliable and competent evidence is considered.

One option is for judges not only to provide a general admonition against considering outside information; judges also could be more specific in terms of prohibited activities and they could warn of potential sanctions for jurors who engage in these activities. Of course, younger jurors have grown up being told by authority figures how to behave on the Internet, and some of them are accustomed to do what they want anyway. Still, more specificity and the threat of sanctions could get the attention of at least some jurors.

Another option is to have a more active conversation with jurors during voir dire. Rather than simply being told how to behave, and it might be prudent to have jurors respond and actually state in their own words their understanding of what they are and are not to consider as part of their role as the finders of fact in a case. This could help solidify how they should act, and it might be reinforcing to other jurors who hear the words of their juror peers.

And, jurors could have more freedom to submit their questions to the judge at trial. This would allow them to voice any confusion they may have in terms of their conduct along the way, and the judge then could provide ongoing guidance. Also, the jurors' questions might elucidate

areas of the case that truly do need to be covered. The judge then could steer the case in that direction as a matter of proper evidence, and this might prevent jurors from going outside the case to learn more.

These solutions will not prevent all jurors in all cases from conducting their own electronic research. However, these measures could reduce the frequency of such conduct.

(link)

Sex.com - The Value of A Domain Name

October 27, 2010

Sex sells, right? And that is true when it comes to domain names, and in particular the domain name sex.com, which reportedly just sold for $13 million.

Adult content always has been at the monetary forefront of technological advances. Still photography long ago, video recordings later, and online images/action more recently all began with people willing to pay for sexually oriented material.

Domain names obviously are important, in that they draw Internet traffic from search engines to particular Web sites. Domain names that include trademarks are valuable to the trademark holders who hope to benefit from their brand and the goodwill associated with their trademarks. And the Anti-Cyber Squatting Consumer Protection Act allows trademark holders to seek relief from others who improperly include the trademarks of the trademark holders in specific domain names.

And domain names that contain generic terms like "bank" or "loan" also can have tremendous value, if those common terms are frequently used in search engines and bring Internet traffic to domain names that incorporate those terms.

Thus, not surprisingly, the generic and valuable domain name sex.com has had a very interesting history, which has included various legal and financial proceedings. And now the most recent owner of sex.com, Escom LLC, has sold the domain name to Clover Holdings Ltd. for the aforementioned tidy sum of $13 million, according to The Register.

It remains to be seen (if you want to see) what becomes of sex.com and the content that will be posted on the site. The term "sex" reportedly is the most searched term on the Internet, so undoubtedly the domain name will generate tremendous Internet traffic going forward.

(link)

Data Retention And The Ability To Start Over

October 19, 2010

In this electronic age, we leave our digital footprints practically everywhere we go on computers and online. What are the limits to data retention and when should our footprints be wiped clean? This question perhaps raises even more questions instead of a firm answer.

Once upon a time, what we said and how we acted was not recorded in any real way. If we spoke to someone, those words disappeared into the atmosphere after having been uttered. Now, of course, so much speech is conducted electronically, leaving a retrievable record of what was said. Perhaps in certain contexts we might like to know that our previously electronically recorded words might not live on forever, only potentially to haunt us later in life.

For example, teenagers frolicking about on Facebook might prefer to think that later when adults their earlier online exploits and comments will not surface and come back to bite them. Individuals evolve over time, and earlier electronically recorded conduct and statements may no longer truly define who they are later in life.

So, when should electronic information be purged and when should it be retained? In certain regulated industries, there are legal requirements in terms of minimum times for preserving information and online privacy. And when there is the potential or actuality of litigation, relevant information pertaining to the issues in the case must be maintained.

But what about data retention outside of those spheres or beyond required timeframes within those spheres? Some companies err on the side of retaining information, for fear of being accused of destroying relevant case evidence or information required to be maintained as a matter of law. Other companies prefer, when possible, to dispense with information, so that they are not maintaining more information than needed as a matter of burden and expense. Plus, they may not want their entire information history and communications to be searchable later on.

And then there is the issue of whether individual consumers and users should have a choice – can they tell the companies who maintain their information how long they prefer it to be preserved? On top of all of this is the issue that even when there is the intention to dispense with electronic information, often times, as a matter of technological sleuthing, there are ways to recover previously deleted information.

The dialog in this area is only just beginning.

(link)

Social Networks Subject To Discovery

September 28, 2010

As you post communications, photos and videos on Facebook and MySpace, do you ever wonder if social networks are subject to discovery in litigation? Well, you should, as one recent court decision indicates.

In the case of Romano v. Steelcase, a New York judge ruled that defendant Steelcase was entitled in discovery to access the plaintiff's current and historical Facebook and MySpace pages and accounts, including previously deleted information, on the basis that information to be found there could prove to be inconsistent with her claims of injuries and loss of enjoyment of life. The plaintiff alleged in her lawsuit that she fell off a defective Steelcase chair, which led to permanent injuries, pain, loss of enjoyment of life, and multiple surgeries. Steelcase contended that public portions of her Facebook and MySpace pages revealed that she had an active lifestyle, including travel, and it wanted further access to her social networking information, which the plaintiff refused.

The judge agreed with Steelcase. He noted that the plaintiff's public profile page on Facebook showed her smiling happily outside of her home, which was inconsistent with her claim that she was largely confined inside her house in bed. He thus concluded that other parts of her social networking pages might contradict her claims. This may seem a bit harsh. Even someone who is bed-ridden in pain could have a photo taken of him or her outside of the home. On the other hand, that may not be a basis to refuse discovery. It could go more to the weight of the evidence, which could be explained at trial.

The judge also ruled in favor of Steelcase's discovery requests because "the primary purpose" of social networking sites "is to enable people to share information about how they lead their social lives," notwithstanding how they "self-set privacy controls" on such sites. This conclusion was buttressed for the judge by the fact that both Facebook and MySpace state explicitly on their sites that they cannot guarantee the privacy of users' posted content.

So, let there be no mistake, it certainly is possible that communications and materials posted on social networking sites can be fair game for discovery in litigation. Of course, that does not mean that judges always will grant discovery requests in this area. If the relevance of the information sought is too attenuated, then the burden, intrusion, and privacy interests involved might outweigh the probative value of the information. Nevertheless, word to the wise – think twice about what you do or say on social networking sites. Living life out loud can have consequences.

(link)

Potential Jail Time For Electronic Discovery Abuse and Spoliation of Evidence

September 21, 2010

Most of us are aware that electronic discovery abuse and spoliation of evidence can lead to monetary sanctions. But one recent case shows that such failures also can lead to adverse judgments and even potential imprisonment. In *Victor Stanley, Inc. v. Creative Pipe, Inc.*, Chief Magistrate Judge Paul Grimm, of the United States District Court for the District of Maryland, was called upon to resolve the plaintiff's motion for terminating and other sanctions arising out of the defendants' alleged intentional destruction of evidence and other litigation misconduct.

In his memorandum, order, and recommendation to the Court, Magistrate Grimm noted that during four years of discovery, during which time the President of the defendant company actually was aware of the duty to preserve relevant information, the defendants nevertheless "delayed their electronically stored information ('ESI') production; deleted, destroyed, and otherwise failed to preserve evidence; and repeatedly misrepresented the completeness of their discovery production to opposing counsel and the Court." As a result, "substantial amounts of the lost evidence cannot be reconstructed." Indeed, the plaintiff identified "eight discreet preservation failures." The plaintiff contended that the defendants did not provide certain categories of discovery notwithstanding numerous prior court orders to do so.

The defendants did not disagree with, and actually agreed that the majority of the plaintiff's assertions were true. They also stated their willingness to abide by the entry of a default judgment against them on the primary cause of action against them for copyright infringement. Magistrate Grimm remarked that the fact that the defendants would willingly accept a default judgment for failure to preserve ESI in the primary claim filed against them speaks volumes about their own expectations with respect to what the unrebutted record shows of the magnitude of their misconduct, and the state of mind that must accompany it in order to sustain sanctions of that severity.

In addition to his recommendation to the court to grant this default judgment, Magistrate Grimm concluded that the defendant President's pervasive and willful violation of serial Court orders to preserve and produce ESI evidence be treated as contempt of court, and that he be imprisoned for a period of not to exceed two years, unless and until he pays to Plaintiff the attorney's fees and costs that will be awarded to the Plaintiff as the prevailing party. Magistrate Grimm reflected that imposing contempt sanctions particularly including a sentence of imprisonment, is an extreme sanction, but this is an extreme case. He went on to say that for such clearly contemptuous behavior, a very serious sanction is required.

Magistrate Grimm pointed out that there would be further proceedings to determine that amount of attorney's fees and costs owing to the plaintiff and that this should total a significant figure. Notwithstanding the foregoing ruling of civil contempt, Magistrate Grimm was clear that the defendant President can avoid imprisonment by promptly paying the fees and costs that are determined, and that the commencement of any confinement will be set when the amount of attorney fees and costs are determined.

Magistrate Grimm stressed that the potential for imprisonment is absolutely essential as a civil contempt sanction because, without it, I am convinced that [the defendant President] will do all that he can to avoid paying any money judgment or award of attorney's fees that is in the form of a civil judgment alone. He went on, without the threat of jail time, [the defendant Presidents] future conduct would be predicated by his past, and Plaintiff will receive a paper judgment that does not enable it to recover its considerable out-of-pocket losses caused by [the defendant President] spoliation.

This case, while involving repeated and egregious failures to comply with discovery and evidence preservation obligations (in addition to spoilation of evidence), makes universally plain that getting it right up-front in the discovery process is essential. Anything less causes greater expense in the long-run, and can lead to monetary sanctions, issue preclusion and adverse judgments, and even the potential for imprisonment in very extreme cases. Companies should work pro-actively internally, with their outside counsel who are skilled in this area, and appropriate vendors to do the right thing!

(link)

Facebook Places: Where You Want To Be?

August 24, 2010

Facebook has just brought to the fore its new service called Facebook Places that allows users to alert others to their physical location and that ultimately seeks to enable Facebook to draw upon local business advertisers. And as Facebook moves forward with Places, it has been confronted with concerns expressed by privacy advocates.

Facebook Places, in some ways similar to other location-based social networks, enables Facebook members to check in via mobile devices and announce their physical location to friends. Using Places, they will be able to ascertain if any of their friends are in the same geographic vicinity. They further will be able to discern whether others, who have broadcast their location, also have checked in at the same place.

And there is more. Friends who are physically with users can be tagged. Plus, Places will provide ideas as to other close by locations that might interest users. Places will broadcast check-ins via periodic status updates.

While Places may provide yet one more feature of interest to users, plainly Facebook hopes that Places will help the company gain advertising revenue from local businesses in specific locations.

Of course, as things seemingly go with Facebook, with each step forward comes a new round of criticism from privacy advocates. Indeed, swiftly on the heels of Facebook's announcement of Places, the ACLU has leveled some specific privacy concerns.

The first primary concern expressed by the ACLU is that "no" is not a true option when it comes to Places. While Places permits friends to tag someone when they check in from a location, and while Facebook makes it simple to say "yes" to allow friends to check in for someone else, when dealing with potentially declining that feature, the only option provided is "not now" (a deferral) instead of "no," according to the ACLU.

The next major concern raised by the ACLU has to do with the "Here Now" feature of Places that provides a list of people who for a given location have checked in recently. According to the ACLU, while Facebook makes it simple to inform others of someone's location, there is limited power to control who actually knows of an individual's location.

Of course, dialogue is helpful. To the extent legitimate privacy concerns are raised as Places becomes more fully understood, hopefully Facebook will listen and implement measures best

designed to alleviate privacy concerns while still maintaining the potential benefits to users of Places.

(link)

Major Software Systems: Heaven or Hell?

August 3, 2010

These days, major software systems make the world go around. Software is used to assist every day mundane functions. Software also is the backbone behind mission critical systems that ensure the health and safety of our society. But does that mean that software always is procured and supplied without controversy and disputes? Absolutely not.

Unfortunately, fights and litigation between major software providers and recipients is all too common. Why does this happen? There are a variety of reasons, and there are ways to avoid such problems on the front-end of software relationships, if due care is taken.

One problem that can occur on the software provider side is that of over-promising. There are instances when providers desperately want to get into a particular software niche or they mightily want to land a specific engagement. In this context, they may over-hype their expertise, prior experience and ability to deliver under the given software scope. Indeed, they may even start to believe their own over-hyping. While that may land the engagement on the front-end, once problems emerge, the software buyer will complain about unfulfilled promises. In fact, the buyer may even argue that the provider engaged in deception and fraud.

On the procuring side, at times software buyers are not sufficiently specific in terms of their precise needs, they keep making change requests to the scope of the software project along the way, and they may not provide sufficient information and assistance to the software provider to enable the provider to do its best on the project.

And, perhaps not surprisingly, there can be a number of disputes and issues that arise from contractual documentation. Software buyers may find that they are limited by contractual terms as far as their potential remedies in the event they encounter software problems. When that happens, they may need to prove fraud to get out from under the contractual limitations. Software providers, on the other hand, may find that contractual representations they make in terms of software capabilities may come back to bite them if those representations are not achieved.

While both sides may be well motivated when a major software project is coming together at the outset, they should not jump into bed together in haste before truly vetting out relevant details relating to the project. Both sides should be careful and frank in terms of what they want and what they can do realistically as part of the project. And then the contractual documentation should be worked out to truly capture the accurate nature of the envisioned relationship on the software project. Plainly, appropriate technical and legal support should be

brought to bear in properly formulating the relationship. It is not a good idea to be penny-wise and pound-foolish when crystallizing the parameters of a major software project.

(link)

State Sales Taxes For Online Sales?

July 13, 2010

A new effort is being made in Congress to impose state sales taxes on online sales. H.R. 5660, aka the Main Street Fairness Act, was introduced earlier this month by Rep. Bill Delahunt (D. MA.). The bill, if it were to become law, would authorize the collection of state taxes on Internet sales, even if a given Internet seller does not have a physical presence with a specific taxing state.

The bill says that "as a matter of economic policy and basic fairness, similar sales transactions should be treated equally, without regard to the manner in which sales are transacted, whether in person, through the mail, over the telephone, on the Internet, or by other means."

This bill goes on to provide that "States that voluntarily and adequately simplify their tax systems should be authorized to correct the present inequities in taxation through requiring sellers to collect taxes on sales of goods or services delivered in-state, without regard to the location of the seller."

The bill would allow those states that sign onto the Streamlined Sales and Use Tax Agreement to impose sales taxes on Internet sellers. This agreement already has been endorsed by a number of states.

While apparently some believe that online sellers currently have a commercial advantage when it comes to not having to pay state sales taxes when selling to customers where the online sellers do not have a physical presence, there has been a backlash to the Main Street Fairness Act, as occurred successfully to prior Congressional efforts to impose taxes on online sales.

Not surprisingly, the Computer and Communications Industry Association (CCIA) and some notable technology companies have expressed opposition to the bill. The argument is that in this poor economy, it would not be wise to saddle online sellers with sales taxes, especially, when the burden would be higher for such sellers than for traditional sellers, as the online sellers would need to obtain expensive professional help to sort through and comply with the rules of a number of different taxing authorities.

Of course, arguments on the other side include the need to raise revenue for taxing authorities for the benefit of the states they serve and the fairness notion set forth in the bill itself. The bill is supported by various retail and government associations.

Time will tell whether this taxing effort will gain traction when prior attempts did not succeed.

(link)

Requesting Greater Facebook Privacy Protection

June 22, 2010

Facebook has been in the press recently in terms of perceived privacy problems and apparent attempts by Facebook to try do better in terms of privacy protection. While Facebook may be trying to improve, various public interest groups do not believe that Facebook has done enough, as evidenced by a recent open letter by the groups to Facebook CEO Mark Zuckerberg.

The letter, sent on behalf of the ACLU Northern California, the Center for Democracy and Technology, the Center for Digital Democracy, Consumer Action, Consumer Watchdog, the Electronic Frontier Foundation, the Electronic Privacy Information Center, PrivacyActivism, Privacy Lives and Privacy Rights Clearinghouse, while conciliatory in tone, demands certain improvements.

The letter begins by stating while the groups are "glad" that Facebook has "taken steps in the past weeks to address some of its outstanding privacy problems," they nevertheless "urge" Facebook "to continue to demonstrate [its] commitment to the principle of giving users control over how and with whom they share" by taking certain additional steps.

Specifically, the groups ask Facebook to: a) fix the "app gap" by enabling users to decide precisely which applications can access their personal information; b) make "instant personalization" opt-in by default; c) not retain data about specific visitors to third-party sites that incorporate "social plugins" or the "like" button unless the site visitors decide to interact with those tools; d) give users control over every piece of information they share through Facebook, specifically including their names, genders, profile pictures, and networks; e) safeguard users from other threats by using an HTTPS connection for all interactions by default; and f) provide users with simple tools for exporting their uploaded content and details of their social network such that users who are not content with Facebook's policies and desire to leave for another social network do not have to decide between protecting their privacy and staying connected with their friends.

The groups state that "'privacy' and 'social' go hand in hand." Namely, "users are much more social with people they know and choose and much less social when their actions and beliefs and connections are disclosed without their control or consent."

The groups express an interest in continuing the privacy dialogue with Facebook so that users can be both social and private on Facebook. Indeed, the open letter to Mr. Zuckerberg ends with the request to make the default on Facebook "social-and private."

It will be interesting to see how this unfolds. While the tone of the open letter is conciliatory, if Facebook does not provide further privacy protection comfort, the next step could be sharp accusations by the groups, and ultimately privacy litigation could follow.

(link)

Watch Out - The Digital Universe Is Huge And Growing Fast

June 8, 2010

If you are thinking that the digital universe that comprises all electronically stored data already is gargantuan, well, fasten your seat belt, because this universe is expanding rapidly.

According to IDC, a research and consulting firm, last year, notwithstanding the global recession, the digital universe expanded 62% to 800,000 petabytes. What is a petabyte? A petabyte constitutes a million gigabytes, and is represented by a tower of DVDs going from earth to the moon and back, according to IDC.

And IDC says that this year the digital universe will expand almost as rapidly to 1.2 million petabytes, aka 1.2 zettabytes. With continued expansion, IDC forecasts that the digital universe in 2020 will be 44 times as large as it was in 2009.

With the tremendous growth in the digital universe come practical concerns and considerations. For example, there could be challenges in terms of searching for and retrieving needed data. Because most of the digital universe is unstructured data like images and voice packets, IDC suggests that new methods to add structure to unstructured data, to analyze the inside of information containers and to recognize content (like a person's face shown in a security video) will need to be developed and implemented.

In addition, there will be issues relating to how to manage, store and delete vast quantities of information. This, of course, is an issue we are dealing with already.

Furthermore, the challenges relating to compliance with governmental regulations and industry rules as respects maintaining privacy, tracking transactions and retaining records could increase along with the size of the digital universe. IDC notes that regulation compliance was a $46 billion industry last year alone.

On top of all of this, as the digital universe grows, so does the portion of that universe that requires secure protection. Indeed, according to IDC, the amount of sensitive data that is not protected but that needs protection is growing at even faster rate than the entire digital universe.

Perhaps the most sobering statistic of all is that while the digital universe is projected to grow by a factor of 44 by the year 2020, the number of IT professionals in the world is expected to grow by only a factor of 1.4 during the same time period, according to IDC.

So, to meet the coming challenges, those dedicated to the tasks will have to be smart, creative and ahead of the tsunami of information to enter the digital universe (to mix metaphors).

(link)

LimeWire Lawsuit: The Day That Free Music and Music File Sharing Died?

June 1, 2010

LimeWire, a software application that allows for free music and music file sharing over the Internet, has suffered a recent and significant judicial defeat in at the hands of 13 major record companies. The LimeWire lawsuit indicates that record companies will not back off from fighting against free music downloads.

Some years ago, the record companies filed a lawsuit in federal court in New York against certain companies and individuals while asserting a variety of federal and state law claims for their alleged role in the distribution of LimeWire. The complaint alleged that LimeWire users utilize LimeWire to obtain and share unauthorized copies of the record companies' sound recordings, and that the defendants facilitated this infringement by distributing and maintaining LimeWire. After several years of litigation, the parties filed motions for motions for summary judgment to adjudicate some claims prior to trial.

While the court denied some of the motions, holding the issues raised in those motions over to trial, the court did grant the record companies' motions on claims of inducement of copyright infringement, common law copyright infringement, and unfair competition. The granting of those motions, obviously, is not good news for LimeWire.

In reaching its decision, the court provided some background on LimeWire, first noting that LimeWire was founded in 2000 and that year released LimeWire as a file-sharing program that utilizes peer-to-peer (P2P) technology on the Gnutella network. The court recognized that LimeWire users can share practically all files stored on their computers with other LimeWire users, and that when a LimeWire user wishes to locate digital files on the network, he simply enters search information into the search function on the LimeWire user interface.

At that point, as the court understood, LimeWire scans the computers of other LimeWire users to find files that meet the search query. Then, as the court noted, the LimeWire user can download any files that LimeWire comes up with. Finally, when the user downloads a file, LimeWire transfers a digital copy of the file from the computer from where it is located to the LimeWire user's computer.

The problem is that of the millions of files transferred in this way by LimeWire, thirty are sound recordings as to which the record companies own copyrights or exclusive rights and that are at issue in the lawsuit. The record companies claim that LimeWire users share and download

unauthorized digital copies of these thirty recordings over LimeWire, and that the defendants are secondarily liable for this infringement because they maintain and distribute LimeWire.

In reaching the conclusion of inducement of copyright infringement, the court found evidence that LimeWire users do infringe on the copyrights of the record companies by sharing unauthorized digital copies of the subject recordings via LimeWire, and that the evidence established that defendant LimeWire LLC (LW) intentionally encouraged direct infringement by LimeWire users. Factors showing encouragement of infringement included: LW's awareness of substantial infringement by users, LW's efforts to attract infringing users, LW's efforts to enable and assist users to commit infringement, LW's dependence on infringing use for the success of its business, and LW's failure to mitigate infringing activities.

And because the court already found that LimeWire users infringe the copyrights of the record companies and that LW has engaged in purposeful conduct intended to foster that infringement, the court also granted summary judgment of the record companies on their claims for common law copyright infringement and unfair competition.

What's next? The remaining claims as to which summary judgment was not granted will still proceed in litigation toward trial. However, with the granting of certain summary judgment motions in their favor, the record companies possibly could seek injunctive relief to stop LimeWire from continuing as it has up until now. Also, the record companies invariably at the appropriate time in the litigation will seek their damages, which could be substantial.

LimeWire plainly does not like this judicial tune.

(link)

Sexy Texts and Privacy

May 25, 2010

We now live in an online world where words like "tweeting" and "defriending" are the new coin of the vocabulary realm. How about sexy texts also known as "sexting"? What is the importance of personal sexy texts and privacy?

Indeed, sexting, the practice of people texting nude photos of themselves, has raised recent legal privacy concerns. The primary question at stake is whether high school students have a privacy right to nude images that have been sexted and are located on their cell phones.

The ACLU and a private law firm have been seeking to establish this privacy point in legal proceedings in Pennsylvania. They argue that while school officials under certain circumstances can confiscate the cell phones of students, they cannot invade privacy by looking at the content of what is contained on the cell phones. They emphasize that cell phones now are repositories of some of the most private data of individuals, including text messages, contact lists, photos and even videos. As a result, cell phones should not be searched absent "reasonable suspicion."

In terms of background, the lawsuit involves a female student who has launched a constitutional attack based on the taking of her cell phone by high school officials, the viewing of nude images of herself on the phone, and the provision of the phone to prosecutors. In a previous case, several students at the same school obtained injunctive relief preventing them from being prosecuted for child pornography based on nude photos contained in their cell phones.

In the current case, the female student argues that the nude photos on her phone were only intended for viewing by herself and possibly her boyfriend and that they should not have been looked at by school officials and prosecutors. As a result of their review, the student apparently was informed that she could avoid prosecution if she participated in a course on violence and victimization. The student did agree to take the course, but by her lawsuit, she obviously believes that her constitutional rights were violated.

It is true that very personal and even intimate information can be contained on hand held devices like cell phones. This may be particularly true for young people, as they seem to live their lives through their gadgets. Is it reasonable to expect that materials contained on cell phones are entitled to a reasonable expectation of privacy? Perhaps that depends on the person involved. One person may make best efforts to ensure that others do not view the content on her phone, including requiring a secret password to open usable access to the phone. Another person may leave her cell phone around without password protection for almost anyone to view its contents.

Of course, at the end of the day, some care and education should be provided to the young in terms of how they use their electronic devices and what they store on those devices. If someone does not want to have nude images of their body viewed by others, it may be prudent not to have those images contained on a cell phone that could be potentially viewed by others. Still, there certainly is an argument that the contents of the cell phone of someone else should not be viewed by others absent some sort of compelling and substantial reason.

(link)

Risky Online Places To Be

May 11, 2010

The Internet crosses geographic boundaries, right? Correct. So, online risks are the same no matter where you are located, right? Wrong! According to a recent study, Internet risks indeed vary depending on where you go online, and ten U.S. cities have been deemed the riskiest. They are, risky online places to be.

The survey, by Norton from Symantec, considered various risk factors in coming up with its results, including cybercrimes such malicious attacks, malware infections, spam zombies, and bot-infected computers, as well as additional factors like wireless hotspots, broadband connectivity and online purchases.

Interestingly, the top four risky cities to be online in the U.S., Seattle, Boston, Washington, D.C., and San Francisco, are some of the most advanced technological areas in our country.

Seattle was the most risky city by a wide margin, and it is the only city to score within the top ten of each risk category in the study. Seattle was second overall in terms of risky user behavior and WiFi hotspots.

Boston came in second for overall online risk principally because of its high levels of cybercrimes (fifth), risky behavior (fourth) and WiFi availability.

Washington, D.C., ranked third overall for online risk, with high risk scores across most categories, and was fourth in cybercrimes and fifth in WiFi hotspots. D.C. residents also are very active online purchasers.

San Francisco, a high-tech U.S. Mecca, ranks fourth overall for online risk, and came in first for risky behavior and WiFi hotspots. The relatively low number of cybercrimes is what has kept San Francisco from being the riskiest online U.S. city.

Rounding out the top ten U.S. cities for online risk are Raleigh, Atlanta, Minneapolis, Denver, Austin and Portland (OR).

Of the 50 cities considered as part of the study, the safest online cities overall, in order, are Detroit, El Paso, Memphis, Fresno, Fort Worth, Long Beach, Tucson, Cleveland, Milwaukee, and San Antonio.

While this survey and its findings are interesting in a macro sense, the risk to a particular Internet user depends very much on the specific practices of that person while online.

(link)

The Cost of Data Breaches: It Ain't Cheap!

April 27, 2010

What has been suspected now has been confirmed - the cost of data breaches is substantial. Indeed, a report titled "2009 Annual Study: Global Cost of Data Breach" shines a very bright light on the actual cost of activities stemming from more than 100 breach incidents across multiple industry sectors, numerous organizations, and a handful of different countries. The average global total cost of each data breach in 2009 was $3.43 million, with an average cost of $142 per affected record. And here in the United States, the average total cost per breach was a staggering $6.75 million, with an average cost of $204 per affected record.

The report compiled by the Ponemon Institute and sponsored by PGP Corporation, analyzed average costs of data breaches in Australia, France, Germany, the United Kingdom and the United States. Perhaps not surprisingly, the costs were highest where data breach notification laws place requirements on organizations that experience a breach to disclose the details of breach incidents. Accordingly, the costs were the highest in the United States, where practically all states at this point have passed data breach legislation. And Germany, where similar laws were placed last year, experienced the second-highest costs. In terms of the average total costs per breach and the average cost per affected record, the numbers were as follows: Australia $1.83 million/$114; France $2.53 million/$119; Germany $3.44 million/$177; the United Kingdom $2.57 million/$98; and the United States $6.75 million/$204. As other countries pass data breach laws, associated costs likely will spike in those locations.

In a wake-up call to companies, on average 44% of incurred data loss expenses related to lost business. When customers learn of data breaches, they evidently take their business elsewhere. This should encourage companies to do their very best in preventing and addressing breaches. With respect to the percentage of data loss expenses relating to lost business, the numbers come in like this: Australia 33%; France 30%; Germany 34%; the United Kingdom 46%; and the United States a whopping 66%.

The report also demonstrates that when third-party and/or criminal attacks caused breaches, costs increased due to added forensics and investigations that were launched. The report further details that when there is a strong Chief Information Security Officer (CISO) who took active responsibility for managing a breach, costs were lower across the board in all five countries that were studied.

Data security breaches plainly can affect that bottom line for an organization, no matter the country, even if the costs are higher in some countries than others. It behooves organizations to get their data houses in order on the front-end, and when a breach happens notwithstanding

best preventative efforts, the breach should be managed swiftly and effectively by a strong CISO with the assistance of legal counsel skilled in this area.

(link)

Supreme Court To Rule on Privacy of Text Messages

April 20, 2010

The United States Supreme Court currently is considering a case involving the potential privacy of text messages sent and received on employer-provided equipment by employees. While the context is that of a governmental employee, it is possible the Court's ultimate ruling could have implications for employees and employers in the private sector as well.

In City of Ontario v. Quon, the issue presented is whether a police SWAT team member had a reasonable expectation of privacy under the Fourth Amendment with respect to text messages sent and received on his work-issued pager.

The City of Ontario had a written policy that had been signed by the SWAT team member, which provided that employees should not expect privacy in their communications using equipment provided by the City. While the policy did afford limited personal use, the City stated that it could monitor all network activity.

The SWAT team member, along with others, was provided with a pager by the City. They were informed by supervisors that the text messages on the pagers were tantamount to emails and were thus governed by the City's written policy. In essence, there was no privacy of text messages. Or so the City thought.

When the SWAT team member repeatedly exceeded the character limit on his pager, he was told by a supervisor to pay for the overages but that he would not be audited to determine if the text messages were work-related.

As it turns out, the SWAT team member had used the pager to send and receive many personal messages, some of which apparently were sexual in nature.

After the character limit continued to be exceeded, the police chief commanded a review of the messages to determine if the operative character limit was sufficient. This review led to the conclusion that the vast majority of the SWAT team member's messages were personal. He, therefore, was written up for not complying with the City's written policy.

The SWAT team member filed a federal lawsuit, claiming that his Fourth Amendment privacy rights were violated by the review of the text messages.

The trial court concluded that the SWAT team member had a reasonable expectation of privacy in the messages and tasked the jury with the question of whether the City's conduct in reviewing the messages in turn could be considered reasonable on the facts of the case. The jury sided with the City, finding that there was a proper purpose in ascertaining the sufficiency of the character limit.

The SWAT team member filed an appeal. The federal appellate court reversed on the ground that the search in this context was unreasonable as excessively intrusive.

The United States Supreme Court has competing arguments to consider. On the one side, the argument is made that the City's written policy is clear in warning of no expectations of privacy with respect to communications on employer-provided equipment and that that policy cannot be abrogated by the informal statements of a particular supervisor.

On the other side, there is the argument that the written policy was never formally updated to include text messages from pagers within its ambit, and that the SWAT team member had a reasonable expectation of privacy; especially given what he was told by the supervisor.

It will be interesting to see how the Supreme Court rules in this case. The Supreme Court could paint with a broad brush beyond the facts of this case to provide guidance not only in the government employee setting, but also as relates to private employer-employee arrangements.

However, this could be difficult, as what constitutes a reasonable expectation of privacy in one factual context, whether in the governmental or private sector, can vary under myriad other factual circumstances.

Indeed, while there has been recognition that employers in the private sector have wide latitude in monitoring electronic communications of employees when advance notice has been provided, over time, courts have been finding exceptions to that general rule.

Stay tuned.

(link)

How Private Are Personal Emails Sent Via Employer Computers?

April 6, 2010

In this day and age, practically everyone communicates electronically often and for a multitude of reasons. This of course, is true in the workplace. While employees communicate by email for work-related reasons, it is not uncommon for them also to send emails relating to personal matters.

Employers frequently put in place and have employees execute employee email privacy policies. These policies provide that emails sent and received by employees on computer equipment provided by employers are not private and are subject to proper employer review.

But does that always hold true? Not necessarily, at least according to the New Jersey Supreme Court based upon the facts of one particular recent case.

In the case of Stengart v. Loving Care Agency, Inc., the New Jersey Supreme Court was called upon to answer the unique question as to whether an employee could expect privacy and confidentiality in emails between herself and her attorney that were sent and received through her personal, password-protected, email account while using a laptop computer provided by her employer for company business. From the laptop, the employee could send emails from her company email account. She also could access the Internet from the employer's server. The employee was not aware that the browser software automatically saved a copy of each Web page she viewed on the laptop's hard drive in a cache folder of temporary Internet files.

The employee ultimately used the laptop to access a personal, password-protected email account on the Yahoo Web site. Through that account, she communicated with her attorney about issues she was having related to her employment. She did not save her Yahoo identification or password on the laptop. When she ceased her employment, she returned the laptop to the employer. She then filed an employment discrimination complaint against the employer based on the issues she felt that she had encountered at work.

As part of the litigation and in anticipation of discovery, the employer hired experts to create a forensic image of the laptop's hard drive; including the temporary Internet files. Those files contained the contents of certain emails that the employee had exchanged with her attorney using her Yahoo account. At the tail-end of the emails sent by the lawyer, there was language that stated that the information in the emails "is intended only for the personal and confidential

use of the designated recipient" and that the emails may constitute "privileged and confidential" attorney-client communications.

The employer took the position in the litigation that the emails were fair game because the former employee had no reasonable expectation of privacy in files on a company-owned computer, especially based on the employer's electronics communications policy. That policy stated that the employer could review, access and disclose "all matters on the company's media systems and services at any time." The policy also provided that emails, Internet communications and computer files are deemed company business records and "are not to be considered private or personal" to employees. However, the policy also stated that "occasional personal use is permitted."

At the end of the day and based on the facts of this specific case, the New Jersey Supreme Court held that the employee could reasonably expect that her emails with her attorney through her personal, password-protected Yahoo account should remain private; and that just because she used a company laptop did not undermine that privacy expectation and the attorney-client privilege.

The Court reached this conclusion for various reasons, including the following: 1) the employer's policy did not specifically state that emails exchanged on personal, password-protected email accounts would be subject to monitoring if employer equipment were used; 2) the reference to review of matters on the employer's "media systems and services" was too vague; 3) the policy did not provide notice that the contents of personal emails stored on hard drives might be forensically retrieved and read; 4) while stating that emails "are not to be considered private or personal," the policy at the same time allowed "occasional personal use of email"; and 5) the lawyer's emails contained language stating that they were personal, confidential and possibly attorney-client communications.

The Court was clear in stating that "whether an employee has a reasonable expectation of privacy in a particular work setting must be addressed on a case-by-case basis." Here, the Court did not believe that a reasonable person in the employee's position would expect that her employer "would be watching over her shoulder as she opened emails from her lawyer on her personal, password-protected Yahoo account." The Court went on to note that while employers can enforce computer use polices "to protect the assets and productivity of a business, . . . they have no basis to read the contents of personal, privileged, attorney-client communications."

Indeed according to the New Jersey Supreme Court, even "a policy that provided unambiguous notice that an employer could retrieve and read an employee's attorney-client communications, if accessed on a personal password-protected email account using the company's computer system, would not be enforceable."

So what are the take home messages from this case? For employers, they must be as explicit and specific as possible in terms of providing notice in their policies to employees as to how they may monitor the employee's electronic communications and the level of privacy. Hardly any employees can expect full privacy in their communications. However according to the New Jersey Supreme Court, notwithstanding all of the clear notice in the world, some monitoring still may not be permissible.

As far as employees, they should read and understand their employers' computer use policies. They should recognize that they indeed may have very little privacy in their electronic communications sent and received using employer computer equipment. When in doubt, they should send personal communications from their own personal equipment using their own private accounts. Of course, that is easier said than done. Employees spend long hours at work and on portable work equipment, and they may not always remember to separate their work and private lives – and some courts may, and some courts may not, find that to be reasonable on the facts of given cases.

(link)

It is Time To Address Data Breaches In Colleges And Universities

March 30, 2010

If you feel like you have been hearing quite a bit about data breaches in colleges and universities, there is a reason. Institutions from the educational sector reported more breaches than any other sector for the recent period of September 2008 to March 2009, according to the Privacy Rights Clearinghouse. Indeed, colleges and universities reported four times the number of breaches than the institutions within the health care sector; the sector that reported the second most data security breaches.

It certainly is laudable that educational institutions seem to take their data security breach notification responsibilities seriously, but it is imperative that they learn to avoid so many breaches in the first place. This is especially true given that colleges and universities collect personal and highly sensitive data not only from students, but also from faculty, personnel, applicants, alumni, business partners and others. This information often includes private financial, health, academic, demographic and other details.

Many of the data security incidents of educational institutions result from the loss or theft of equipment and errors leading to unauthorized access. Steps can and should be taken to safeguard equipment and access.

For those colleges that have not done so already, they really ought to have a Chief Privacy/Security Officer in place who provides overall guidance and direction. An analysis of how and where an educational institution collects, maintains, and distributes private information should be conducted. A privacy and security policy should be developed and followed by the institution.

In going about this process, colleges and universities should consult with legal counsel who are knowledgeable and skilled in this area. This is true for many reasons including the fact that many federal and state laws come into play in terms data requirements. These laws include state breach notice laws, the Gramm-Leach-Bliley Act, the Health Insurance Portability and Accountability Act, data security laws requiring encryption under certain circumstances, and other laws.

Hopefully as time goes on and as educational institutions get it right, we will hear less and less about data security breaches in this important sector.

(link)

Safety In the Cloud

February 9, 2010

The cloud computing technology currently available is carrying us into the future in terms of the remote off-site handling and storage of our data. But are we safe in the cloud? Is our private data secure? Good questions

According to a recent survey commissioned by Microsoft, while 58% of the general population and 86% of senior business leaders are excited with respect to the prospect of the cloud computing technology now available, more than 90% of them are worried about the security, privacy and access of their cloud data. The survey also revealed that the majority of respondents would like the federal government to create laws, rules and policies specifically governing cloud computing.

Following up on these results, Brad Smith, Vice President and General Counsel for Microsoft, has called for a "national conversation" designed to create confidence in cloud computing and he has proposed a Cloud Computing Advancement Act to address cloud privacy and security.

Features of the proposed legislation would include:

- Enhanced privacy protection and data access rules to protect privacy, while specifically strengthening the Electronic Communications Privacy Act;
- Updating the Computer Fraud and Abuse Act to give law enforcement officials the tools they need to pursue hackers and to deter Internet crimes;
- The adoption of truth-in-cloud-computing principles to allow consumers and businesses to understand how information will be accessed, used and protected by service providers; and
- Efforts to create a grapple with cloud computing data protection issues on a global basis.

Frankly, some of the laws on the books, like the flexible Computer Fraud and Abuse Act, already can be triggered to provide legal protection and recourse in the relatively new cloud computing era. And while Microsoft may be trying to get out front of the issue to generate favorable PR for its own business practices, that is not a bad thing.

There certainly is no harm in generating a "national conversation" about cloud computing and the protection of data in the cloud. Whether any of the proposals by Mr. Smith of Microsoft actually gain traction remains to be seen. But the conversation could lead to some goods ideas that ultimately are worthy of implementation.

(link)

Will Getting Rid of Free Online Content Save The Newspaper Industry?

January 20, 2010

The days of reading a daily newspaper appear to be part of the past, and newspapers are trying to come up with solutions to remain viable. With online content available on the internet, less people are reading printed newspapers. Free online content is available, but will charging readers for online content save the newspaper industry? The answer, unfortunately for now, appears to be "no," according to a recent poll.

An Adwork Media/Harris Poll of last month indicates that while 64% of Americans aged 55 and above still read a daily newspaper practically every day, the percentages of readership go down with age. Indeed, 44% of Americans aged 45-54, 36% aged 35-44, and only 23% aged 18-34 read a daily newspaper most days. And 17% of Americans aged 18-34 never read a daily newspaper.

These readership percentages obviously are not good news for the newspaper industry. So, what is to be done to solve the problem and to try to increase revenue?
One option would be for newspapers to charge a monthly fee for readers to gain access to online content. But here again, there is bad news, as revealed by the poll.

In fact, 77% of online adults report that they would not be interested in paying anything to gain newspaper content over the Internet. And even though some may be willing to pay, 19% of online adults only would be willing to pay between $1 and $10 per month, with only 5% saying that they might pay more than $10 per month.

Perhaps because online readers are used to free online content; they have come to expect that, especially while it is currently available. Back in the Napster days, there was a prevailing view among some that online music should be free for download. Now of course, Apple is making a fortune as people purchase songs from iTunes.

So, it is possible that the game later could change in terms of pay-for-play with online newspaper content. But, at least for now, newspapers cannot count on that future revenue stream, and they need to come up with other ways to survive.

(link)

Social Networking While At Work: Networking Comes of Age

January 12, 2010

Once upon a time, and actually not that long ago, online social networking truly was the province of high school and college students. Those days are over, and whether the youth likes it or not, older generations now are rampant on Facebook, Twitter, MySpace and other social networking sites like LinkedIn; who manage online social networking while they carry on other daily tasks.

The demand for online social networking has become so ubiquitous that a recent reported outage of severe Internet controls in China was greeted with enthusiasm as usually blocked socially networking platforms briefly opened up. While social networking does present a number of potential benefits, care must be taken that proper practices are followed, especially in the workplace.

Companies initially were reluctant to allow employees to engage in online social networking while at work. The concern was that they would not pay attention to their work functions, and as a consequence, their productivity would suffer. However, more recently, companies are "getting it"; understanding that social networking can be a valuable business tool.

Business owners and managers now recognize that social networking sites can provide an excellent launching pad to expand potential business contacts. Even a small business can focus on an audience of thousands of people with little investment or burden. Ultimately, major but inexpensive marketing campaigns can be initiated and promoted via social networking while companies can save on money.

Furthermore, targeted groups and individuals can be "touched" a bit more personally through socially networking. Indeed, businesses can foster connections between their customers, essentially creating their own fan base. You can see this when you search major companies on Facebook; many of them have their own fan page.

In addition, companies can position themselves as "ahead of the curve" with new ideas by way of social networking, thus enhancing their reputations. Social networking is a very effective way to disseminate information about new products and programs.

Even with all of these potential benefits coming into the consciousness of business leaders, valid concerns remain in terms of how social networking practices are integrated into the business world.

Employers still are concerned that if their employees spend time on social networking sites during the work day, they will do so at least in large part for purely personal purposes, and not while advancing business objectives. Perhaps to a lesser extent, companies may encounter bandwidth issues, as videos and other large files are posted and retrieved on social networking sites by employees.

Business owners also must be vigilant to make sure that employees do not inappropriately disparage or defame others (or the company, for that matter), and that they do not inadvertently or purposely disclose company intellectual property or trade secrets. Companies need to take care that employees do not fall victim to scams or cybercrime perpetrated through social networking sites.

For some companies, the solution still might be to ban social networking by employees. But as time goes on, the movement probably will be even further in the other direction. Thus, it is imperative that companies educate their employees as to the policies and practices that must be followed.

Not only should employers take technological steps such as updating anti-virus software on a regular basis and putting appropriate firewalls in place, they need to tell their employees specifically the types of social networking communications that are permissible and those that are not. Employees should be told which social networking sites can be used, the parameters in terms of content of communications, the allowed intended audience(s), and other related details. Employees also need to be informed that their work-related social networking will be monitored by the employer.

Companies should work with IT and legal professionals to come up with specific social networking policies for employees. Employees, in turn, should be given a written copy of the policies, and they should provide their written agreement to follow the policies.

Plainly, as social networking evolves, and as the nature of a given business changes over time, social networking policies will need to be revised and updated.

Fasten your seatbelts; welcome to the social networking future; full speed ahead.

(link)

The Decade of Technology Convergence

January 5, 2010

I have been writing weekly on technology issues the entirety of the past decade - and what a decade it has been! Technology convergence has been fantastic, with more to come, but we need to make sure that our gadgets do not extract too much of a social cost.

Sure, when the decade began, there was the initial Internet novelty fascination and the Wild, Wild West free-wheeling mentality associated with all things Internet-related. VC's were throwing money hand over fist for practically anything tied to a new online idea. Valuations and share prices of start-up companies went through the roof, even if the supporting economic fundamentals were not in place.

Along came the dot-bomb period, and the bottom seemed to drop out of the tech sector. But while prior gains were lost, and even though many new tech companies fell by the wayside, the strong remained and ultimately became stronger. Companies like Google, Amazon, eBay and Apple now are mainstays of current American life. If we want to find something out, we "Google" it; if we want to buy something, we probably can find it on Amazon; if we want to participate in the world's largest online marketplace, we go to eBay; and if we want the latest cutting-edge computer or media device, and online music, we likely will get what we want from Apple.

Tech stocks did crater along with other stocks during the 2008 meltdown. But the NASDAQ has been leading the stock rebound of this past year. Why? Perhaps because tech is here to stay. Even with the ups and downs of the stock market and certain tech companies, the Internet no longer is subject to slow dial-up connections or is the plaything of "geeks" only. Tech and portable wireless access have become ubiquitous.

When I first started writing on tech issues, in the late-1990s, I was much like "Inspector Gadget" - I had a different device for every conceivable function, because I wanted it all. On my belt back then, I would clip on my PDA that simply coordinated my calendar and tasks, as it was an island with no outside access. I also would attach my MP3 player for stored music. When I wanted to take pictures, I would clip on my camera, and at times I would strap on my video camera. I dreamed of the day when all of this technology would come together, and it has beyond expectation.

Now, our PDAs do it all. In a device the size of a deck of cards, we can make phone calls, we can send and receive email, we have full Internet access, we can listen to stored music, we can access music wirelessly, we can take and view photos and video, and we can send media files. This technology is widely available and is not the province of the few. The younger generation

has been growing up with this convergence of technology during this decade and has come to expect many functions, speed and convenience, driving the technology push further forward.

Where there is wireless access, we now can perform so many of life's functions right out of our hand. This was not at all true a decade ago. Back then, long ago and far away, we were afraid that Y2K might grind all computers to a halt. Of course, that did not happen and we have moved forward at warp speed.

But with advances in technology comes social challenge. It is not uncommon to be in a public place where the annoying chatter of others' cell phone calls can be disturbing. Or, whether in public or private locations, rather than interact with one and other, people often are glued to their hand-helds and removed from the world right in front of them. Some people have retreated so much into technology that they are "Internet addicts," and others spend more time in "virtual worlds" than in real life. And there are safety issues as well, when people are distracted so much by their devices that they do not pay sufficient attention when they are driving or performing other tasks that require full attention.

Technology when used properly, can increase productivity, convenience and speed. But our hand-held devices cannot give us a hug - at least not yet! So while further technological advances in the next decade likely will be exciting, let's not also forget the old adage that "simple things are the best."

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 Web site is http://www.sinrodlaw.com 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.