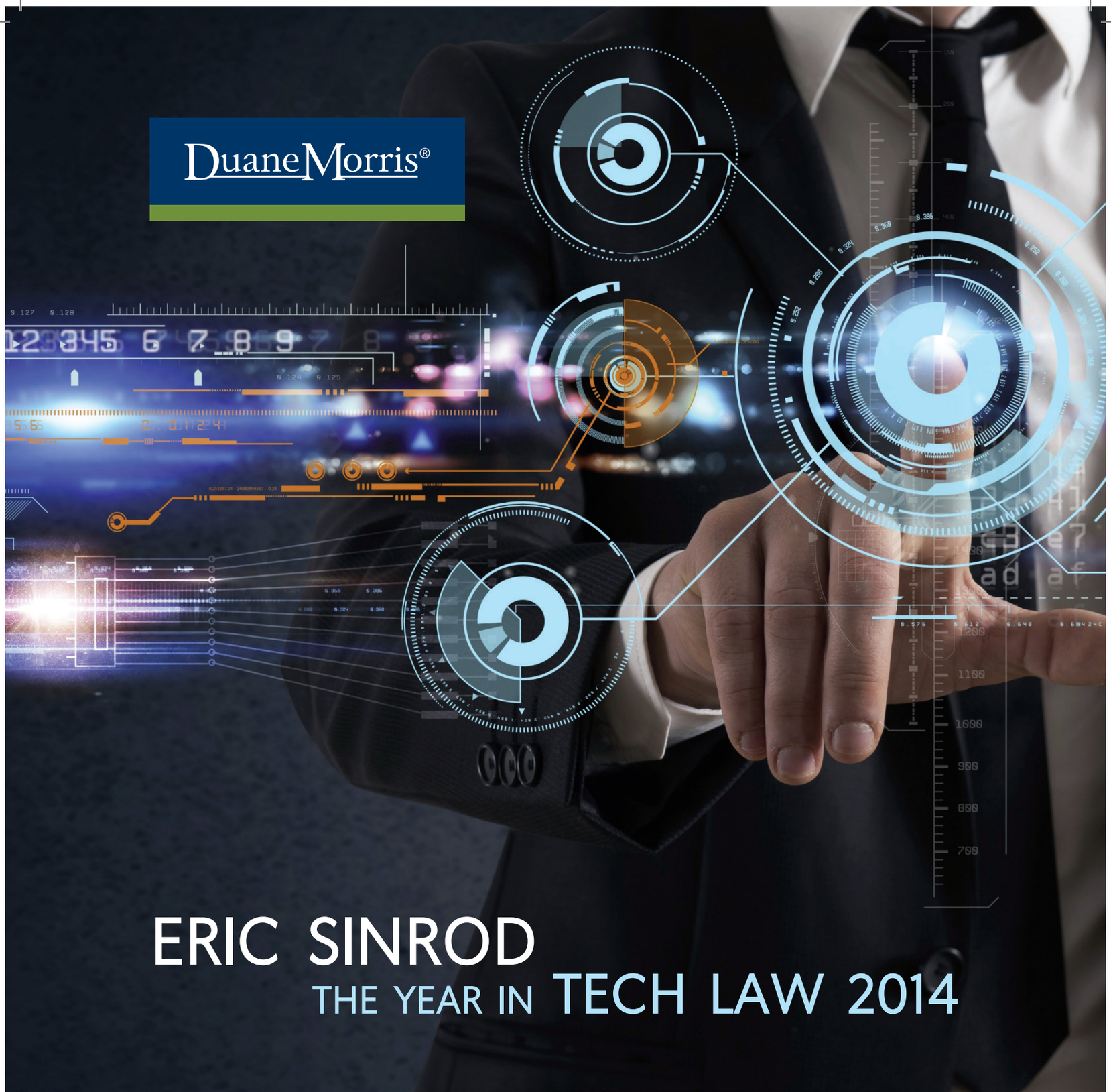

DuaneMorris®

# ERIC SINROD

## THE YEAR IN TECH LAW 2014

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

JANUARY – NOVEMBER 2014

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.*

# Veterans Day: One WWII Vet Lives Long and Goes Tech

November 11, 2014

Today is Veterans Day. We have much to be thankful for in terms of the valuable service dedicated to our country by our veterans. I want to take the opportunity in this blog to talk about one amazing veteran in particular.

Phil Economon just celebrated his 97th birthday. He still is going strong, working out in the gym, driving his car, and living independently in the house that he has owned for years. Phil is a dear friend and a mentor to me. On numerous occasions Phil has provided indispensable wisdom, counsel and advice to me, and to other people who know and count on Phil. Indeed, when in doubt, we always go by this mantra: "Do what Phil would do."

In World War II, Phil landed on Omaha Beach at Normandy. He was part of the Allied forces who marched across and liberated Europe. Phil is an American hero. Phil was honored this year by the California Assembly as the Veteran of the Year from his district.

Amazingly, Phil never was hurt in the war. However, on July 4th of this year, Phil was riding in a military vehicle as part of a local Fourth of July parade when someone inadvertently rolled up a window on his finger. So, about 70 years after landing on Omaha Beach, Phil in 2014 suffered his first World War II-related injury!

But that has not stopped Phil. He does has not let injury, or the fact that the rest of us in comparison are age-challenged, get in the way of his many pursuits.

And here is the tech angle, as this is a tech-related blog: Phil, who was born in 1917, regularly logs onto his computer and corresponds with his close friends by email. While Phil is surprisingly tech-savvy -- especially given that tech did not really even exist until many decades after he was born -- Phil still appreciates personal contact. Every day, Phil gets out and meets people face to face. He is a great believer in direct in-person communication.

Even though Phil has seen the ravages of war, he believes that the valiant efforts of those soldiers who fought alongside him truly saved the world. Nevertheless, Phil is the first to state that he believes in peace, and not war. He says that people operating from the goodness of their hearts will continue to lift this world up and to move civilization forward and better.

On this Veterans Day, let's honor Phil and other veterans who sacrificed for the rest of us. I therefore also honor my father Harold Sinrod, who served as a Captain in the U.S. Army in Germany soon after World War II; my uncle, U.S. Army General Bernard Waterman, who served with distinction during his lifelong military career; my uncle, Joseph Laskin, who, like Phil, landed on Omaha Beach and helped to liberate Europe; and my cousin, Frank Laskin, who was killed in Vietnam toward the end of his tour of duty.

Last but not least, you might be interested in Phil's secret for health and longevity. OK, here is the secret: a banana with peanut butter every morning!

# The Skies Are Still Friendly, Despite Virgin Galactic Crash

November 4, 2014

First, we took to the air by hot air balloon. Next, we went even higher via ever-developing aircraft. Astronauts then made their way into outer space and even to the moon.

And now, with the advent of Virgin Galactic, there has been the prospect of non-astronauts going into outer space in a new-age space plane. Indeed, more than 700 celebrity non-astronauts have reserved seats on Virgin Galactic with tickets costing $250,000 a piece.

Unfortunately, as we know, Virgin Galactic's SpaceShipTwo recently crashed in the Mojave Desert. It is easy to think that this calamity, along with prior notable aviation accidents, means that it is not safe to fly. Is that true? Read on.

**Prior Aviation Accidents**

The first fatal aviation accident actually occurred as long ago as 1875, with the crash of a hot air balloon near Wimereux, France. The balloon's inventor and passenger died as a result of the crash.

The first airplane fatality resulted from the crash of a Wright Model A plane that crashed in Fort Myer, Virginia, in 1908. Orville Wright, the co-inventor and pilot of the plane, was injured, but a passenger was killed in the crash.

The Tenerife disaster, which occurred in March 1977, still is the accident with the highest number of airline passenger fatalities. Indeed, 583 people died when two 747s collided on the runway; one had tried to take off without clearance and collided with the other that was taxiing on the runway.

As far as single-aircraft disasters go, the highest number of fatalities was the crash of Japan Airlines Flight 123 in August 1985. The aircraft experienced explosive decompression which destroyed the vertical stabilizer and all of the hydraulic lines, making the 747 incapable of being controlled; 520 people died because of this crash.

And the deadliest commercial aircraft crash here in the United States took place in May 1979, when American Airlines Flight 191 crashed near O'Hare International Airport because of the loss of an engine following improper maintenance. This crash caused the death of all 271 passengers and crew on board the plane.

**Aviation Safety**

This may sound bleak, but excluding the four aircraft that crashed during the 9/11 attacks, there have been only a total of 15 separate aviation accidents ever worldwide with a death toll between 250 and 499 people; and only the aforementioned two disasters with over 500 deaths.

Given that there are many tens of thousands of people in air every single day of every year and every decade -- from a percentage standpoint -- the number of fatalities from aviation accidents

has been incredibly low. Indeed, on a per-person and per-mile basis, air travel is consistently ranked as the safest form of transportation.

It is incredibly important to major manufacturers of aircraft, and to commercial airlines, that they offer a safe means of travel. Obviously, if airline travel were not perceived as safe by the public, people would not fly and these companies would go out of business.

The airline industry, as aviation technology has developed, has developed various safety devices such as evacuation slides, advanced avionics, engine safety features, and landing gear that can be lowered even after loss of power and hydraulics.

Yes, it is true that any life lost from an aviation accident, like the loss of the co-pilot of Virgin Galactic's SpaceShipTwo, is a tragedy. But generally speaking, the skies still are a friendly place to fly.

# Cyberwarfare Is Here; Is the U.S. Prepared?

October 28, 2014

Practically every aspect of life now takes place in cyberspace in addition to in the traditional world we know. While at first blush that generally may sound like a good thing, warfare now also takes place online as part of real conflicts, and not just in the realm of computer games.

**U.S. Strategy; Sectors at Risk**

As *The Wall Street Journal* has reported, U.S. military planning considers cyberattacks to constitute acts of war, just like traditional acts of war. Accordingly, cyberwarfare currently is part of U.S. military strategy, not only as part of cyber defense, but also as a platform for attacks. And prominent American lawmakers have been warning that the threat of a major attack on U.S. telecommunications and computer networks is greatly on the rise.

U.S. intelligence officials even have indicated that cyberwarfare, for the first time, is considered a larger threat than Al Qaeda and standard acts of terrorism. This is not altogether surprising, given that President Barack Obama has declared America's digital infrastructure to be a strategic national asset.

A number of critical sectors of the U.S. economy are at risk from cyberwarfare. These sectors include banking and finance, transportation, manufacturing, medical, education, and government -- all of which are dependent on computers and online communications and information for their daily operations.

**Some of the International Players**

*The Economist* has written that China plans on "winning" informationized wars in the 21st century. It also notes that other countries, such as Russia and North Korea, are mobilizing for cyberwarfare. And Iran reportedly claims to have the second-largest cyber army in the world.

Of course, in this climate, more and more U.S. taxpayer money is being poured into U.S. defensive and offensive cyberwarfare efforts.

**The Bottom Line**

It is imperative that cyberattacks on U.S. mission-critical and strategic systems be thwarted. Our air traffic control systems, for example, cannot be disrupted while we literally have hundreds of commercial and military planes in the air.

Likewise, just as in the context of traditional warfare, the United States needs the capability to attack in cyberspace for reasons of retaliatory self-defense, perhaps anticipatory self-defense, and when "just" wars might be necessitated as a matter of a "lesser of two evils."

# High-Tech Violations of International Human Rights

October 21, 2014

The United Nations was born in the aftermath of the atrocities committed leading up to World War II. The United Nations Charter is plain in its support for the development of international human rights protection.

The most fundamental human right is the right not to be killed by another human being.

Indeed, Article 6.1 of the International Covenant on Civil and Political Rights, for example, provides: "Every human being has the inherent right to life. This right shall be protected by law. No one shall be arbitrarily deprived of his life."

At times, the concept of the right to life has been at the heart of debates on the issues of abortion, capital punishment, euthanasia, self defense, and war.

Notwithstanding the United Nations Charter, and international conventions and treaties proclaiming the fundamental human right to life, unfortunately, too often people still are wrongly killed in many places in the world. (In addition, many people are enslaved and/or tortured in certain locations).

And in some ways, information technology has provided the leverage to take violations of fundamental human rights to yet another horrible level.

The recent ISIS beheadings of innocent people bring this point home. It would be bad enough for ISIS to execute these people as ISIS had done.

But ISIS has gone further by broadcasting the beheadings on the Internet to show the world the horror of these terrible deeds. So not only do the victims lose their lives in this process, but the rest of us, including families and friends of the victims, potentially witness the vicious killings.

While there are so many things that are good about information technology, regrettably, it also provides a platform for the truly malicious -- even the broadcasting of the violation of the most fundamental right to life.

# The Limitations of the International Court of Justice

September 23, 2014

The world is becoming a much smaller place given international transportation, multinational corporations, and Internet communications that know no geographic boundaries. With more frequent and heightened dealings with people across the globe, there necessarily are increased international disputes that require resolution.

So, one might think that there is a global court in place to deal with such disputes, right? We do have the International Court of Justice (aka the World Court or the ICJ). But can the World Court get the job done in terms of resolving the vast majority of international disputes?

Unfortunately, the answer is a resounding "no."

The ICJ is the main judicial branch of the United Nations, based in The Hague, Netherlands, and was established in 1945. The ICJ is made up of 15 judges. Each of these judges is elected to nine-year terms by the UN General Assembly and the UN Security Council. Elections are staggered with five judges elected every three years. There cannot be more than one judge from a given country on the court.

While not written in stone, it is understood that five judges will come from Western countries, three from African states, two from Eastern European states, three from Asian states, and two from Latin American and Caribbean states. The five permanent members of the UN Security Council always have one judge on the World Court. This means that the United States, Russia, China, the United Kingdom, and France always have a judge on the court (except when China did not submit a candidate from 1967 to 1985).

The ICJ can hear adversarial proceedings (referred to as "contentious cases") seeking to resolve active disputes (and the court can render certain, non-binding advisory opinions). But only states can be parties to contentious cases. This means that a tremendous number of disputes involving individuals, corporations, parts of states, NGOs, self-determination groups, and even UN bodies are beyond the purview of the World Court.

And even when it comes to states, the ICJ only has jurisdiction based on consent, not compulsory jurisdiction. Thus, if there is a dispute between two states, and one of the states has not consented to World Court jurisdiction by treaty, by specific agreement once the dispute has arisen, or by some other declaration, the ICJ cannot hear the case.

Not surprisingly, the World Court has had a relatively light caseload since it was created back in 1945. And without an overarching court to handle the massive number of international disputes, parties must bring their cases for resolution to domestic courts within states, or certain regional or specialty courts.

Thus, do not let the name "International Court of Justice" fool you. It is the rare international dispute that ultimately finds resolution by this judicial body.

# When It Comes to Tech, Size Matters

September 16, 2014

Big, small or in-between? When dealing with tech, it seems that there are preferences, and fortunately there options currently.

Long, long ago and far away, back in the disco days of the 1970s, the only available computer to me was a massive, computer punchcard-eating behemoth that appeared to take up the entire basement of my college library. While it was a floor-to-ceiling piece of junk by today's standards, size was not an issue -- because if you wanted to work on a computer, that was the only game in town. I declined.

Some years later, the personal computer was developed. Indeed, eventually CPUs, monitors and keyboards could be found in lawyers' offices. No longer were lawyers completely dependent on their secretaries/assistants for word processing and other functions. Lawyers were freed from dictation and hand-written red-lining of drafts of documents. Obviously, of course, this "new" technology, while a great advance, still did not allow for much choice when it came to size.

But then laptop technology developed. Computers became mobile. Lawyers could take their portable computers with them on the go. They could even use laptops during meetings/negotiations, and in depositions and in court. The first wave of laptops were fairly heavy and bulky. Over time, they became lighter and more nimble.

And once upon a time, telephones were wired into phone jacks. If you wanted to speak on the telephone, you essentially were tethered in place.

But, as we all know, mobile phone technology came onto the scene. The original mobile phones were unwieldy contraptions. Indeed, the large phone and its companion battery pack basically filled an entire carrying briefcase.

Long story short, the phones became smaller as did computers, and then there was the great convergence. Computers also became telephones and telephones became computers. All in one wireless device, practically every function imaginable now can be accomplished. Sure, documents can be created and phone calls can be made, but lawyers also can text, email, post, conduct research, make purchases, and organize in ways never before imaginable.

Enter the size issue. It seemed for a while, the smaller the device, the better. The more technology that could be packed into smaller and smaller devices, the greater the appeal. This represented progress. Lawyers at times moved away from laptops to their handheld devices.

But the smaller devices had tiny screens and felt cramped for some functions. As a result, rather than going completely back to laptops, tablets were developed. Tablets are not as big as laptops, but not as small as handheld devices.

If this were not enough, tablets themselves come in different sizes. And then handheld devices started coming in various sizes. Indeed, with other mobile phones offering larger screens in the marketplace, Apple's new iPhone 6 likewise can boast a larger screen than the iPhone 5 and prior iPhones.

Apple wants it both ways currently in the marketplace. Not only is it offering the new larger screen iPhone 6, but it also is coming out with its wrist wear Apple Watch.

And, of course, there is other wearable small technology available, such as Google Glass. Perhaps at some point we will have technology accessible in our contact lenses.

Cutting to the chase, when it comes to size, there are so many choices out there right now. Some lawyers may prefer to work primarily on their desktop computers, others may choose their laptops, and others still may like their tablets, while there are so many choices when it comes to the size of handheld and other devices.

One size does not fit all, and fortunately currently there is an abundance of choice out there right now.

# It's a Small World After All

August 26, 2014

It just is not realistically possible for countries to be isolationist in this current era. Indeed, the entire world is interconnected by the Internet and other technologies.

Consider this fact that shows how the world is becoming smaller as we group together even more closely: 3,000 years ago there were about 600,000 independent world communities; now there are fewer than 200 such communities.

And when a disease breaks out like Ebola in Africa, with our means of transportation, such a disease can show up and infect people in distant other places.

Here in the United States, we drive automobiles imported from Europe and Asia.

McDonald's serves nearly 70 million customers daily in 120 different countries.

Coca-Cola is served 1.7 billion times daily in essentially every country on Earth.

Starbucks, a relatively new company, is already present in more than 65 countries, and you even can order your nonfat decaf latte at the Great Wall of China.

Various countries currently are sitting on approximately 20,000 nuclear weapons -- the equivalent of 200,000 Hiroshima bombs. That is difficult to ignore.

And over 100 million people were killed in 20th century wars alone. Plainly, countries continue to fight with each other around the world and are not keeping to themselves.

Given all of the inevitable interaction between countries, disputes unfortunately are inevitable. But hopefully whenever possible, these disputes can be negotiated successfully so that further wars do not erupt and doomsday bombs never drop again.

# Wait, Now USB Devices May Be Unsafe Too?

August 12, 2014

Thumb drives, keyboards, and mice, oh my! That's right, these USB devices now may be the latest "lions, tigers, and bears" to fear in our high-tech world.

According to a recent Reuters article, such USB devices possibly can be compromised to hack into personal computers in a previously unknown form of attack that supposedly can side-step current security precautions.

As reported by Reuters, Karsten Nohl, a chief scientist at SR Labs in Berlin, has stated that hackers potentially can load software onto very small and inexpensive chips that control the functions of USB devices, but which presently do not have "built-in shields" that would prevent tampering with the devices' operative code.

Nohl states that one "cannot tell where the virus came from." He adds that it is "almost like a magic trick."

Nohl's firm has tested this out by writing malicious code onto USB control chips used in thumb drives and smartphones to perform attacks. Apparently, when a compromised USB device then is attached to a computer, the malicious software can cause all kinds of mischief, like monitoring communications, deleting data, and logging keystrokes.

Once a computer has become "infected," Nohl believes that it could be programmed to infect other USB devices that later are attached to the computer, which devices then would infect subsequent computers into which they attach.

And quite problematic is Nohl's claim that computers do not detect the "infections" when the compromised devices are inserted because current anti-virus programs do not scan "firmware" that controls the functioning of the devices -- instead they only scan for software written onto memory.

Nohl has speculated (and this appears to be pure speculation) that intelligence agencies like the NSA may be launching these types of attacks already.

Is this a real and present USB danger, or are Nohl and SR Labs together a lone voice in the wilderness?

Hopefully, this problem will not materialize, and if it does or if it is about to launch, efforts will be made to erect adequate security protections.

# Police Banner 'Ads' Warn About Potentially Pirated Content

August 5, 2014

Internet ads can be annoying. At times, for example, you may be seeking to read an article or watch a video clip online, but first you have to click off an advertisement that is in the way, or you have to wait out a video ad before you can watch the video content of your choosing.

Perhaps these ads once in a while may be successful in gaining your interest to buy the advertised products, but certainly most of the time these ads simply are a nuisance and a waste of time.

But (and there always is a "but") there can be Internet "ads" that truly are beneficial. What, really? Yes, really! So, what am I talking about? This:

According to BBC News, police in London have begun utilizing banner ads (so to speak) on websites that are suspected of providing illegally pirated content.

These truly are warnings, not so much ads, but they show up where paid advertisements otherwise would appear. One such banner warning reads: "This website has been reported to the police. Please close the browser page containing this website."

The purpose behind this London police approach is to prevent sites that to seek to benefit from pirated content from ultimately gaining revenue through Internet advertising.

"Copyright infringing websites are making huge sums of money though advert placement," the head of London's Police Intellectual Property Crime Unit said in a statement. "Disrupting advertising on these sites is crucial and this is why it is an integral part of Operation Creative."

Furthermore, these warnings would make the pirated sites look much less authentic to Internet users. Indeed, a warning about potentially pirated content certainly should cause an Internet user to have hesitancy about a site upon first review, rather than an authentic look and feel caused by an advertisement from a well-known brand appearing on the piracy site.

Overall, this is a laudable effort by London police, and hopefully it will help users steer away from piracy sites. Generally speaking, the more that can be done to provide clarity to Internet users in terms of site content authenticity, the better.

# Freedom of Anonymous Online Speech Has Potential Limits

July 22, 2014

It is very easy to communicate freely and anonymously on the Internet. And some people believe that if they do not use their real names and easily identifiable information, they can basically say whatever they want online, without needing to worry about the impact that their Internet speech may have on others.

Is this true? Read on, because the answer is not simple.

**Defamation Suits, Damages Are Possible**

Yes, the right to speak anonymously is within the ambit of freedom of speech safeguarded by the First Amendment to our Constitution. And courts have held that this right has been extended to Internet speech. So, are we done with the analysis? Can people say anything online without concern for repercussions? No!

To the extent speech (including Internet speech) is false and causes harm to someone else, there is a potential cause of action for defamation and recoverable damages.

The tricky part for the victim is not only proving defamation/damages, but also ascertaining the identity of the actual defendant/defamer when the online speech at issue has been anonymous (usually presented under a pseudonym). Without the ability to "unmask" the actual author of the communication, there is no point in further trying to pursue legal action. Thus, can the speaker's true identity be unmasked? It depends.

Often, the victim of alleged online defamation files a lawsuit against a "John Doe" defendant. From that defamation legal action, the victim/plaintiff then issues a subpoena to a third-party Internet Service Provider (ISP) seeking the true identity of the Doe defendant to insert into the defamation lawsuit.

The ISP usually notifies the actual online communicator of the issuance of the subpoena. The communicator who was the author of the Internet speech then has the ability to file a motion to quash the subpoena, arguing that his right to speak anonymously online would be compromised by the ISP revealing his true identity. If a motion to quash is not timely filed, the ISP then might go ahead and provide the identifying information.

When a motion to quash is filed, the battle is joined. The Internet speaker argues in favor of his anonymous speech rights, and the victim/plaintiff asserts that she has been the victim of defamation and that she will not be able to seek legal redress without obtaining the identity of the Internet speaker.

What happens next? The court is called upon to balance these important and competing interests. But how?

**'Unmasking' Doe Defendants**

Courts have fashioned different tests, but the test set forth in *Highfields Capital Mgmt. L.P. v. Doe*, 385 F.Supp. 2nd 969 (N.D. Cal. 2005), is fairly representative. In that case (in which I successfully represented the Doe defendant), the court created a two-prong test:

- First, it is incumbent on the plaintiff to submit competent evidence supporting each element necessary for the defamation claim (namely, falsity of the online statement and actual resulting harm).

- Second, if the plaintiff meets that initial burden, then the court has to decide whether the magnitude of harm that would be suffered by the plaintiff in the event of an adverse ruling would outweigh that of the defendant.

Clearly then, online communicators still have significant protections for their anonymous speech. But equally clear from the foregoing is that people cannot say whatever they want on the Internet and think that they can walk away free from all consequences. If an Internet communication is false about someone else (whether a person, organization or company), and if that false communication causes true harm, and that harm outweighs the harm of the Internet speaker's identity being unmasked, then unmasking will take place and legal action will continue to be pursued against the speaker in his true identity -- and the damages eventually awarded to the victim could be significant.

Free speech, and even anonymous speech, are vitally important. But there are limits -- and freedom of speech protections do not guarantee freedom to speak anonymously to the serious harm of others.

# Uber and Lyft Halted in Pittsburgh, for Now

July 8, 2014

More and more, people are migrating away from the traditional call-a-taxi model, and are instead searching on their smartphones for the closest Uber or Lyft vehicle. You might remember the Beatles' lyric "Baby, you can drive my car," and now Uber and Lyft drivers likely are singing to themselves, "Baby, you can ride in my car." Copasetic, right? Well, maybe....

Just when this new business model has been taking the country by storm, along comes a cease and desist order commanding Uber Technologies and Lyft Inc. to immediately stop operations in Pittsburgh, according to the *Pittsburgh Business Times*. The two judges who issued the order have ruled that Uber and Lyft cannot operate in Pittsburgh until they obtain the proper authority from the Pennsylvania Public Utility Commission (PUC). And to top this off, the judges have taken the position that the order prohibiting operations will not be stayed while this matter is reviewed by the PUC.

So what is going on here? Ultimately and fundamentally, the judges are concerned about public safety. While in their order they recognize that the transportation needs of the citizens of Pittsburgh are not adequately met currently, they believe that the PUC has a higher duty than public convenience -- namely, public safety.

The PUC has reportedly stated that its primary concerns relate to proper inspections, adequate insurance, and appropriate driver background checks. Uber and Lyft drivers do not currently maintain certificates issues by the PUC, allowing them to offer vehicle passenger service for compensation.

There are indications that Pittsburgh residents generally have welcomed Uber and Lyft in their community. To the extent that there truly have not been safety or insurance issues beyond that to be reasonably expected with traditional taxi service, it seems quite conceivable that the Pennsylvania PUC will work productively with Uber and Lyft coming up so that they can obtain the requisite certificates.

Uber and Lyft have the ability to file a response to the judges' order with the PUC, and the Commission will render its decision within the next several weeks. Interestingly, a spokesperson for the PUC has reportedly stated that the Commission will work with Uber and Lyft to obtain certification.

It thus seems that rumors of Uber and Lyft's ultimate demise in Pittsburgh are premature. While there has been a cessation of operations, do not count out Uber and Lyft in the Pittsburgh or any other market. This appears to be a business model with legs -- or more on point, with wheels!

# ABA: Lawyers Can Snoop on Jurors' Social Media Sites

July 1, 2014

urors always are admonished by judges not to conduct any independent factual research with respect to the cases they are considering. In this way, the rules of evidence will be adhered to and jurors will only be permitted to evaluate evidence deemed admissible and relevant by the judge.

But what about lawyers? How much sleuthing can they do with respect to the potential and actual jurors for their cases? Can they, for example, snoop on social media sites to learn more? Read on.

**Researching Potential Jurors**

We know that lawyers can conduct a certain level of research when it comes to potential jurors. For example, when I previously worked as a prosecutor, we were provided in advance with information relating to the geographic demographics of potential jurors, as well as their prior run-ins with the law.

Potential jurors from one part of the county were known as prosecution-oriented, while the opposite was true as to those from another part of the county. Also, potential jurors who had previously been arrested or convicted were not thought to be prosecution-friendly. Thus, during jury selection, efforts were made to maximize the odds of jurors who might be prosecution-inclined based on the foregoing information obtained.

An entire cottage industry has developed when it comes to jury selection. There are many jury consultants now plying their trade, and at times they even sit at counsel's table in the courtroom helping the lawyers decide whom to try to keep (or not keep) on the jury based on information such as gender, age, occupation, and other variables.

However, do lawyers (and their consultants) go too far to find out more by visiting the social media sites of potential and actual jurors? Somewhat amazingly, the ABA's answer is "no." Or put another way: Yes, social media sites can be checked out!

**Jury Consultants Will 'Like' This…**

Yes, indeed, the American Bar Association (ABA) has determined that it is ethical for lawyers to look at the publicly available social media posts of prospective and actual jurors. The only caveat is that the ABA cautions against lawyers actively friending or following these people or otherwise gaining access to them via private Internet spaces.

Perhaps the ABA's guidance is not all that shocking. Public information is public information and should not be precluded from use by lawyers in their jury machinations just because that information shows up on social media sites, some might argue. Others might take the position that even though some social media posts are publicly available, this just goes too far and is too invasive.

One thing is for sure, though, the depth and breadth of jury research will be exponentially expanded under this new regime. And this cottage industry might come more and more outside of the cottage. Plus, thorough jury research of social media sites could become very expensive, as social media searches can be very time consuming, with further time incurred leading to more costly jury-consultant bills.

At the end of the day, will information from social media posts lead to a better jury selection process? Not necessarily. If both sides to a case utilize this information, there could be nullification -- each side challenging the best potential jurors for the other side -- pushing toward a balanced jury in the middle.

# Internet Law Is All Grown Up

June 24, 2014

When I first started working on legal issues relating to electronic data, we were back in the dark ages of the 1980s. This was well before Bill Clinton talked about the coming "information superhighway" when he was running for president in the early 1990s. We were living in a world where document production in legal cases meant the production of actual hard copy pieces of paper and nothing else. There was no "e" when it came to "discovery."

As we all know, the technological communications age started to grow exponentially in the late 1990s and early 2000s. During this time, people began communicating more and more by email, cell phones, Internet chats, and website postings. Of course, where people flock, legal issues emerge.

When the Internet really started to flourish as a commercial and personal communications medium, the legal rules of the game were unclear and were fairly wide open. In some respects, these were the early "Wild, Wild West" days of the Internet, during which people were gobbling up domain names, for example, akin to the Oklahoma land rush of days of yore.

I have participated as a speaker and a moderator at the annual Stanford E-Commerce Best Practices Conference since its inception 11 years ago. It feels like those 11 years have been like a century in terms of the maturation of the field of Internet law. Truly, when the conference first kicked off, there was a feeling that together the speakers and participants were at the beginning of something important yet relatively amorphous.

Since then, so many high-tech legal issues have arisen and have been dealt with in terms of policies and practices adopted by companies, and by legislation and court decisions that have been of vital interest. But information technology keeps exploding out of the box at warp speed, and further new and different legal issues must be addressed.

Nevertheless, a true legal framework has developed over the past decade to address legal matters that arise in cyberspace. At the most recent Stanford E-Commerce Best Practices Conference that took place last week, speakers provided significant legal guidance with respect to the following issues, among others: digital copyright, cybersecurity, new content distribution models, patents in the high-tech arena and global IP protection, privacy protection and litigating privacy policies, virtual currencies and mobile payments, Web development, social media, geo-location tracking, cloud service and transactional issues, big data, domain name system expansion, data collection and retention (yours truly was the moderator and a speaker on this topic), as well as general counsel perspectives.

Interestingly, the most recent conference showed that there is a new generation of lawyers coming up -- those who essentially have known the Internet for their entire adult lives. To them, the current robust nature of Internet law probably comes as no surprise. But to some of us older warhorses, we remember a day, frankly not that long ago in real time (while eons ago in Internet time), when we really felt like we were mapping out the law in cyberspace on a fairly constant basis.

# Detoxing From Always-On Technology Overload

June 17, 2014

We now live in a world in which we constantly are connected electronically. We spend so much of our time in front of computers, laptops and tablets. Our smartphones can accomplish feats unimaginable not so long ago. These days we can even surf the Internet with smart eyeglasses.

Plainly, connectivity presents numerous advantages from business and professional standpoints. If that were not the case, people likely would not be so addicted to their instant electronic communications and access. However, does there come a tipping point when an individual just becomes bombarded with connectivity overload and truly needs a cleanse – a detox, if you will, from the always-on world? Perhaps once in a while each one of us, even if briefly, needs to harken back to an earlier time and just turn off and be present in the real world.

Case in point: my recent trip to Alaska with my family. There we were, on a ship, off the Alaskan coast, exploring incredible fjords and glaciers, and we had the choice to pay for expensive Wi-Fi ... or not. We actually considered this option for quite a while. Mind you, our daughters are 22 and 19, and they literally live on their hand-held devices. And, as I need to confess, I am a tech junkie.

But we bit the bullet, and we decided to forego the Wi-Fi connectivity option. What happened? Something amazing, actually.

I expected there to be serious withdrawal suffered by my family, replete with constant hand movements back and forth to lifeless gadgets and consequent withdrawal symptoms like twitches, shakes, irritability, confusion and ultimate depression. True? False!

Almost immediately, we all seemed calmer. Conversations lasted longer; indeed, they sweetly lingered. Not only that, but our uninterrupted family conversations were so much deeper and more interesting than usual. And when we went about our daily activities, we were so much in the here and now (Huxley would have been proud).

We truly arrived at connectivity detox when we canoed across a glacial lake in silence past icebergs and waterfalls as we approached a glacier. Trust me, nobody was thinking about emails, texts, or tweets. We were overwhelmed by the splendor and majesty of nature in all its glory. As our trip progressed, there did come a moment when I needed to access Wi-Fi for some important work and extended family matters. While that was necessary, I did have some regret, as by doing this I became a bit removed as compared to my wife and daughters.

Our trip, as all trips, finally came to an end. When we were at the Vancouver airport waiting for our flight home, it was interesting to see so many people hovering around the few charging stations provided so they could ensure that their laptops and devices were fully charged. God forbid if they lost battery power and connectivity! Maybe they would go through withdrawal from their connectivity addiction. Or more likely, they would simply take a breath and pay attention to their surroundings.

Long live tech -- and long live tech breaks!

# Cyber Insurance Becoming a Necessity for Online Businesses

April 22, 2014

This blog for years has highlighted the potential risks and liabilities presented by communications and activities on the Internet. The Internet provides the possibility of privacy violations, security breaches, intellectual property disputes, defamation, hack attacks, and even cyber warfare, among other threats.

So what should companies do to be as safe as possible as they conduct business over the Internet?

In addition to implementing security and protective measures, companies more and more are turning to cyber insurance policies in an effort to protect their exposure to Internet risks.

Indeed, according to a recent CNBC article, cyber insurance is now the fastest growing area of insurance. Companies buying cyber insurance policies increased a whopping 21 percent from 2012 to 2013, as reported by Marsh Risk Management. And companies seeking protection from major Internet risks also rose, as those companies purchasing coverage of at least $100 million increased substantially during this same time frame.

Cyber insurance certainly has not been around as long as more traditional insurance policies, such as homeowners, automobile, life and health insurance. Thus, these policies are not as standardized, and the terms of cyber insurance policies can be more likely to vary from one issuer to another. Therefore, care must be taken by a potentially insured company to closely review the terms of available cyber insurance policies to ensure a good fit for the risks faced by the company.

And while a company must be careful in analyzing the coverage provisions of a potential cyber insurance policy -- to ensure that the risks actually faced by the company would be covered -- equal care must be exercised in analyzing an insurance policy's exclusions. Why? Because what coverage provisions provide, exclusions may take away.

The Internet presents a brave new world, but at least cyber insurance can help mitigate possible risks faced by companies as they move forward in cyberspace with their business activities.

# WTO Nixes China's Restrictions on Rare Earth Exports

April 1, 2014

In early 2012, the United States sought a World Trade Organization (WTO) consultation regarding China's restrictions on the export of tungsten and molybdenum -- forms of "rare earths." These rare earths are raw materials that are used in the production of some electronics products. Subsequently, the European Union, Japan and Canada requested to join the consultation. China then accepted the request for a WTO consultation.

In support of the restrictions, China argued that they are related to the conservation of exhaustible natural resources. China also asserted that they are needed to reduce mining pollution.

The complaining countries strongly disagreed, arguing that the restrictions really were designed to provide protected access to the subject materials to Chinese industries.

China has imposed three different types of restrictions on the export of tungsten and molybdenum. China first has imposed duties on the export of the materials. Second, it also has imposed an export quota on the amount of those materials that can be exported in a specified time period. And third, it has imposed certain limits on the very enterprises that potentially may be permitted to export the materials.

The WTO panel in its recent report concluded:

1. That China's imposition of export duties violated China's WTO obligations;
2. That China's imposition of export quotas were not "even-handed" under GATT 1994; and
3. That China's trading rights restrictions breached its WTO obligations.

What is the moral of this story? Perhaps it is that while seeking to protect natural resources and preventing pollution are laudable goals, those stated goals cannot be used as justifications when in reality they are being used as a smokescreen to not engage in fair international trading practices.

# What's Up With Facebook's Acquisition of WhatsApp?

March 11, 2014

WhatsApp, a messaging service that is often used for international texting and other services, is about to be gobbled up by Facebook, right?

Well, that is Facebook's plan. Indeed, Facebook intends to fork over a hefty $19 billion to acquire WhatsApp. However, that is not the end of the story.

**Privacy Groups Try to Block WhatsApp Deal**

The Federal Trade Commission (FTC) has been contacted by privacy advocates -- the Electronic Privacy Information Center (EPIC) and the Center for Digital Democracy (CDD) -- in an effort to block Facebook's acquisition of WhatsApp, according to Reuters.

Why? Privacy advocates are concerned that there has not been sufficient transparency in terms of how Facebook plans to utilize the personal information of approximately 450 million users of WhatsApp.

WhatsApp previously assured its users that it would not use their personal information for advertising-related purposes. But EPIC and CDD are anxious that the personal information collected as part of this regime might be treated differently once it's in Facebook's hands.

**Should WhatsApp Users Be Worried?**

Facebook has more than 1 billion users and does indeed derive revenue from advertisements that focus on demographics like gender, age, and other personal characteristics. While Facebook has used its own users' personal information for ads, it is not clear yet, according to privacy advocates, whether Facebook would take that approach with WhatsApp users -- who were promised a different treatment of their data.

In response to the FTC issues -- which are unlikely to be resolved any time soon-- Facebook has said that WhatsApp will remain a separate company even after the acquisition, and that the messaging company will continue to honor its prior privacy guarantees.

If that is true, one would think that there should not be a problem. But the privacy advocates argue that Facebook previously has amended privacy policies post-acquisition, as supposedly happened after it acquired Instagram.

Stay tuned as we see whether the potential acquisition of WhatsApp by Facebook sparks an inquiry by the FTC, as requested by the privacy advocates.

# Is Facebook a Marriage Killer?

February 18, 2014

If you are married, you may wish to pause and consider how you behave on Facebook and other social media outlets. Why? Because as much as one-third of divorce filings in 2011 included the word "Facebook" within them, according to a report by ABCNews.com. And the numbers may be even higher a few years later.

On top of that, the article states that more than 80 percent of divorce attorneys report that social networking behavior is finding its way into divorce proceedings.

Facebook and other social media posts can be used to insinuate bad parenting, depending on the behavior displayed. They also can be referred to in an effort to suggest infidelity.

At times, Facebook and other social behavior is the last straw that breaks the camel's back in a marriage, according to the article. While one partner may have been enduring an unhappy marriage to a point, once the outrageous online behavior of the other partner is uncovered, the marriage crumbles.

Interestingly, some people have deactivated their Facebook accounts in order to preserve their relationships.

So what is the cart and what is the horse here? Does conduct on Facebook and other social media outlets simply bring home already faltering relationships? Or do Facebook and other social media outlets present an irresistible urge that results in bad behavior that otherwise might not occur?

The answer may depend on the specifics of particular relationships. But all that being said, if you value your marriage or relationship, you might want to think once, twice, and more than twice as to how you present yourself and act in the social media realm.

# If Cyberwars Erupt, Will Damages Be Recoverable?

January 28, 2014

Unfortunately, warfare has been part of the human experience for centuries and even millennia. Historically, wars were fought on the ground between individuals. Often, in more recent times, mass physical destruction has been caused from a distance, with bombs dropping from planes and missiles launched from remote locations.

And now, in the Internet age, wars can be waged electronically by purposely disrupting mission-critical systems of a perceived enemy state. Damages caused by such disruptions could be quite high, but there are potential international mechanisms by which such damages could be awarded.

**'Conventional' War Reparations**

To understand that point, let's use an example from the direct physical invasion of Kuwait by Iraq in 1990. As you likely will recall, Kuwait's oil fields were set ablaze, resulting in tremendous loss of oil assets and significant environmental harm.

The United Nations Compensation Commission (UNCC) was set up in 1991 as a subsidiary organ of the UN Security Council. Its mandate has been to handle claims and compensate losses caused by Iraq's invasion of Kuwait.

The UNCC's Governing Council has addressed six categories of Iraqi invasion-related claims: four for individuals' claims, one for corporations and one for governments and international organizations (which includes claims for environmental damage).

There have been claims made for loss of property, harm to and loss of natural resources, environmental damage, harm to public health and death. In total, the UNCC has handled nearly 3 million claims stemming from Iraq's invasion of Kuwait.

Amounts paid for successful claims are drawn from the UN Compensation Fund. This Fund is financed by a percentage of the proceeds created by export sales petroleum and related products from Iraq.

The UNCC has just authorized $1.03 billion to be made available to the Government of Kuwait as a result of the harm caused by the Iraqi invasion, according to a recent United Nations press report. This reportedly brings the total amount of damages distributed by the Commission to $44.5 billion with respect to the 1.5 million prevailing claims by individuals, corporations, governments and international organizations relating to the damages caused by the invasion.

**Redress for Cyberwar?**

Hopefully, a mass tragedy caused by a "cyberwar" initiated by one state against another will not occur. But, regrettably, it is a possibility.

If that happens, just like the UNCC was set up to process and redress claims relating to the Iraqi invasion of Kuwait, perhaps a similar subsidiary organ of the UN Security Council could be established to do the same thing in the aftermath of a major cyberwar event.

However, it could be more complicated and difficult in this latter context. What if the cyberwar event is not actually launched by a recognized state, but instead by a terrorist group? Even if the UN Security Council could set up a potential body to deal with the cyberwar's aftermath, how effective would it be, and would there be resources available (like revenues from Iraqi petroleum sales) to pay down claims?

Let's cross our fingers that major cyberwarfare will not erupt and that we will not have to find answers to these questions.

# Driver Not Culpable for Wearing Google Glass; Wait, What?

January 21, 2014

Google Glass brings the Internet right to your face. Indeed, it brings computer functionality to an eyeglass device. So now, you can frolic online literally while on the go.

Is that a good thing? Well, we already live our lives via all sorts of technology, including desktop computers, laptops, tablets, and smartphones. Do we need more? That can be debated in terms of the ramifications of living constantly in cyberspace instead of the here and now of the real world.

But what about safety? Do we want people operating motor vehicles and other types of machinery while potentially distracted by surfing the Web on eyeglass devices? Probably not in most instances. So, let's turn to a real situation, as opposed to theoretical hypotheticals.

Last week, according to The Associated Press, a San Diego traffic court addressed a citation that had been issued to a woman thought to be the first person in the U.S. who had been ticketed for operating a motor vehicle while wearing Google Glass.

Ultimately, the traffic commissioner held that the motorist was not guilty. Wait, what?

The commissioner came to this result because the motorist had been cited pursuant to a code provision that requires proof that the device actually was in use while the motorist was driving. In this case, the police officer did not provide such proof.

But warning everyone, the commissioner did conclude that the code does bar the use of a TV, video screen or similar device in the front of a car while moving -- something that could be broad enough to apply to Google Glass. Similar language may be found in existing traffic laws elsewhere. In addition, the AP reports that at least three states -- New Jersey, Delaware, and West Virginia -- have introduced bills that specifically would ban driving with Google Glass.

The question arises: How is proof to be presented showing Google Glass use while driving? Absent an admission from the driver, perhaps the device and/or records pertaining to the device would have to be analyzed to determine whether the device was being used at the time a police officer suspects motorist use while driving.

Long story short, legal considerations aside, please do not use Google Glass by driving. Indeed, perhaps it should not even be on your face while you are driving, so that you are not suspected of use and so that you are not tempted to use it then.

Just like texting can be a somewhat irresistible urge while in the car, Google Glass could be the same and perhaps even more dangerous. Also, the device might partially block a driver's side vision.