DuaneMorris®

ERIC SINROD

THE YEAR IN **TECH LAW 2016**

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

JANUARY – NOVEMBER 2016

P: 415.957.3019 | ejsinrod@duanemorris.com

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

TABLE OF CONTENTS

ABOUT THE AUTHOR

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

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

U.S. 'Sniffer' Jets Seek to Detect North Korea Nuclear Detonations

JANUARY 12, 2016

http://blogs.duanemorris.com/techlaw/2016/01/12/u-s-sniffer-jets-seek-to-detect-north-korea-nuclear-detonations/

There have been recent claims that North Korea successfully conducted a hydrogen bomb test. Plainly, if North Korea has this capability, there would be cause for concern. But, according to CNN, the White House is skeptical, and the Air Force may send a "sniffer" jet in the region of the Korean Peninsula to help ascertain whether North Korea's claims are accurate.

CNN has been informed by a U.S. official that any type of nuclear detonation would cause certain distinctive elements to be present in the air, and collected air samples could find out what if anything occurred.

The aircraft tasked would be a WC-135W jet, referred to as the "Constant Phoenix." The Air Force has two of these jets that operate from Offutt Air Force Base in Nebraska, according to CNN. (In addition, the US reportedly has ground stations that can help refute or verify the claimed detonation).

The Constant Phoenix jet reportedly contains external devices with filter paper that collect radioactive particulates from the atmosphere. According to CNN, the Constant Phoenix program began long ago in 1947 with General Dwight D. Eisenhower; the Army Air Forces (the forerunner of the Air Force) started using certain bombers to try to detect nuclear tests by the Soviet Union.

Constant Phoenix jets not only have been tasked to monitor compliance or not with nuclear weapons treaties, but they also reportedly have had broader application, like monitoring the consequences of the Chernobyl nuclear power plant explosion in 1986 in the Soviet Union.

The Constant Phoenix "sniffer" jets serve a valuable purpose. Let's just hope in this instance that if such a jet is employed, that it determines that North Korea in fact has not successfully detonated a hydrogen bomb test. The latest reports indicate that we won't know for certain at least for a few days.

David Bowie: Internet Predictor and Precursor

JANUARY 19, 2016

http://blogs.duanemorris.com/techlaw/2016/01/19/david-bowie-internet-predictor-and-precursor/

Sadly, we lost David Bowie last week. Most of us remember his songs — so many, and so varied across the decades. And, of course, there is no way to forget Bowie's ever-changing image over the years. But not to be lost in the shuffle is the fact that Bowie was such an innovator, he also anticipated the full impact of the Internet.

Bowie's prescience when it came to the Internet was explained in a recent article in The Verge. Let's delve in a bit.

As far back as 1994, Bowie issued a CD ROM accompanying his song "Jump, They Say" — and this enabled users to create their own music videos.

On top of that, in 1996, Bowie released his song "Telling Lies" only on the Internet — and causing a stunning 300,000 purchases in this process back when Internet sales were not at all common.

Believe it or not, Bowie assisted the New York Yankees in creating the team's first Internet site.

Amazingly, in 1998, Bowie created his own Internet Service Provider — an ISP that allowed users on the Internet to access many of his songs, videos, and photos. This ISP fittingly was called BowieNet, and users paid $19.95 per month. Users were given five megabytes of space to create their own personal sites, where they could insert music and videos into regular web pages. In effect, this was a music-oriented social network long before the advent of MySpace and then Facebook.

When interviewed years ago about the coming Internet, Bowie said "We're on the cusp of something exhilarating and terrifying." He described the Internet as a "communal power." He said "I don't think we've even seen the tip of the iceberg" in terms of that power. And he foresaw that "what the Internet is going to do to society, both good and badd, is unimaginable."

David Bowie always was ahead of his time. He is missed now.

Facebook Is All Over the News

FEBRUARY 3, 2016

http://blogs.duanemorris.com/techlaw/2016/02/03/facebook-is-all-over-the-news/

Facebook is the largest "nation" in the world, with more than 1.65 billion users across the globe. Not surprisingly then, with such global reach, Facebook is in the headlines fairly often.

In terms of Facebook news items, a recent example includes a Thai criminal court putting a man in prison for six years because he posted comments on Facebook that were construed to be insulting to the king of Thailand. The court so ruled because the law of Thailand criminalizes statements that are defamatory, insulting or threatening to the Thai royalty.

On a lighter Facebook news note, President Obama has been recognized as the most "liked" politician on the social media network. While Indian Prime Minister Narendra Modi comes in second place with 31 million likes on his Facebook page, President Obama ranks first with in excess of 46 million likes on his Facebook page.

And when it comes to Facebook "likes," Facebook relatively soon is reported to be rolling out other emotion buttons. Rather than only a like button, users perhaps will have access to buttons such as love, sad, angry and other emotions. Imagine, users will have options when it comes to emotion buttons! This makes abundant sense, as it can be highly awkward to click on the like button when responding to someone's sad post on Facebook.

Last but not least for now, Facebook has announced that it is banning on its site the sale of firearms that can bypass background checks. Well, phew, that is good news! Some of us did not even know that such sales were happening in the first place.

Undoubtedly, Facebook will continue to show up in the news going forward. Stay tuned.

Facebook Potentially Liable in French Nude Painting Case

FEBRUARY 17, 2016

http://blogs.duanemorris.com/techlaw/2016/02/17/facebook-potentially-liable-in-french-nude-painting-case/

An appellate court in Paris has ruled recently that Facebook can be sued in France and a case thus can proceed against the social media giant in France with respect to Facebook's decision to remove the account of a user in France who posted a well-known 19th century nude painting, according to *Reuters*.

This legal decision could be of concern to Facebook, as it has more than 30 million users in France, and because the French appellate court rejected the clause contained in Facebook's terms and conditions, that requires worldwide lawsuits to be heard in Santa Clara, California, as "unfair." Facebook still has the option to seek review by the highest appellate court in France.

This particular case was brought by a Parisian teacher and art lover who had his Facebook account terminated without any advance notice. The account was terminated shortly after he posted a photo of a painting entitled "The Origins of the World" by Gustave Courbet from the 19th century. That particular painting includes a depiction of female genitalia.

In this lawsuit, this Facebook user seeks the reactivation of his account, and he also is seeking damages. He has stated his belief that he has a free speech right to post an artistic masterpiece without being censored by a social media network. He also stated his belief that it is not up to Facebook to try to determine whether a particular work is a masterpiece or pornography.

On its site, Facebook explains that it may restrict the display of nudity so that some audiences within its global community may not be offended due to sensitivity with respect to this type of content. But Facebook also explains that it does allow photographs of certain artistic works that depict nude figures.

The lawyer for this particular Facebook user has stated that Facebook in essence is hypocritical by allowing images of violence while seeking to limit the display of nudity within artistic works.

Facebook likely takes the position that its users are bound by the terms and conditions on its site, and that it also has the corresponding right to remove what it deems as inappropriate content on Facebook. Facebook obviously also believes that disputes relating to the site and its content should be venued in Santa Clara California, as stated on its site.

This Facebook user believes that he has a free speech right to display art like the photo of the painting he posted, and that Facebook should not be in the position of acting as the world's social media referee regarding artistic and other content.

Facebook most certainly believes that it has immunity from liability for content posted on its side by its users, pursuant to Section 230 of the Communications Decency Act. However, the more active Facebook becomes in terms of deciding which content should or should not be displayed on its site, it is conceivable that its immunity under the statute could be eroded.

Cyber Security – The Topic Avoided by the Presidential Candidates

MARCH 2, 2016

http://blogs.duanemorris.com/techlaw/2016/03/02/cyber-security-the-topic-avoided-by-the-presidential-candidates/

It already seems like the Presidential campaign has been going on forever. There have been countless debates, speeches and statements by and among the candidates. Some topics such as immigration and whether to build a wall have been rehashed over and over – beating dead horses further to death. But what is the one topic the candidates consistently ignore?

Cyber security!

Sure, the candidates talk tough, and each seems to suggest that he or she will be the mightiest of the mighty when it comes to dealing with the likes of Russia, North Korea and ISIS. But hardly ever, and almost never, do they talk about cyber security.

The Internet is wonderful in many respects. We have all sorts of information at our fingertips instantaneously. We can communicate with people all over the world in many online ways. Shopping never has been easier — as we can buy practically anything with just a simple click.

But just as the commercial world has gone online, so has conflict, crime and war (yes, war!).

A number of countries are beefing up their cyber warfare capabilities, not only for defensive purposes, but for potential offensive attacks. Such attacks could bring down all sorts of critical systems — like banking, air traffic control, electrical and nuclear power, and the list goes on and on. The attacks also could disrupt our military capabilities.

Some experts believe that the United States needs to do more in this new era of potential cyber warfare. They suggest that the U.S. should hire thousands of more Internet security experts. And President Obama has just suggested billions more budgetary dollars for cyber security purposes.

Getting back to the Presidential candidates — why aren't they talking about cyber security when they otherwise are talking tough about fighting the enemies of the United States?

The frightening answer is that they likely do not understand the issues relating to cyber warfare well enough to express opinions and to outline strategies and plans. Whoever becomes President will need to get up to speed very quickly. Better yet, the candidates right away should learn the issues so that they can be discussed as part of the campaign and in order for the next President to be able to lead immediately upon taking office.

Will Your Smartwatch Save Your Life?

MARCH 16, 2016

http://blogs.duanemorris.com/techlaw/2016/03/16/will-your-smartwatch-save-your-life/

The love affair with smartphones has led to further rapture with smartwatches. Right now, we can act like Dick Tracy, with the world on our wrists within these tiny smartwatch gadgets. But these smartwatches might not all be about work, communications, and fun and games. Why? Because there is the potential that smartwatches might evolve soon to have the capability of saving lives.

We know that smartwatches presently have health sensors that can monitor steps taken, flights climbed, and heartbeat rates for exercise and physical fitness purposes. And Apple, ever on the cutting edge, apparently believes that it can go further to use such monitoring capabilities to facilitate calls for help during health emergencies.

As recently reported by Time, a new Apple patent application, unearthed by Apple Insider, describes a potential feature that would have smartwatches call for help if the devices pick up monitoring information that suggests that users are having medical emergencies. For example, an Apple Watch might detect that a wearer's heartbeat is tremendously high or low, and in such event, it could push a signal that would call for medical assistance.

The Apple Watch owner in advance would set up a list of pre-established contacts who would be contacted in an emergency — perhaps 911, the owner's doctor, and the owner's spouse. Indeed, there would be two levels of "care" lists — one for personal contacts like family and friends, and another for 911 and emergency services.

You might already think that your smartwatch is one of your best friends. But if your device eventually saves your life, BFF status likely would be cemented forever between you and your smartwatch.

Stay tuned and let's see if Apple is awarded a patent for this asserted invention and whether Apple later rolls out this potentially life-saving feature on its smartwatches in the future.

Drones Pose a Real Threat to Commercial Flights

APRIL 7, 2016

http://blogs.duanemorris.com/techlaw/2016/04/07/drones-pose-a-real-threat-to-commercial-flights/

Drones have become cheap and fun to operate for many people. Operators love to fly their drones up into the sky, maneuvering them around while taking photos and videos from aerial vantage points. But do these activities come with risk? Absolutely!

Indeed, last week it was reported that on just one day, April 1st, three drones almost collided with aircraft that were landing at the Schiphol Airport in Amsterdam, Netherlands. And one of these drones apparently came within a mere 300 meters of a plane as it was heading toward a runway.

Pilots from the KLM Cityhopper fleet who were operating a Fokker 70 and an Embraer 190, as well as the pilot of an EasyJet Airbus A319, each reported a drone flying near their respective planes. On top of all of that, if that were not enough, the pilot of the EasyJet reported to air traffic controllers that it had three separate drone sightings.

As a result of the foregoing, the air traffic controllers shut down one of the runways at the Schiphol airport. Moreover, these near-misses are subject to investigation by public safety agencies and Dutch law enforcement. In addition, Air Traffic Control Netherlands is conducting its own investigation.

Could a drone bring down a commercial aircraft upon collision? Well, the concern was high enough that one runway was closed, and the operation of drones in the vicinity of airports in the Netherlands is against the law. And the use of drones is seriously restricted in urban areas — they must be kept at minimum of 50 meters from buildings and roads and 150 meters from railroad tracks and people. These regulations in essence have banned drone operation in the largest cities of the Netherlands.

The concern about drones is heightened enough that it has been suggested that Dutch police have tested whether certain birds of prey might be able to intercept drones out of mid-air.

And, of course, the worry about drones is not confined to the Netherlands. Several months ago, New York-based Bard College issued a report that revealed 327 drone-aircraft near-misses between December 2013 and September 2015. Of these near-misses, pilots had to take evasive action 28 times. One drone came as close as 8 meters of an aircraft.

Plainly, more needs to be done to minimize the danger drones pose to aircraft.

Children May Proceed With Climate Change Case, Federal Judge Rules

APRIL 12, 2016

http://blogs.duanemorris.com/techlaw/2016/04/12/children-may-proceed-with-climate-change-case-federal-judge-rules/

What are we going to do about climate change? Can government get the job done to protect us? Well, some children do not believe so, and they have taken the matter to federal court. Indeed, a federal magistrate has just ruled that their climate change lawsuit may proceed.

Thomas Coffin, U.S. Magistrate Judge for the federal district court in Eugene, Oregon, has ruled in the case Juliana v. United States, that a climate change lawsuit, brought by twenty-one youth from the ages of 8 to 19 years-old, may proceed. The lawsuit specifically asserts that the federal government of the United States is in violation of their constitutional rights to life, liberty, and property by allowing and supporting ongoing production and combustion of fossil fuels.

The lawsuit not only is brought by these young people, but it also is supported by the organization called Our Children's Trust. Furthermore, Dr. James Hansen, an advocate for climate change, who recently was arrested with others for protesting the potential storage of natural gas under Seneca Lake in upstate New York, also is a plaintiff in the children's lawsuit.

Magistrate Coffin ruled that the children's legal complaint states a cognizable claim and may proceed and should not be dismissed out of hand. Thus, the issue of climate change now is up for decision in one federal court.

Magistrate Coffin referred to the children's case as an "unprecedented lawsuit" that involves "government action and inaction" leading to "carbon pollution of the atmosphere, climate destabilization, and ocean acidification." In ruling that the lawsuit may go forward, Magistrate Coffin stated the following in his legal decision: "The debate about climate change and its impact has been before various political bodies for some time now. Plaintiffs give this debate justifiability by asserting harms that befall or will befall them personally and to a greater extent than older segments of society."

He continued in his decision: "It may be that eventually the alleged harms, assuming the correctness of plaintiffs' analysis of impacts of global change, will befall all of us. But the intractability of the debates before Congress and state legislatures and the alleged valuing of short term economic interests despite the costs to human life, necessitates a need for the courts to evaluate the constitutional parameters of the action or inaction taken by government. This is especially true when such harms have an alleged disparate impact on a discrete class of society."

This decision by Magistrate Coffin simply marks the starting line for the children's case, and the case is far from the finish line. Magistrate Coffin has ruled that the case may proceed. Likely there will be considerable opposition to the case by the government, with potential opposition support from the fossil fuel industry.

The fight about climate change now not only will be considered by politicians within legislatures, but it is joined within the judicial branch.

Plainly, this is a case worth watching as it unfolds.

Ashley Madison Class Representatives Cannot Remain Anonymous

APRIL 27, 2016

http://blogs.duanemorris.com/techlaw/2016/04/27/ashley-madison-class-representatives-cannot-remain-anonymous/

It seems like just yesterday that the Ashley Madison site became big news. The Ashley Madison site claimed that it was the world's largest place on the Internet for married people to find adulterous partners. Indeed, the site boasted that it had more than 38 million users. And importantly, the Ashley Madison site claimed that people looking for affairs could do so anonymously. Unfortunately for Ashley Madison users, the site was hacked in July, 2015, and some of the personally identifiable information of some of the site's users was leaked.

As a result of this hack and the leaks, marriages suffered, jobs were lost, suicidal activity was reported, and potential blackmail of government personnel who used the site reportedly was attempted by foreign governments. Ashley Madison users affected by the hack have sought legal redress. A federal class action lawsuit has been filed in the Eastern District of Missouri.

For this lawsuit to proceed, plaintiff class representatives must be approved by the court. These representatives must have claims that re similar to those of the class, and they must be adequate representatives, among other requirements. The proposed class representatives have sought to proceed on an anonymous basis. They do not want to cause any or further publicity to themselves based on their use of the Ashley Madison adultery site.

In an important initial legal development in the case, Judge John A. Ross has ruled that the class representatives for the case cannot proceed on an anonymous basis. While he acknowledged that in cases of great sensitivity, such as those involving child abuse or rape, the plaintiffs may go forward using pseudonyms instead of their real names, but in a case like Ashley Madison, mere embarrassment is not enough to counter-balance the presumption of openness of court proceedings in the United States.

The judge ruled that while class representatives have certain duties to adequately work on behalf of the class and thus should be identifiable, Ashley Madison class members do not have to be identified by real names in the case. Accordingly, if the currently proposed class representatives do not want to be identified, they can drop out as proposed class representatives and simply remain anonymous as general class members.

Given this ruling, the lawyers prosecuting the case will need to find potential class representatives who do not mind that the case would proceed with their actual names set forth as the class representatives. Of all the many Ashley Madison users impacted and who already have been publicly disclosed by the leaks, it seems likely that the lawyers will find at least a few potential class representatives who will fit this bill.

How to Keep Your Personally Identifiable Information Secure Online

JUNE 7, 2016

http://blogs.duanemorris.com/techlaw/2016/06/07/how-to-keep-your-personally-identifiable-information-secure-online/

It seems like we constantly are hearing about Internet hacks and the stealing of personally identifiable information online. At this point, we use the Internet for so many positive aspects of our lives. Given that we inevitably are online, what are some steps that we can employ to keep our private information safe?

Here are just a few simple tips to keep in mind:

First, it is important to protect your credit card information. One way of doing this is to check and see that the website you are logging onto is secure. One thing to look for is whether the URL begins with HTTPS and not just HTTP. Also, it is important to log out of your customer accounts when you are done with transactions — especially financial transactions.

It also is a good idea to turn off your Bluetooth and Wi-Fi functions on your computer and mobile devices when not using them. By doing this, other people nearby may not be able to gain access. Moreover, you should have your sharing settings configured only with trusted devices that you own.

Unfortunately, it is becoming a fact of life that computers and mobile devices are lost and stolen. Therefore, it is prudent to back up important files and information on the could. Cloud computing has become more secure over time. Indeed, even sensitive sectors such as the healthcare industry now use the cloud for data storage.

This particular tip is especially critical to the younger generation, but to others as well: be as safe as possible when using social media. People tend to share fairly personal details of their lives on social media, and because of this everyone should be very careful about what is posted on these networks. For example, the simple posting of photos showing that someone is on vacation could leave potentially to a robbery in his or her home while away. Furthermore, details shared on social media could come back to bite when someone is applying for a job.

People seem to believe that the simple use of the delete button gets rid of information for all time. However, that is not the case. Data seems to live on forever and can be recovered if certain steps or not taken. One simple step is to make sure that drives are fully and completely wiped before a machine is thrown away or sold. The machine also should be given a factory reset.

In addition to the foregoing, password protection is critically important. Unbelievably, the most common password on the Internet is the word “password.” Obviously, that is not a safe password, nor are many others used frequently. The best passwords should be impossible to figure out even by family members and friends. Indeed, the best tactic is to use a random password generator, and random passwords created should be saved on a safe and encrypted file.

The Internet provides many benefits to millions of users. Nevertheless, personally identifiable information often is vulnerable to misappropriation. Hopefully, the tips suggested before here be useful if employed properly.

Donald Trump Arrives on the Internet as a New Pokemon Character?

JUNE 22, 2016

http://blogs.duanemorris.com/techlaw/2016/06/22/donald-trump-arrives-on-the-internet-as-a-new-pokemon-character/

The news reports lately have been grim in the wake of the Orlando massacre. And at the same time the Presidential candidates have been proclaiming that they each are best suited to combat terrorism going forward.

But, rather than delve into that morass, how about something on the lighter side for a moment? Let's talk about Pokemon characters, and how a newly introduced Pokemon character might bear a resemblance to one of the Presidential candidates whose initials are DT. We can thank a recent CNET article for bringing this to our attention.

As CNET points out, various Pokemon characters resemble animals or are inspired from "real life." Examples include Magikarp, which comes from the yellow rockfish. Another is Caterpie, which is derived from none other than the caterpillar.

And now comes Yungoos, just introduced last week. Yungoos appears to be inspired by the mongoose, at least in terms of its body. However, the head of Yungoos could be intended to resemble Donald Trump, according to CNET. Indeed, Yungoos' hair and teeth, in side by side comparisons, really do show a striking similarity to those of Mr. Trump.

The official Pokemon site talks about Yungoos like this: "It has strong fangs, so it can crush and consume the hardest of objects." Yungoos also "can deal twice the normal damage to any Pokemon that switch in or enter the field mid-battle." Hmm. Trump did crush his rivals from the GOP nomination …

Not everyone agrees that Yungoos is best compared to Donald Trump. There has been the suggestion that Yungoos looks more like London Mayor Boris Johnson.

The mind reels … We can only speculate as to whether Trump, who is clearly not one to shy away from litigation, has considered any legal action.

OK, so much for your light distraction. Plainly, the world has more urgent and pressing matters to address, but every once in a while we need a brief reprieve.

Government Surveillance of Internet Traffic

JULY 6, 2016

http://blogs.duanemorris.com/techlaw/2016/07/06/government-surveillance-of-internet-traffic/

At this point, it may come as no surprise that the US government has some ability to monitor internet traffic. However, the tremendous extent of government surveillance may be somewhat alarming to those who are interested in privacy on the internet.

An article by RT.com reports that the NSA has the ability to read 75 percent of all U.S. internet traffic. The article points out that programs referred to as Stormbrew, Lithium, Oakstar, Fairview, and Blarney all have the ability to monitor the actual text of emails, not just email metadata.

According to the article, NSA officials have downplayed the issue, stating that the NSA "touches" only 1.6 percent of internet traffic. While this at first blush may provide some solace to privacy advocates, TechCrunch has speculated that this 1.6 percent simply refers to information that has been sent directly to the NSA and that has been "culled to their liking."

The article also makes plain that the NSA can zero in on all types of information relating to particular events for a sustained block of time. For example, the NSA, in conjunction with the FBI, reportedly were able to monitor all email and text messages for a six-month period with respect to the 2002 Olympic Games in Salt Lake City, Utah.

Interestingly, even though lawmakers have argued that NSA surveillance is essential in protecting national security, Blarney reportedly was in use prior to the September 11, 2001 terrorist attacks. This particular program was in use close to important fiber-optic landing points, including one near San Francisco and another in New Jersey, with the purpose of intercepting foreign communications coming into an going out of United States.

Of course, government surveillance concerns arise in other countries too. According to IbTimes.com, a new law was recently enacted in Russia that requires companies to store data they collect about Russian citizens on Russian territory. This new law reportedly has created uncertainty among companies and has caused heightened worries about surveillance and threats to privacy rights. This comes at a time when the Russian government has been seeking to tighten its control over the internet. Certain privacy advocates worry that the new law is an effort to obtain access to personal information for surveillance purposes.

We live in uncertain times. There is a dynamic tension between security and privacy. We will see which direction the pendulum swings in the upcoming near future.

Potential Federal Criminalization of Revenge Porn

JULY 20, 2016

http://blogs.duanemorris.com/techlaw/2016/07/20/potential-federal-criminalization-of-revenge-porn/

Revenge porn is unacceptable and should not be tolerated. Some federal lawmakers agree, and they now seek to push legislation aimed at criminalizing revenge porn.

So, what exactly is revenge porn? It often goes something like this:

A man and woman are in a committed, consensual relationship. As part of that relationship, they engage in sexual activity, and they agree, for their own enjoyment purposes, to take photos and videos of their activities. Later, the relationship, whether husband and wife, fiancees, or boyfriend and girlfriend, ends. But the sexually explicit photos and videos still exist. The man (it usually is the man) then posts the photos and videos on the internet to get back at the woman, to humiliate the woman, or to make demands on her. And there are websites that seek such photos and videos — the women who are the victims often must pay a fee to the sites to have the photos and videos taken down.

As revenge porn unfortunately has become more prevalent, there have been efforts made at the state level to criminalize such conduct, and now some lawmakers in the U.S. House of Representatives have introduced previously-stalled legislation that would make it a federal crime to share sexually explicit photos and videos on the internet without the consent of the consent of the subjects, according to Reuters. The legislation is referred to as the Intimate Privacy Protection Act.

Jackie Speier (D-CA), the lead author of the legislation, is quoted as saying that "these acts of bullying [revenge porn] have ruined careers, families and even led to suicide."

The Intimate Privacy Protection Act would authorize prison terms of up to five years and fines for the posting online of sexually explicit photos or videos with "reckless disregard" for the consent of the subjects. Thus, actual intent is not even required, and the penalties are severe. This federal legislation, if it becomes law, would cover revenge porn across the United States; whereas, presently more than 30 states have enacted their own laws.

The statute does contain a few exceptions. One such exception has to do with a person posing in the nude voluntarily in a commercial or public setting, which seems to make sense. Another exception has to do with material that is in the "public interest" — but one would like to think that sexually explicit photos or videos taken in private and not intended for sharing should not be in the public interest.

Previous efforts to pass this type of federal legislation were delayed based on concerns by Internet Service Providers that they somehow could face liability for content posted by third-parties on their sites. They likely would have had immunity in this context under Section 230 of the Communications Decency Act. That aside, the proposed Intimate Privacy Protection Act exempts Internet Service Providers in this area to the extent that they do not promote or actually

solicit revenge porn. And many Internet Service Providers have updated their terms of service explicitly to prohibit revenge porn on their sites.

Now that this anti-revenge porn legislation is on the move in Congress, let's stay tuned to follow its progress and whether it actually becomes law.

The Ultimate Impact of Sex Robots

AUGUST 24, 2016

http://blogs.duanemorris.com/techlaw/2016/08/24/the-ultimate-impact-of-sex-robots/

Technology continues to advance to help humans in so many countless ways. And now we are getting to the point that we are not simply dealing with cold machines, but we are dealing with features and contraptions that are becoming quite human.

For example, we can talk to Siri on our Apple devices, and a human voice, programed to our liking by gender and accent, will talk back to us. And when we call all sorts of businesses, we are guided through various prompts by a human voice that is powered by voice activation software. Who knows, is it possible that some people can become smitten by these voices, like the protagonist in the movie "Her"?

Of course, we are not just dealing with voices coming in from out in the ether. Robot technology is developing at an exponential rate. And these robots do not have to be confined to unappealing, metallic creatures. Instead, they can be rather life-like. Indeed, will some of us start falling in love with robots that resemble human beings and that respond perfectly to commands without any hesitation? The protagonist in the move "Ex Machina" fell in love with an attractive, female robot; but unfortunately for him, she refined herself so that she ended up furthering her own self-interests to his detriment.

Getting away from the movies, people already in real life can order customized, full-sized sex dolls with complete simulated anatomy. There are arguments on both sides as to whether this is appropriate. Advocates in favor of the dolls say that these dolls ease the loneliness of single people in a way in which they do not take their urges out into the public in a way that in certain circumstances might be less than savory. Detractors argue that these dolls, that have no free will of their own, potentially encourage their users to objectify real people and to believe that they can do whatever they want with real people after their use of dolls.

So, what are we to do? Well, researchers and experts in technology and sexuality are going to discuss related issues at a conference scheduled to take place in Manchester, England in early September. The conference will focus on the most up-to-date theories and research on how humans engage with robots, artificial intelligence and other technology in exploring their sexuality, according to Observer.com. Topics to be included are: whether there can be true love and intimacy between a human and a robot; and, if sex robots encourage the objectification and oppression of women sexually.

It is unlikely that the conference will be the final word in addressing and trying to solve these issues. Indeed, it really marks the beginning of the conversation.

The Different Layers of the Internet

SEPTEMBER 14, 2016

http://blogs.duanemorris.com/techlaw/2016/09/14/the-different-layers-of-the-internet/

Most of us regularly use the surface level of the internet. But there are other deeper and darker levels. So, let's briefly explore three levels of the internet.

First, there is the "surface web." As you read this blog, you are operating on the surface web. When you access your email, when you tweet on Twitter, when you conduct Google searches, when you listen to Pandora, when you watch YouTube videos, when you buy and sell things on eBay, and when you shop on Amazon, you are utilizing the surface web.

This part of the internet probably is the most familiar to you, so you might think that it comprises the vast majority of the internet. Wrong! According to a recent blog by Vinay Kumar, the surface web comprises only 4 percent of the internet.

Second, we come to the "deep web." This part of the internet is not indexed and cannot by searched by Google or any other search engine. Apparently, as stated by Kumar, practically 96 percent of the internet is made up of the deep web. What is there? It is very common now for individuals and companies to save information in the cloud. This information can include text data, audio files, photos and videos. Unless purposely made publicly available, this information is not locatable through search engines. Probably it is a good thing that the deep web generally is not searchable, given that much of the content there is private and/or personal.

And third, there is the "dark web." This is a place on the internet where you really should not want to go. In the dark web, there can be the trafficking of guns, ammunition, illegal drugs, slaves, and other illegal items. Criminal activity of various types takes place in the dark web. Usual search engines do not lead to the dark web. Obviously, there are ways of getting into the dark web, but your faithful blogger (moi) has not looked into such access, nor would your blogger tell you about how to access this part of the internet even if he knew.

Be smart and safe out there! Hopefully, your life will benefit from the surface web in many ways, you will have private access to your personal information in the deep web, and you will say away from the dark web.

Are Election Systems Vulnerable to Upcoming Hacks?

OCTOBER 5, 2016

http://blogs.duanemorris.com/techlaw/2016/10/05/are-election-systems-vulnerable-to-upcoming-hacks/

One presidential candidate with the initials DT has claimed generally that "the system is rigged" and he has speculated in advance as to whether the election also might be rigged against him. At the first presidential debate, he did say that he would abide by the election result if the candidate with the initials HRC won the election.

But what does it mean to "win"? If the election result is a close one, and if she apparently tallies sufficient popular and electoral college votes to put her over the top, would he concede her victory if there are suggestions of hacking of voting systems? This question is posed because a recent Associated Press article asserts that hackers recently have targeted registration systems in greater than 20 states and cites a Homeland Security Department official for support for this assertion.

While at first blush this might fan the advance flames of controversy, federal officials and cyber security experts are reported in the article to have said that it would be "nearly impossible" for such hackers to actually change the outcome of the presidential election, primarily because election systems are "very decentralized and not connected to the internet."

Interestingly, the FBI just last month warned state officials to improve election security subsequent to hackers targeting systems in Illinois and Arizona. And the Director of the FBI said to lawmakers only last week that the FBI is looking "very, very hard" at Russian hackers who might consider trying to disrupt the election, according to the AP article. And while DT has voiced concern about the propriety of the upcoming election, the allegations from HRC have been that DT has been too cozy in his admiration for Putin of Russia.

The Department of Homeland Security has increased its efforts to educate states and localities about election handling, and up to now twenty-one states have shown interest in "cyber hygiene." DHS also is offering more in-depth on-site risk and vulnerability checks, but only four states so far have stepped up for such an assessment.

Earlier this month, according to the AP article, Rep. Henry Johnson, D-Ga, introduced two bills that would mandate that voting systems be designated as critical infrastructure, but this is unlikely to be passed before the presidential election. Such a designation would prioritize this sector as one for protection of its physical and cyber threats, like for other sectors in the areas of energy, financial services, healthcare, transportation, communications, and food and agriculture.

We are one month away. If the election is not close, any potential irregularities surrounding voting systems would not loom as large in subsequent discussions. If the election is close … Well, remember the Florida hanging chads from the year 2000? Fasten your seat belts, this may (or may not) be a bumpy ride.

The Emails That Came Back to Bite Clinton

NOVEMBER 22, 2016

http://blogs.duanemorris.com/techlaw/2016/11/22/the-emails-that-came-back-to-bite-clinton/

It is with regret that your blogger here must report that he was correct as far back as early-April 2015 in predicting that the private email scenario surrounding Hillary Clinton would be a real threat to her efforts to gain the White House. Indeed, in a podcast of April 9, 2015 this blogger described the problem as a "hornet's nest" that would be the "Achilles' Heel" of the Clinton presidential campaign.

As revelations of Ms. Clinton's use of a private email server for government affairs while acting as Secretary of State first emerged, she attempted to deflect and then minimize the problem. Later, when Emailgate would not disappear, Ms. Clinton admitted that she had made a "mistake" and that if she had it to do over again, she would not have handled government emails in a private fashion.

The April 9, 2015 podcast and contemporaneous writings by your blogger made plain that government records must be treated as such so that they are available for public review. For example, under the Freedom of Information Act, the public is entitled to seek information in terms of "what the government is up to," as has been held by the United States Supreme Court.

Why? For democracy to work, those who govern must be accountable to those who are governed, and therefore, government cannot operate in secret. Yes, the Freedom of Information does contain some exemptions to allow the government to shield certain records (such as to protect national security interests), but those exemptions are construed narrowly and the presumption is that government information must be available for review. But if government records are maintained in private, the purpose of the statute is thwarted.

During the campaign, Donald Trump supporters chanted "lock her up, lock her up" in response to Trump's many statements that Ms. Clinton had violated the law and that she should be prosecuted. But in July, FBI Director James Comey, while faulting Ms. Clinton in terms of how she handled government emails in private, stated that no reasonable prosecutor would bring an action against Ms. Clinton. It seemed then that the email problem largely was behind Ms. Clinton.

Of course, there were many warts that plagued the presidential campaign of Donald Trump. And when the election was close approaching, the national discourse mostly was focusing on allegations that Trump previously had groped women against their will.

But less than two weeks before the election, FBI Director James Comey dropped a bombshell by reporting that the private laptop of disgraced Anthony Weiner potentially contained emails between Hillary Clinton and his ex-wife and Clinton aide Huma Abedin. There was not any confirmation at all that such emails would shed any further light on Emailgate, but the genie was back out of the bottle.

Once again, the chants of "lock her up, lock her up" grew louder and louder. The entire narrative of the presidential campaign changed in the waning days from Trump's alleged, improper sexual predatory conduct back to Emailgate. A reasonable mind certainly could ask why the FBI Director came forward at all so close to the election with news that really was not news but that was very inflammatory.

Then, two days before the election, FBI Director Comey surfaced again to say that nothing contained on Weiner's laptop warranted changing his July conclusion that no legal action should be taken against Ms. Clinton. By this point, many people already had voted by absentee ballots. And we know that voter turnout was low, and very possibly potential voters who were considering voting for Ms. Clinton decided that she just could not be trusted after all; this was the theme played by the Trump campaign with respect to the email problem, and they did not show up in support of her at the polls.

This blogger believes that Emailgate was a substantial reason why Ms. Clinton is not the President-elect. One of Trumps campaign promises was that he would seek to put Ms. Clinton "in jail" if he were elected. Now questions are being asked whether he will follow through.

In a recent 60 Minutes interview, Trump said that the Clintons are "good people" and he does not want to "hurt" them. Hopefully, that is the case. Trump soon will ascend to the White House, and one would like to think that he has better things to do than to try to arrange for the prosecution of his political opponent, especially when the FBI Director concluded otherwise. But some of Trump's supporters truly hate the Clinton machine, and they may be out for more than an election victory. Again, hopefully that is not the case.