DuaneMorris®

www.duanemorris.com

ERIC SINROD: THE YEAR IN TECH LAW 2011

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

JANUARY – DECEMBER 2011

P: 415.957.3019
ejsinrod@duanemorris.com

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

About the Author

Eric Sinrod is a partner in the San Francisco office of Duane Morris LLP (http://www.duanemorris.com) where he focuses on litigation matters of various types, including information technology and intellectual property disputes. His 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.

Table of Contents

(link)

Will Your High-Tech Holidays be Naughty or Nice?

December 20, 2011

Well, it's that holiday time of year again. Have you been naughty or nice?

If you have been naughty, perhaps we will give you the low-tech equivalent of a lump of coal — a broken typewriter.

That's right, we are talking about an old machine that actually requires some finger strength when you push down on the keys. And you are correct, this baby is so wireless that it is not connected to anything, not even an electric outlet. To add insult to injury, not all of the keys even work.

When my computer-raised daughter once saw a typewriter on display at a museum, she exclaimed, "look, an old computer." Not! And this is your lump of coal if you have been naughty.

But if you have been nice this year, the sky is the high-tech limit as to the gifts you may receive.

From Apple, you could receive an iPad, an iPhone, an iPod Touch, an iPod Nano, an iPod Shuffle, an iPod Classic, a MacBook Air, a MacBook Pro, a Mac Mini, or even an Apple TV, not to mention a wide variety of supporting accessories.

From other providers, you might fancy something from among an array of phone and radio devices, televisions, video equipment, music and audio players, computers and tablets, cameras and camcorders, GPS devices, and video games and tech toys.

Plainly, having been nice will bring its rewards, and naughtiness will yield little.

Would you rather receive a hand-held device that can do practically everything at your fingertips, or a prehistoric piece of metal that on a good day might allow you to punch and print some letters onto a piece of paper?

The choice was yours and now it is time to find out what you will receive!

(link)

Is Teen Sexting a Real Problem or Just Hype?

December 13, 2011

Most of us have heard about sexting -- the practice of people sharing naked pictures of themselves online. Indeed, there have been press reports that suggest texting has become the latest teenage craze. Fact or fiction? Perhaps a bit of both.

Recent studies by the journal Pediatrics show that 1% of children between the ages of 10 to 17 have engaged in sexting. About the same percentage have shared less explicit but still suggestive photos of themselves. And 7% report that they had been the recipient of either type of photo.

This does not suggest rampant sexting on a percentage basis. However, on a sheer numbers basis, even 1% of all children between the ages of 10 to 17 means that many thousands of such kids have engaged in sexting.

Furthermore, other studies have shown a higher percentage of sexting among teenagers 14 and older, and also among young adults.

The recent studies tend to show that few children actually are prosecuted or compelled to register as sex offenders by virtue of having sexted. That is not the real danger.

Rather, just one sext can have a life of its own. It is true that people have been fascinated by the human body since humans first walked the earth. Indeed, cave paintings and sculptures from past millennia depict the nude human form in all of its splendor.

But instead of a cave painting or sculpture that might be available for viewing by just a few people, a sext can go viral all over the Internet.

Imagine this scenario: A 13-year-old girl sends a text message with a photo of her topless to her boyfriend of the same age. He then sends it to his friends, who send it to others by text and email, and then one of them posts it on various Internet sites for all of the world to see.

Needless to say, the poor girl could be humiliated and embarrassed, and she may then be harassed by others. It could also be difficult to track down, take down, and delete of copies of the photo.

So, while the percentage of all teenagers who are sexting may not be as high as originally thought, the sheer numbers are not irrelevant and the impact on people directly affected can be dramatic.

(link)

Fake News Websites Touting Weight Loss Shut Down By FTC

December 7, 2011

The FTC is intent on stopping online deceptive health claims. It has been especially interested in shutting down sites that make false and misleading dietary claims.

As part of its crackdown efforts, the FTC, along with the State of Connecticut, filed a complaint that sought to stop a specific operation based on Connecticut.

And the FTC has now announced that the parties have agreed to a court order that temporarily halts the allegedly illegal conduct.

The fake news sites promoted these deceptive dietary products. They also allegedly asserted weight-loss claims that were deceptive. They allegedly informed customers that they could receive free product trials when they actually then ended up paying for the trials and monthly shipments. This operation allegedly brought in more than $25 million from U.S. consumers.

The stipulated court order halts the marketing or selling of certain product plans. It also prohibits the making of unauthorized charges while selling any product. It also prevents the assertion of certain deceptive claims about the products.

Furthermore, the order requires the cessation of collecting on customer accounts, and puts in place an asset freeze pending a final resolution of the court action.

The FTC has stated that this is its eleventh case targeting fake news websites designed to promote dietary supplements. The FTC notes that it works for consumers to prevent fraudulent, deceptive and unfair business practices, and it appears that the FTC is getting the job done at least with respect to this particular Connecticut-based operation.

(link)

Technology and the Internet By the Numbers

November 9, 2011

Back in the 1990s, there was talk of the coming "information superhighway." Now we are traveling at warp speed on that highway. Take a look at some of these jaw-dropping stats:

Facebook

- Facebook now boasts more than 800 million active users, with 350 million gaining access from mobile devices.
- Roughly 70 percent of Facebook users are located outside of the United States.
- Every month about 30 billion content links are shared on Facebook.
- Remarkably, Facebook users install 20 million apps every day.
- Almost half of 18-34 year-old users check Facebook when they wake up, with more than a quarter of users doing so before they even leave the bed.

YouTube

- More than 3 billion videos are viewed daily on YouTube.
- Eight years of content are uploaded on YouTube daily, with more than 48 hours of video uploaded every minute.
- The video content uploaded onto YouTube in just one month exceeds the content created by the three major US networks in 60 years.
- Almost three-fourths of YouTube traffic comes from outside of the United States.
- By 2014, 90 percent of Internet traffic will be video.

Consumer Products

- Ten million iPads were purchased in 2010.
- Seven million Kindle (relaunch) were purchased in 2010.
- Eight million Kinect for Xbox 360 were purchased in 2010.

Business Social Networking

In 2009, only 42 percent of major companies used wikis, blogs or social networking to communicate with customers, suppliers and partners.

Now, 77 percent of such companies employ these tools.

Connectivity

- There were 4.6 billion cell phones in use as of 2010.
- As many as 48 million consumers have mobile phones but no electricity.
- Sixty billion instant messages are sent every day, and 40 percent are business-related.
- Skype boasted 29 million simultaneous online users in early 2011.

These eye-popping statistics were provided by Ken Trombetta, Cisco Area Vice-President.

There is little doubt that we are moving forward on the information superhighway. The journey so far has been fascinating, and surely the highway will take us to future destinations that we cannot even imagine presently.

(link)

Controlling E-Discovery Costs In Patent Cases

November 1, 2011

Electronic discovery can be time-consuming, burdensome and expensive. Indeed, at times, e-discovery can be the tail that wags the litigation dog.

As a consequence, Chief Judge Randall Rader of the U.S. Court of Appeals for the Federal Circuit, on behalf of an E-Discovery Committee, recently introduced a Model Order for Patent E-Discovery.

The Committee's discussion underpinning the Model Order notes that federal district courts have inherent power to control their dockets in the interests of time and economy. Accordingly, it is the Committee's view that the Model Order may be a "helpful starting point for district courts to use in requiring the responsible, targeted use of e-discovery in patent cases."

Key features of the Model Order include the following:

- electronic discovery will not include metadata absent a showing of good cause (however, certain basic fields like the date and time that a document was sent and received will be included);
- general e-discovery requests are not to include email or other electronic correspondence;
- email requests shall be propounded for specific issues, shall occur after initial disclosures and basic patent documentation, and shall be limited to five custodians and five search terms absent other agreement or leave of court; and
- inadvertent production of privileged or work production electronic information shall not constitute a waiver.

Plainly, if district courts adopt the Model Order or enter similar orders, the scope of electronic discovery potentially would be vastly circumscribed. And, of course, this would reduce the burden and cost of patent litigation.

And while that has value, there also is benefit to sufficient discovery to obtain facts important to a particular case. It is possible that some relevant facts may not come to light in litigation with electronic discovery restrictions.

It will be interesting to wait and see if the Model Order gains traction in patent cases. Indeed, if it does, it could spur such limitations in other types of cases. Time will tell.

(link)

Foreigners' Email on Domestic Servers Protected, Ninth Circuit Rules

October 10, 2011

Foreigners can be protected by the Electronic Communications Privacy Act (ECPA). The parts of the ECPA that prevent ISP's from revealing electronic communications apply to foreigners when their emails are stored on a domestic server, the Ninth Circuit has ruled.

In Suzlon Energy v. Microsoft, the plaintiff had directed a subpoena to Microsoft seeking the substance of emails between a citizen of India with respect to fraud litigation in Australia. Microsoft did not comply with the subpoena, taking the position that to do so would violate the ECPA. The federal trial court agreed and quashed the subpoena.

The case went up on appeal to the Ninth Circuit. A unanimous appellate panel decided that the statutory language of ECPA extends its protections to the Indian citizen. The Ninth Circuit reasoned that if Congress had intended to limit the application of the statute to citizens of the United States only, Congress would have done so explicitly.

The Ninth Circuit also stated that limiting the ECPA only to US citizens could cause practical problems. An ISP would have to go about the difficult task of trying to ascertain whether an account holder was a US citizen.

Still, the Ninth Circuit was clear that the ECPA governs "at least" when the requested information is stored on servers within the United States. In this case, the emails in question were housed on Microsoft's U.S. servers.

The Ninth Circuit made plain that it was not considering whether the ECPA could apply to information stored outside of the United States. Indeed, two years ago, another Ninth Circuit panel concluded that the ECPA does not govern email interceptions beyond the U.S.

This is an important and developing area of the law. Stay tuned for further developments.

(link)

Ever Feel Like Unplugging from All this Technology?

October 4, 2011

Information technology overload can be a very real thing. Don't get me wrong – technology is fantastic. Instantaneously we are on top of fast-breaking news developments. And we are in immediate and constant contact with our "friends."

But sometimes doesn't it all seem a bit too much? Do you ever just want to turn off, take a breath and simply observe the real world around you?

Once upon a time, the spoken word was the coin of the realm when it came to human interactions. Usually, only one person would be listened to at a time. People also captured their thoughts by taking their time and communicating in correspondence and other written works.

Along came the printing press, and the advent of mass communication emerged. But still, people only read a limited number of books and letters as part of their lives.

Later, the telephone arrived, and for the first time people could talk to each other while not being in the same place. Yet, while land line telephones proliferated, usually there was only one phone line per house, limiting how many people could be engaged in phone conversations at a time.

Time marched on, and along came faxes, then Internet access, emails, text messages, instant messaging, social networking, Skyping, and more. In any given moment, we now can reach out and be touched in a myriad of ways from devices smaller than a deck of cards.

The advantages of such instant and all-encompassing access are obvious. That is why we are where we are now with information technology. However, there are personal downsides.

It really is possible to allow information technology to gobble up all waking time, such that a person is oblivious to the actual world in which we live. We all have seen people in gorgeous scenic spots staring into their handheld devices or squawking on their cell phones. They miss magic moments right in front of them, if they bother to look.

So, while information technology is good and is here to stay, let's commit to turning off once in a while. Perhaps we each should set aside just a bit of time each day just to be – free and unfettered by electronic communications. Indeed, this can be very liberating, and we later return to our devices refreshed and happier.

(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'a 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)

Sensitive Company Information Bleeding Out The Door

September 8, 2010 11:45 AM | No TrackBacks

Companies naturally want to protect their internal, sensitive company information. Indeed, intellectual property and trade secrets often constitute the crown jewels of a given operation. Companies also have practical and legal obligations to protect confidential information of their customers. Accordingly, prudent companies develop policies that are designed to ensure the security of such highly valuable, proprietary and sensitive data. But does that mean that company employees necessarily follow those polices? Au contraire!

Indeed, according to a recent study in Europe by Ipswitch, a file transfer security vendor, 69% of IT managers transmit highly confidential data, such as payroll, financial and customer information, over the Internet using unsecured emails.

And practically half of surveyed employees readily concede that at least once a week they send confidential or regulated content, the type of which could potentially require data breach notifications under governing laws if the content is stolen or lost.

On top of this, 69% of those surveyed said that they send highly confidential information at least once per month simply using regular, unencrypted emails and attachments. Moreover, 34% report that they do so daily! In addition, 70% of respondents answered that they house company information on their PDAs, USB drives, and elsewhere through remote connections.

While 62% of companies surveyed have security policies in place that detail how sensitive information must be secured for transmission, 72% admit that they do not have enough transparency to ascertain how data is transferred internally and externally.

So, when it comes to protection of sensitive information maintained by companies, perhaps the biggest fear is not external hackers. Instead, companies may need to look in the mirror and follow through on true data security.

Companies technically must be able to track how and under what circumstances their data is transmitted. They also need to motivate their personnel to actually follow their data security policies.

Perhaps in this regard a carrot and stick approach could work; namely, providing positive incentives for compliance and penalties for non-compliance. And companies should consider working actively with skilled data security support vendors and knowledgeable legal counsel in this area.

(link)

Workplace Social Networking: Is Facebook During Work Hours Good?

August 30, 2011

Gone are the days when employers generally blocked or otherwise prohibited social networking by their employees.

Why?

The business upside evidently outweighs the potential downside. But still, employees must be informed as to how best to conduct their social networking activities on behalf of their companies.

The used to be worries that employees would use social networking for purely personal pursuits, thus resulting in lost productivity. Of course, those types of fears were present earlier when it came to simple Internet access.

The concern was that employees would spend their time Web surfing or online shopping while it work, instead of performing their job functions. But employees ultimately were provided Internet access, just like now they often are allowed to engage in social networking.

The benefit from employee social networking can be tremendous from a business standpoint.

Business partners and customers can be contacted, coordinated and expanded via social networking. Advertising campaigns can be launched and maintained through social networking at a fraction of a cost of traditional advertising. Information about products, services and programs can be disseminated by social networking, and companies essentially can create their own fan base.

Nevertheless, employees can "get it wrong" when it comes to social networking, and they need to be educated by their employers in terms of what will fly and what will not. Employees need to be instructed specifically how to hold themselves out on behalf of their companies and how they are to fulfill the business mission while social networking. There is no "one size fits all" approach here, and it therefore is incumbent on companies to think through carefully their respective approaches.

Employees also need to be informed about not inappropriately disclosing the intellectual property, trade secrets and other confidential information of their companies when engaging in social networking activities. They therefore need to know what is and is not fair game for social

networking discussion. They also need to be instructed not to defame or disparage others, and they should be educated whether and how to address business competitors.

Employers may instruct employees as to which social networking sites they can and cannot use, the intended audiences to address, and also that their social networking communications will be monitored. As part of this overall process, companies should work with counsel to draft written social networking policies that will be reviewed, agreed to and executed by employees.

(link)

Flashmob Justice: Legal to Unplug Twitter, Messenger For Safety?

August 17, 2011

London was recently besieged with riots. In the wake of these often-organized riots, Prime Minister David Cameron has stated that Britain is evaluating whether to clamp down on social networking activities such as Twitter or Blackberry Messenger during these tumultuous periods.

Cameron's statement very possibly stems from reported comments from law enforcement authorities and other politicians that Blackberry Messenger was used by the rioters to plan their civil disobedience activities. Blackberry Messenger may have been preferred by the rioters because it allows for private, encrypted messages.

It does not appear that Cameron is contemplating a mass blockage of social networking for the British population at large.

Rather, he reportedly told Parliament during an emergency session relating to the riots that "we are coordinating with police, the intelligence services and industry to look at whether it would be right to stop people communicating via these websites and services when we know they are plotting violence, disorder and criminality."

Thus, it appears that the key would be whether and to what extent there is actual knowledge that certain individuals are planning dangerous activities before there would be contemplation of disrupting their social networking coordination efforts.

Of course, government would need to work with social media companies as part of law enforcement efforts, and it is not entirely clear exactly how much cooperation can be expected up front from these companies in turning over information about their customers.

Social networking is a tremendous means to bring people together – hopefully, for legitimate, beneficial, and lawful purposes. When online communications of citizens have been shut down and prevented by certain foreign governments, that has been criticized internationally as repressive.

But what about the disruption of social networking in democratic nations when the goal is to prevent perceived, negative, civil disobedience? On the one hand, there certainly is a place for proper law enforcement. On the other hand, some people argue that rather than blocking social networking of plotting evil-doers, others online should speak out against such riotous activities in an attempt to create a groundswell of momentum against the riots. However, to the extent

the rioters plan in advance in private, that may not be practical, and the rioters may not care what others say.

(link)

Should I Buy Cyber Insurance for Online Protection?

August 9, 2011

The Internet presents a variety of risks for companies, including systems crashes, hacking attacks, security breaches, and the mishandling of private information.

While companies should do all they can as a matter of policy, practice and technology to prevent such risks from coming to fruition, there is no such thing as perfect prevention. Accordingly, as a backstop, companies would be prudent to procure appropriate insurance for their Cyber risks.

A variety of insurance products to address Cyber risks have entered the marketplace for the past decade. And, according to recent press reports, the demand for Cyber security insurance has surged in recent months in the wake of some noteworthy data breaches and an increase in privacy claims.

And the reported good news is that the rates charged for some Internet-related insurance has come down recently. In the mix, certain coverage limits have been raised and some deductibles have been lowered.

Insurance policies still could evolve in this relatively new area as information technology grows and changes. Indeed, the recent social media explosion could result in new risks that may call for even newer insurance products.

Companies would be better off safe than sorry and they should seek insurance that matches up with the profile of their Cyber risks.

(link)

Can't Blame Google Maps for Car Accident Injuries, Court Rules

July 12, 2011

Google's attorneys have seen all manner of lawsuits come across their desks. The search giant gets blamed for a lot of things. Here's another:

Google was sued recently for injuries sustained after a pedestrian was injured by a car after she used Google Maps - she alleged that Google did not adequately warn her of the dangers of automobiles in the area.

Not surprisingly, the judge dismissed the case, holding that Google did not have a duty to warn the pedestrian that crossing the particular street could be dangerous.

In Rosenberg v. Harwood, the plaintiff in the Utah District Court case was hit by an automobile when she tried to cross a road in a country area. She asserted that she was using the instructions from Google Maps when crossing the road. Not only did she sue the driver of the car that hit her, but she also sued Google for failing to warn her of pedestrian perils of crossing this road.

Even though Google provided her with customized search results for her Google Maps directions, the court held that Google did not have a heightened duty of care toward the plaintiff, as this type of information is also available to the general public.

Plus, as the court recognized, the potential dangers in this situation could be readily apparent to the pedestrian and she had responsibility to take care for herself to ensure that she not get hit by a car.

Indeed, even though we now are in the information age, we do need to lift our heads away from our hand-held devices, look around, and be aware of the real world around us!

(link)

FBI Seizes Servers, Takes Down Web Sites in Raid

June 28, 2011

It's obviously important for law enforcement officials to do their best to combat Cyber criminals. But is it possible that their efforts actually can cause harm by bringing down innocent Web sites in certain instances?

Perhaps.

The FBI seized certain web servers as part of a raid, which caused several websites to go offline, including the sites of publisher Curbed Network, according to *The New York Times*. The raid apparently occurred late at night at as a hosting facility in Virginia utilized by DigitalOne, a company based in Switzerland. DigitalOne did not have any employees on the premises when the raid happened.

DigitalOne, reportedly, in an email to a client, disclaimed being the cause of the problem, and pointed the finger at the FBI. DigitalOne stated that while the FBI supposedly was focusing on one of its clients, the FBI nevertheless had seized servers that were utilized by many of its clients.

An unidentified government source apparently reported that the FBI was investigating the Lulz Security group as well as any associated hackers, and was working with the CIA and cybercrime European officials as part of this mission.

Various sites of the Curbed Network, which include restaurant and real estate blogs, reportedly were unavailable for a certain period of time. The FBI raid also apparently impacted a server utilized by Instapaper, a site that saves articles for later review.

Assuming that a legitimate and innocent Web site is brought down as part of law enforcement efforts, and that Web site suffers business interruption and resulting lost revenues, can the company to whom that site belongs seeks legal redress from the governmental entity behind the law enforcement activities? It will be interesting to see if such losses further occur and if such claims are made.

(link)

Is Facebook's Facial Recognition Software Legal?

June 14, 2011

Facebook is about to be subject to a probe by European Union data protection regulators. They will be looking at Facebook's implementation of facial recognition software to propose, without permission, the names of people to be tagged in photos, according to press reports.

These regulators will study the issue to determine whether there have been any data protection violations.

So, what is this all about?

Well, as we know, people can tag the names of others who appear in photos posted on Facebook pages. These can be handy, as viewers get to know who they are looking at in the photos.

On the other hand, there are times when persons appearing in photos do not wanted to be identified by name in those photos. Photos, for example, can be taken without consent and can show people in compromising situations, and the more identification the less desirable for the photos subjects in those instances.

Along comes a Facebook feature that, based on facial recognition software, proposes names of people to tag in photos premised on photos in which they previously have been identified by name. While this feature creates greater ease in tagging, it also potentially increases instances in which people are tagged in photos without their permission and against their wishes.

Apparently, this facial recognition feature is a default setting that can be disabled. But even if this were reversed, such that the feature had to be activated to be put in service, it still raises the possibility of increased instances of tagging against the desires of people who appear in photos.

It is important to put this into context. Many millions of people are tagged daily in photos placed on Facebook. Given this tremendous volume of tagging, and the relatively low level of complaints, it is possible that most people do not mind that they are tagged in photos placed on Facebook by others. But still, if you are someone whose incriminating photo shows up on Facebook with your name tagged without your permission, you likely will not be happy.

One potential idea is that when someone's name is generating for tagging in a photo, that person should be contacted for consent prior to tagging. However, this could be cumbersome.

Plus, Facebook does not want to be responsible for third-party content posted by others. And Internet service providers generally have immunity under the Communications Decency Act with respect to such third-party content.

Time will tell how the European Union regulators and others grapple with this issue.

(link)

Can I Get Busted For Someone Else's Cyber Attack?

May 31, 2011

Businesses, governments, and individuals rightly are concerned about potentially becoming victims of Cyber crimes and attacks.

However, should there also be worry that the blame for such crimes and attacks could be directed to the innocent who had no intent and took no affirmative action in furtherance of evil deeds?

Maybe. Let's explore a hypothetical. Assume that a disgruntled Cyber terrorist on a remote mountain top wants to wreak havoc on a major commercial Web site.

Assume also that the terrorist launches a distributed denial of service attack on the major commercial Web site.

In an effort to cover his tracks, the terrorist routes the attack via an innocent third-party site. As a result, the major commercial site shuts down, after being relentlessly bombarded with packets of information, last emanating from the "zombie" third-party site, as originally triggered by the terrorist.

Naturally, the terrorist could have criminal and civil liability for the attack. But he may be difficult to track down, he could be overseas, and even if found, he may not have any financial resources to satisfy any legal judgment against him.

While the major commercial Web site might like to know that the terrorist will get put behind bars in prison. But the commercial site would want to be made whole financially. The shut down of its site caused business interruption to the tune of millions of dollars.

So, from whom can the major commercial Web site recover? The innocent third-party site?

Again, perhaps.

When these types of attacks were fairly unknown, they were not anticipated and foreseeable. But now, the major commercial Web site might argue that these types of attacks are known to be with us, and thus, Web sites not only have a duty to implement enough security measures to protect themselves from harm, but they also should do enough to make sure they are not the launching pad for attacks by others to others.

The commercial Web site would argue that what happened was foreseeable, and because the third-party site did not implement current security measures, it is liable under a negligence theory.

The third-party site would counter by pointing out that this particular attack was not foreseeable and that it has no independent to protect the commercial Web site. Who is right?

This is the stuff of litigation coming to a courtroom near you. The outcome in a given case would depend on the factual circumstances.

(link)

Anti-Spam Law Governs Social Media Pages, Court Rules

May 3, 2011

Once upon a time, and without a federal law in place, more than half of the states enacted their own laws to address the pervasive problem of unsolicited commercial email, affectionately known as "spam."

Then in 2003 Congress stepped up to the plate and enacted the CAN-SPAM Act. This federal statute imposes certain requirements and restrictions on a nationwide basis with respect to the sending of unsolicited commercial email. Problem solved, right?

Not quite.

For one thing, email spam has continued, relatively unabated. Why? Because many spammers are overseas and/or cover their tracks in a way in which they believe that they will not be caught and punished. In addition, some spammers frankly have meager financial resources, making them somewhat judgment proof when it comes to monetary damages.

In addition to these problems, unsolicited commercial electronic communications now can take varied forms, not just by way of email. Thus, it has been an open question whether "electronic mail messages" addressed by Congress in the CAN-SPAM Act include social networking communications that do not necessarily involve the sending of communications to an email box. Well, that question has just been answered in the affirmative by one federal trial judge.

Several months ago, Facebook, the largest social media company, filed a lawsuit in federal court in San Jose, California alleging that MaxBounty, via affiliate publishers, established fraudulent Facebook pages that sent Facebook users to outside commercial web sites. MaxBounty sought to dismiss the complaint, arguing that the CAN-SPAM Act specifically is confined to email messages that are not at issue in the case.

Ultimately, the judge disagreed with MaxBounty and held that the CAN-SPAM Act does apply in this social media context because the legislative intent was to help cure the volume of unsolicited and potentially inaccurate and misleading commercial communications that burden the growing Internet. This means that Facebook's case against MaxBounty may proceed toward trial.

As information technology advances, the law seeks to catch up. This is one more example of a law (and a relatively recent one at that) being applied in a new context that may not have been envisioned perfectly when enacted.

(link)

Effective Tips on How to Use Social Media Marketing

April 12, 2011

Initially, some companies were reluctant to embrace social media, perhaps being concerned about lack of control and other issues.

However, as the world truly has migrated to social media sites (with Facebook boasting hundreds of millions of users), there now is little doubt that most companies now want to embrace social networking as a way to get the word out about their products and services.

But, what are the best strategies for businesses to employ in the social media context? Buddy Media, Inc. seeks to answer that question in its recent publication "Strategies For Effective Facebook Wall Posts: A Statistical Review."

For example, one issue examined by the report is the best timing for posting content on Facebook. And interestingly, it turns out that companies that post content outside of normal business hours experience a 20% higher engagement rate on their posts.

In addition, Thursdays and Fridays tend to be the best days of the week to post content, as the "happiness index" for users peaks toward the end of the week. And weekends can be effective days for posts, yet many businesses avoid the weekends. Monday is the least effective day for posting.

Also, the paper indicates that it is important to keep business posts "short and sweet." Posts that are less than 80 characters have a 27% higher engagement rate than longer posts. Yet, only 19% of such posts are less than 80 characters. So, remember to keep it simple.

Furthermore, URL shorteners can be bad news, as full-length URLs result in engagement rates three times higher. Users know that a URL such as www.buddymedia.com will take them to the Buddy Media website, whereas a shortened URL like http://tinyurl.com/yhlw3c6 does not make clear where the user will be directed if she clicks on that link.

And, posts that end with a question cause 15% higher engagement rates, because they seek action from users.

Businesses would be smart not only to market appropriately via social media, but they should think how best to do so.

(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)

European Union Circling the Antitrust Wagons Around Google?

January 18, 2011

The European Union is conducting an investigation of Google to ascertain whether the Internet search giant has committed antitrust violations, according to a recent New York Times article.

Specifically, the EU antitrust investigation is seeking to find out from companies that advertise via Google if they were asked by Google to increase their advertising spending on the site in exchange for better prominence in Internet search results. Furthermore, an effort is being made to understand whether Google sought to get in the way of companies that sought to take their advertising business to other places on the Internet.

Apparently, a confidential questionnaire was sent to companies who advertise on Google and that is intended to find out if Google played with search results to maintain advertising business and to cause detriment to online Internet search and advertising competitors, as reported by the New York Times and supposedly reviewed by The International Herald Tribune.

This questionnaire is reported to contain questions such as: "Please explain whether and, if yes, to what extent your advertising spending with Google has ever had an influence on your ranking in Google's natural search"; and "Has Google ever mentioned to you that increasing your advertising spending could improve your ranking in Google's natural search?"

The EU antitrust investigation also apparently seeks to ascertain whether Google has attempted improperly to exert influence as to advertising on mobile devices, and if Google is trying to hang on to customers by erecting roadblocks for them to transfer information to competitor services. The targeted companies reportedly have been requested to respond in February.

These questions, if posed as reported, are significant, because natural search results are supposed to display most relevant information responding to users' specific search requests, as opposed to paid advertising that appears on search engines.

The New York Times article states that Google is blaming Microsoft for creating opposition to its business in Europe, because in antitrust authorities there have been more aggressive recently than in the US to look into alleged antitrust violations.

It will be interesting, to say the least, to see how this plays out after the companies respond to the EU questionnaires.