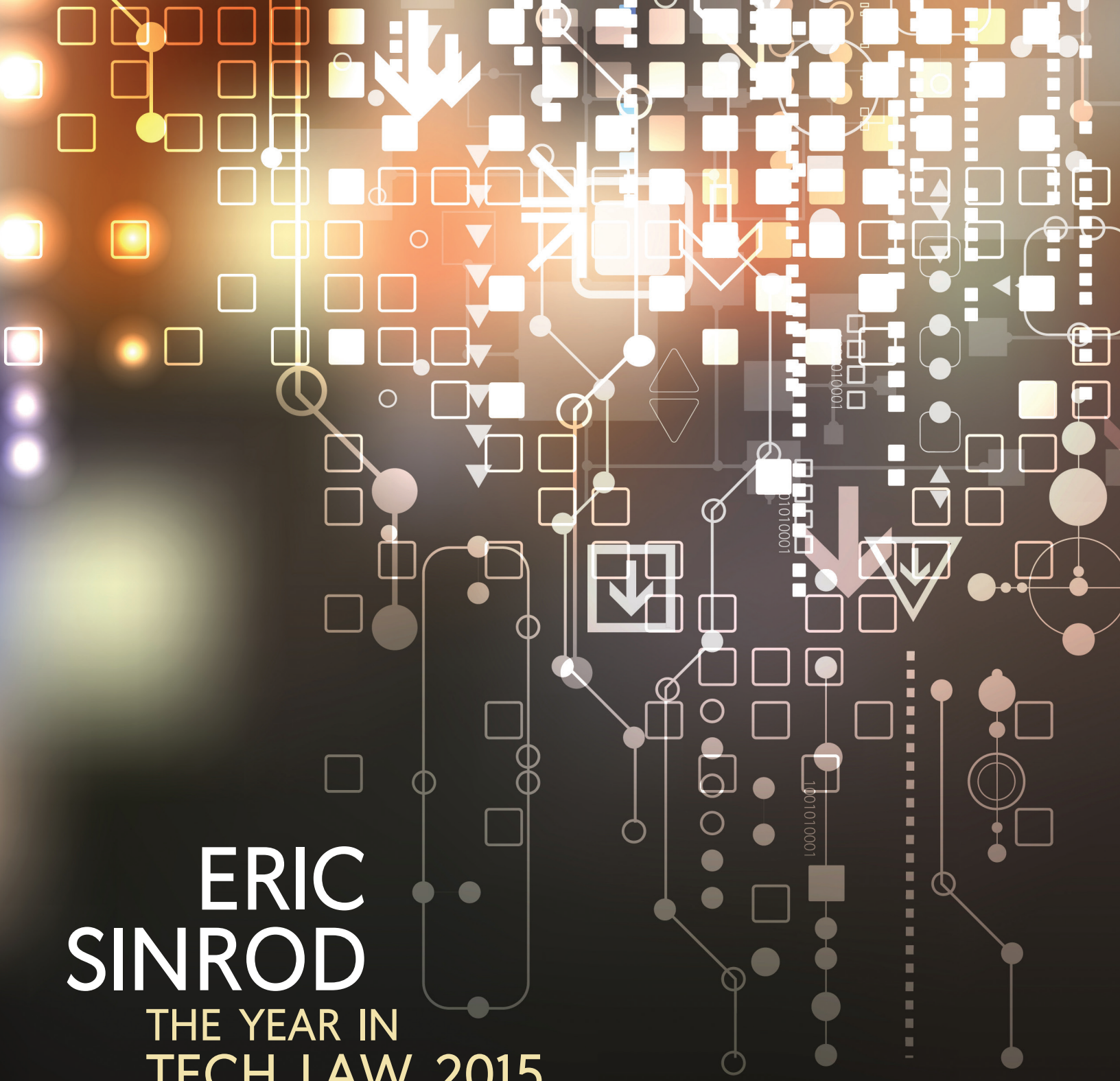

ERIC SINROD

THE YEAR IN TECH LAW 2015

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

JANUARY – NOVEMBER 2015

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.

DuaneMorris®

Table of Contents

About the Author 2

It's 2015: The Future Is Here for Legal Tech 3

Do We Need a 'Right to Be Forgotten' in the U.S.? 4

FTC Seeks to Thwart 'Revenge Porn' 5

Smartphones Can Do Anything, Right? 6

Fla. Agency Bans the Words 'Climate Change.' Really? 7

Be Afraid, Very Afraid Of Who You Meet Online? 8

Your Shopping Experience Is About to Get Even Easier 9

Internet-Connected Aircraft Potentially Subject to Hack Attacks 10

Selfie Sticks — Love Them, Hate Them, Ban Them? 11

Cyber Risks Are Here and Now 12

Drones, Drones Everywhere 13

Artificial Intelligence – The Potential Emergence of New 'Human Beings' 14

Self-Driving Cars — Are We Ready? 16

Adultery Gone Awry on the Internet 17

Twitter Faces Copyright Infringement Allegations 18

Cyberwar Happening Here and Now? 19

Online Adultery Leads to Cyber Warfare? 20

Hackers Are Coming After Your Private Data 21

Rating People 1 to 5 Stars on Peeple App — Yikes! 22

Government Censorship of Internet Speech 24

Facebook: The World's Largest Nation 25

Lawsuit Reveals Extent of FBI Internet and Telecom Surveillance 26

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.

It's 2015: The Future Is Here for Legal Tech

JANUARY 6, 2015

It may be hard to believe, but we already have closed the books on 2014, and we now have started making our legal way into 2015. The year 2015 at first blush sounds futuristic, and in many ways we really are living in the legal tech future we could have barely imagined not that many years ago.

When I started practicing law approximately 30 years ago, advanced technology meant that legal secretaries used mag cards in their electronic typewriters. When we conducted legal research, we actually went into the law library and cracked open real, hard-backed books. Once upon a time, it was a very, very big deal to receive a fax.

Back then, we used dictaphones to dictate letters, memoranda and briefs. When it came to document production, we actually met in conference rooms with opposing counsel and exchanged boxes of hard copy documents for in-person review. When we made telephone calls, we were tethered to the phones and phone cords at our office desks. And, of course, when we were working, we definitely were physically present at our law offices.

In what seems like a heartbeat, those days are gone.

Now, lawyers, and not just their secretaries, have all sorts of technology available to them 24/7. From our computers at work and at home, and via all sorts of portable and hand-held devices, we can perform practically every legal function in a nanosecond.

We can communicate electronically and wirelessly across various media, we can create documents and we can conduct electronic and factual research literally on the fly. No longer are we chained to our desks, which creates abundant flexibility. And we now have all sorts of creative technological ways to present evidence throughout legal proceedings and trials.

But all of these tech advances also present challenges. Just because we can perform legal functions faster than ever does not mean that we have more free time. Human nature is competitive. So, as one lawyer speeds up, so does the competition to keep apace. And work now can follow us everywhere, which creates true boundary issues between law and personal time.

We have just started with 2015. We are geared up with tech to make our legal year as productive as possible.

There will likely be more and more tech advances for lawyers. Will we be hyped up even more as a consequence? Or, can we collectively learn to use tech to work smarter in our legal practices so that we also have more satisfying personal lives?

The choice is for each lawyer to make. Choose wisely.

Do We Need a 'Right to Be Forgotten' in the U.S.?

JANUARY 20, 2015

Should our digital pasts always follow us around, or should we have the right periodically to wipe our digital slates clean?

The notion of "the right to be forgotten" has garnered quite a bit of attention in Europe, where privacy is more strictly protected than here in the United States. And while there have been some rumblings on our soil, perhaps now is the time for this notion to be taken more seriously in the United States.

The band Simple Minds in the 1980s had the famous song and lyric, "Don't You (Forget About Me)." Back then, before we played our lives out loud on the Internet, the fear was that an individual might not be noticed and might disappear into oblivion.

Fast-forward: We currently live in much different times. Practically everything is recorded for posterity. And this includes not just warm and friendly family photos, but also material that at the time may seem funny and perhaps edgy, and that later may came back to bite.

Imagine a teenager who posts online all sorts of photos, videos and comments related to alcohol consumption, recreational drug use, and her sexual preferences and activities.

In her early 20s, she becomes involved in fringe political groups and posts political rants far outside of mainstream views. She also makes online comments that are disparaging against certain industry groups and employers.

Now, she is in her late 20s, approaching her 30s. She has matured. She does not condone her prior conduct and views, and she wants to get on with her life to build a productive career and more seasoned social relationships. She wants to move on from what she now views as her immature past.

Can she? Or will she be haunted by the digital footprints from her earlier years? Does she have the "right" to say (unlike the song), "forget about me"?

Potential answers to these questions certainly will be explored more thoroughly going forward. Once upon a time, the past easily disappeared into the past and people could reinvent themselves as their lives progressed. This really does seem to be an important interest, and perhaps even a "right" that will need to be more fully mapped out.

In the meantime, with everyone now online, as I have said before, hopefully we will give others the benefit of the doubt in terms of what might show up from the past — we do all live in glass houses.

FTC Seeks to Thwart 'Revenge Porn'

FEBRUARY 3, 2015

While the Internet provides many obvious advantages to people in this digital age, it can also enable a dark side for those intent on mischievous and criminal online behavior. "Revenge porn" is part of that dark side.

So, what is revenge porn? It usually consists of a nude photograph or video which is publicly shared online (most frequently by an ex-lover of the nude subject) for the purpose of spiteful humiliation.

The nude photograph or video generally is recorded when the couple is in a positive relationship, and then later is shown to the world on the Internet after the relationship has crumbled, most often by the male posting nude content of his female ex.

There also are revenge porn ransom websites. Specifically, such a website posts nude photos and videos provided by ex-lovers of their former lovers, and then offers to take down the content if paid a certain amount of money. The Federal Trade Commission has been seeking to root out these types of websites.

As a recent example, the FTC took action against Craig Brittain, who allegedly operated a website from 2011 to 2013 that displayed nude photos of women; at the same time, he was accused of operating another site that enabled those women to pay between $200 and $500 to have the photos removed.

Brittain allegedly sought nude photos of women and their contact information, and also allegedly created a bounty scheme that offered financial incentives to provide nude photos of women and their contact information to him. Brittain allegedly received nude images of more than 1,000 women as a result of his efforts.

The FTC was able to achieve a settlement of its action. Brittain must destroy all nude images he obtained, and he is banned from sharing similar nude images in the future. Essentially, Brittain is out of the revenge porn business forever. Brittain was not forced to pay any fines.

Plainly, it is a good thing that Brittain will not engage in further revenge porn activities. And, the FTC certainly wants to make an example of him to prevent revenge porn by others going forward.

However, is simply stopping Brittain from further revenge porn without any other penalty enough to get the job done as a deterrent? Hopefully, others will want to stay clear of the FTC in this area; on the other hand, if the worst case in their view is that they simply will be forced by the FTC to stop, that might not be sufficient to deter their revenge porn behavior, unfortunately.

Smartphones Can Do Anything, Right?

MARCH 11, 2015

Once upon a time, frankly not that long ago, a telephone was something that was tethered by a wire to a phone jack and that enabled people to make telephone calls — nothing more. A home had one phone line, and perhaps multiple phones for that line.

Things became just a bit more interesting later when a home had more than one phone line. That meant, for example, that a teenager could stay up all night gabbing on the teenager's phone line without interfering with the ability of family members to make a phone call on another home line.

This still was a fairly simple situation. When we were out and about in the world, our phones did not follow us. Our communications tended to be more in-person, and perhaps we observed what was happening in the world around us with a bit more of a keen sense, without any technological distractions.

In the late 1980s, we witnessed the first "mobile" phones. These phones were behemoths. Such a phone and its battery pack literally took up a large briefcase to carry around. Other than the cachet of parading the fact of owning the behemoth mobile phone, it honestly was easier to use a pay phone when out of the home or office.

But in the 1990s and thereafter, mobile phone technology developed exponentially in terms of size, functionality, and convenience. And now, in a small device about the size of a pack of cards, or smaller, we literally have the world at our fingertips.

Today's smartphones, of course, allow for phone calls while on the run. But we can do so much more — so much more! We can search the Internet, communicate by emails and texts, engage in all sorts of social media outlets, take photos and videos, make financial transactions and purchases, make reservations at hotels and restaurants, make travel arrangements, check on the weather, obtain the news from various sources, listen to music, watch movies and TV shows, use a flashlight, view maps and get directions, use a compass — and the list goes on and on.

This, naturally, provides many benefits. People like to utilize the myriad functions offered by smartphones. On the downside, users may become more distracted and less in the real world. While smartphones can perform hundreds of tasks, they are not magic. They cannot do absolutely everything. For example, not too long in the past, customers were duped into paying for, and downloading, an app that was represented to cure acne. It claimed that, by holding a smartphone with the engaged app up to your face, the smartphone with the app ultimately would cure acne. But not surprisingly, there was no scientific proof that the app actually could accomplish that goal.

And very recently, the Federal Trade Commission announced enforcement actions against the providers of two apps that were represented to detect the signs of melanoma. Apparently, by taking a photo of a mole, the app on a smartphone could detect melanoma. The apps, called Mole Detective and Mole Detect, were on the market in 2011 and 2012 and could be purchased for up to $4.99. Obviously, the FTC does not believe the apps were accurately represented to the public.

So what is the moral of the story? The moral appears to be that smartphone technology will continue to develop as it has since its infancy. But while these phones can do more tasks than previously imaginable, if a function offered appears to strain your imagination, think twice before purchasing the app, lest you lose your money while gaining some potential embarrassment.

Fla. Agency Bans the Words 'Climate Change.' Really?

MARCH 17, 2015

It's baaaack. Florida, that wacky state that brought us hanging chads and other irregularities during the 2000 Bush v. Gore presidential election, has returned full force with some new controversy.

Indeed, while the great weight of scientific evidence has persuaded the vast majority of scientists skilled in the field that global warming is real and a looming danger for the planet, government officials at the primary environmental agency in Florida have been prohibited from using the words "climate change," according to Time.com.

The Florida Department of Environmental Protection (DEP) issued an unwritten directive to not use the words "climate change" or "global warming" in official reports and communications, claims the Florida Center for Investigative Reporting (FCIR).

Christopher Byrd, an attorney in the DEP's Office of General Counsel from 2008 to 2013, informed FCIR that "[w]e were told not to use the terms climate change, global warming or sustainability," and that "that message was communicated to me and my colleagues by our superiors in the Office of General Counsel."

Moreover, additional former DEP personnel reportedly told the FCIR that this unwritten directive was put in place after Rick Scott, who has rejected the argument that climate change has been caused by humans, took the helm as the governor of Florida in 2011.

In the humble view of this blogger, Al Gore won the state of Florida in the 2000 presidential election, based on the ruling of the Florida Supreme Court, and thus should have become president based on the Electoral College vote tally. And he won the national popular vote by approximately 500,000 votes. Gore, and his book "An Inconvenient Truth," have been at the forefront of global warming education.

Gore ultimately did not become president, as we know, because the U.S. Supreme Court overturned the decision of the Florida Supreme Court. Gore was not able to implement his vision for the environment from the White House.

And now, 15 years later, Florida government officials reportedly are seeking to pretend that climate change and global warming are not happening by eliminating these words from governmental reports and communications. Let's hope we are not living in an Orwellian world where government can try to invent "truth" based on words allowed or disallowed.

Eliminating words does not alter the unmistakable fact of global warming. Rather than retreat into denial, best efforts must be taken to save the planet. Leadership should come from government.

Where have you gone, Al Gore? A nation turns its lonely eyes to you.

Be Afraid, Very Afraid Of Who You Meet Online?

MARCH 24, 2015

Before the explosion of online communications, our world necessarily was smaller and who we came in contact with tended to people we already knew. Then our ability to reach out and communicate with others expanded dramatically and exponentially as we all started traveling at warp speed down the information superhighway.

We learned that not only could we interact with people locally, but with a few keystrokes and mouse clicks we could be communicating with people across the country and even in countries on the other side of the globe. Part of the fun was our ability to communicate anonymously, using pseudonyms.

We could be informal, we could be creative, and we could reinvent ourselves. Indeed, most of us probably remember the cartoon with a dog in front of a monitor and a keyboard that had a caption which read: "On the Internet, nobody knows you're a dog." Case law developed making clear that First Amendment protections extended to the right to speak freely and even anonymously on the Internet.

All well and good, right? Perhaps for the most part. The Internet has provided a medium that has led to many beneficial communications and interactions for personal, business, and other purposes. However, human nature is not always pure. From the beginning of human history, it seems there always have been some people intent on mischief and even violent behavior. And unfortunately, with the increased ability for people to contact others via the Internet, there also is a heightened possibility for such contacts to lead to terrible results.

A recent example brings this point home. A 26-year-old Colorado woman who was seven months pregnant recently placed a Craigslist ad for the sale of baby clothes. When she went to the home of a woman who answered the ad, the other woman allegedly stabbed her and cut her fetus out of her womb. The 26-year-old victim has had surgery and is expected to survive, but the unborn baby did not. The accused attacker had showed up at a hospital with the fetus asserting that she had had a miscarriage. The accused attacker is potentially facing charges of attempted first-degree murder, first-degree assault, and child abuse knowingly and recklessly resulting in death.

Prior to the Internet, it is less likely that a stranger like the accused attacker would have been able to communicate with the 26-year-old victim — meaning that they would have been less likely to meet and such a disaster might not have occurred. But we are in the online era, and there is no turning back.

So what is the moral of the story? Yes, there are so many advantages to life on the Internet, many of which have been chronicled in this blog over the years. But people must be careful and they must take prudent precautions. We must remember that we truly do not know those on the Internet other than our true friends and colleagues. If we intend to meet someone in person who we first met online, it is critically important to do so only when necessary, in public with other people around, and we should not supply highly private information like our home addresses.

This is not to say that all strangers on the Internet are bad or evil. Indeed, quite the contrary. But still, an ounce of prevention can be worth all the cure in the world in the rare event that we unwittingly are dealing with someone online with less than benevolent intentions.

Your Shopping Experience Is About to Get Even Easier

APRIL 7, 2015

Once upon a time, shopping was a time-consuming endeavor. We had no choice but to actually get out of the house and physically travel to different stores to buy what we needed.

Then, the online shopping revolution occurred. Rather than traveling out of the house, all we now need to do is move ourselves up to our computers, and the shopping world is at our fingertips. Practically anything can be purchased over the Internet from a multitude of different Web sites. And Amazon, for example, has sought to be a one-stop shopping site, where countless thousands of items are available for purchase at any given moment, from books, to apparel, to electronics, to furniture, to food, to toys — and the list goes on and on.

Now, Amazon seeks to start yet another online shopping revolution, with the recent unveiling of its Dash Button, according to Time.com. These buttons can be hung or stuck practically anywhere within the home. So, for example, if someone is running low on dishwashing soap, that person can simply push on the button near where that soap is kept — and magic — an order is sent to Amazon for a shipment of more of that soap.

The Dash Button is Wi-Fi enabled and connects to a smartphone using an Amazon app. The button reportedly allows purchasers to cancel orders within thirty minutes. More than 250 household products across more than a dozen brands that frequently need to be replenished are available currently as part of the Dash Button program.

When news of the Dash Button program first came out, there were some doubters who speculated that this was an April Fool's Day joke. However, an Amazon spokesperson reportedly confirmed to the Los Angeles Times that the Dash Button is for real. For now, however, even if real, it only is accessible to Amazon Prime customers, and then, only by invitation. But if those customers like Dash Button, we can expect its reach to grow.

So, how easy does shopping really need to be? At this rate, some day we only will need to think about what we want to purchase, and it will show up right away at our doorstep. Indeed, it may show up there delivered by a drone; Amazon reportedly already has received approval to test drones at low altitudes in a rural part of Washington state.

While this blogger certainly loves the ease and convenience of online shopping, there still remains the simple joy of getting out of the house and going to a store or market and shopping in the real world, not cyberspace.

Internet-Connected Aircraft Potentially Subject to Hack Attacks

APRIL 21, 2015

We keep hearing about new and different ways that data can be hacked in the online and wireless world. And, generally speaking, our concern tends to be that our personally identifiable information may be stolen and misused. But that may be just the tip of the iceberg when it comes to the negative consequences of hack attacks.

Indeed, the Government Accountability Office (GAO) now is concerned about the security of modern aircraft that are more and more dependent on the Internet, as reported by The Guardian. According to a recent GAO report: "Modern aircraft are increasingly connected to the Internet. This interconnectedness can potentially provide unauthorized remote access to aircraft avionics systems."

And the report goes on to state that cybersecurity experts interviewed by the GAO believe that "Internet connectivity in the cabin should be considered a direct link between the aircraft and the outside world, which includes potential malicious actors."

So connecting the dots, the GAO report appears to be saying that there exists the possibility of a flight being brought down by malicious hackers. If this truly is a possibility, all best efforts should be made to minimize this risk.

While the GAO report lauds the Federal Aviation Administration (FAA) for improvements in cybersecurity policies, it nevertheless states that there is the "opportunity for further action." With that being the case, further action should be taken forthwith.

Having personally identifiable information hacked is negative, but the potential of a hack attack bringing down an aircraft is truly unacceptable.

Selfie Sticks — Love Them, Hate Them, Ban Them?

MAY 5, 2015

The topic for today: selfie sticks. How do you feel about them — positive, negative or indifferent?

Let's backtrack a bit first with a brief history lesson.

Long ago, actually more than a century ago, self portraits usually were created when an artist looked into a mirror and then attempted to paint his or her likeness on a canvas.

That was well and good, perhaps — until photography came into being. The early versions of cameras were quite unwieldy, so if someone wanted a photo of him or herself, generally someone else would use the camera to take that photograph of the intended subject.

Fast forward a bit closer in time to now. Cameras became ever smaller and easier to use, to the point now that practically every smart phone is camera-ready at all times. And with these cameras no longer requiring the expense and time delay of film development, people can take photos willy-nilly of anything while on the go, and specifically, photos of themselves.

Of course, taking a photo of yourself (and perhaps others in the same photo with the backdrop of your choosing) requires holding your arm out as far as possible while trying as hard as you can to capture all that you can in the photo. But a human arm can only extend so far, so what can be included in the photo is limited, right?

Yes, until the recent advent of the selfie stick, which brings us current to the initial question posed in this piece.

First, what is a selfie stick? To the uninitiated, it is a small, compactable baton that can hold your smart phone on the far end. When fully extended, it can go out several feet past the human arm to take photos when its button is pressed on the handle. The selfie stick therefore allows a person to take a photograph of him or herself with others without concerns about cutting off the intended scope of the photo because a person's arm is just too short.

So, is this a good thing? Well, sure, in terms of allowing people to take these kinds of photos (and videos too). And probably most of us have seen some fairly interesting and perhaps entertaining photos that have been taken this way.

On the other hand, selfie sticks can get in the way of others. If you are at a beautiful spot or sporting or other event, do you want your view cluttered up with selfie sticks? Probably not. And do we want to further enable the self-glorification practices of other people? That might be their business, but still ... And, there actually can be an issue of safety. It is possible a person could turn around in a fairly crowded area only to be rewarded with someone else's selfie stick hitting him or her in the eye.

Maybe because of some of these reasons, Apple reportedly banned the use of selfie sticks at its June developers' conference, WWDC. These sticks also reportedly have been banned from other public venues and events, like the National Gallery in London, the Kentucky Derby, the Coachella music festival, Disney World, New York's Metropolitan Museum of Art, the Palace of Versailles, and English Premier League soccer stadiums.

Bottom line: Selfie sticks likely are here to stay, and while banned in some locations, they otherwise have their own time and should be used with discretion so as not to interfere with the enjoyment of others.

Cyber Risks Are Here and Now

MAY 12, 2015

The Internet provides an abundance of benefits in so many aspects of our lives. We have information at our fingertips. We are in touch with our family and friends in myriad new and different ways. We can make purchases from our computers and our phones, without the hassle of having to go to out to the store. And the list of benefits go on and on.

But that is not the end of our story. No, indeed. The Internet, unfortunately, also creates many risks and liabilities for us as well. Recent data suggest the following disturbing trends.

The vast majority of emails are not legitimate; most are spam.

There has been a many-fold increase in malicious Web links.

The average unprotected computer can become infected with malware within a matter of minutes.

Many tens of thousands of Facebook accounts are compromised daily.

The average security breach is not detected for months, creating ample time for such a breach to wreak havoc.

The most commonly used computer password is "123456" — which leaves much to be desired when it comes to personal security.

The majority of Internet users at some point will become victims of cybercrime.

A majority of companies have suffered at least one cyberattack with the past year.

The healthcare industry has been experiencing an increase in security incidents.

Power and utility companies are seeing a dramatic rise in security incidents.

Most corporate security incidents are perpetrated by insiders — usually employees leaving to form their own competing companies or who intend to go work for an already existing competitor.

The average cost of a corporate data breach is more than $3 million, so we are talking about real money in this context.

Ever ubiquitous mobile devices (smart phones and tablets) are the weakest security link.

Social media comes next as the next weakest link, and with more than 1 billion Facebook users alone, this presents a challenge.

And to top it all off, the vast majority of information security professionals believe that cyberattacks represent a credible threat to national and economic security. Cyberwar thus is not confined only to science fiction movies and novels.

There is no going back. We are living in the online world. But while we can enjoy the many benefits of the Internet, companies, government and individuals must be proactive, prudent and careful to minimize risks and liabilities.

Drones, Drones Everywhere ...

MAY 20, 2015

What are we going to do with all these drones? Indeed, drones are coming at us from all sorts of angles. As a consequence, law firms are even coming up with practice groups devoted to the legal issues presented by drones.

Let's explore just a few of the many issues that may arise from drones.

Drones, of course, have been used for military purposes. Not only can they be used for unmanned surveillance, they also can be implemented for military attacks. The question arises as to when the deployment of military drones is sufficient to constitute an act of war by one country against another. And the launching of drone attacks is not necessarily limited to countries, as terrorists and other groups also potentially could use drones for attacks.

Next comes the idea of drones delivering products purchased over the Internet. Imagine: With a few clicks you order your favorite book from Amazon, and before you know it, the book shows up at your front door, delivered by a drone. Is this practical and economical? We should find out relatively soon, as this idea is being actively explored right now. And if drone delivery of commercial products comes true, what will that be like? Will it be annoying and disturbing to have these little craft flying all over the place? Is it possible that people might try to shoot down or otherwise interfere with drones as they vent their frustrations? Will drones be messed with by thieves as they might seek to steal the products carried on the drones? The answer potentially is "yes" to all of these questions.

And last, but not least, comes the issue of privacy in the world of drones. Many of us have seen amazing and wonderful aerial photos and videos taken by drones. Drones are inexpensive and do not necessarily require pilots' licenses to get up in the air to record what is happening below. But because they are cheap to use and easy to navigate, drones could be used to follow people, spy on them, and peek in on them where not previously expected.

Once upon a time, for example, we believed that we had ultimate privacy in our homes. If you were changing your clothes in your third-floor bedroom, you might not expect anyone to be looking at you, especially if your bedroom window is not directly across from the window of another building. But now, conceivably, a drone could fly near your window, and take photos and video of what you are doing in your bedroom. Because of drones, do we need to lower our expectations of privacy? Or, do we need to fight where drones can go and what they are doing when they go there?

The possibilities as to what drones can do and the issues that may arise boggle the mind. Stay tuned — drones are not going away.

Artificial Intelligence – The Potential Emergence of New 'Human Beings'

JUNE 2, 2015

Perhaps by now you have seen the recent movie, Ex Machina. If you have not, suffice it to say, an Internet coder is drawn into an unusual experiment in which he engages with a true artificial intelligence (AI) being delivered in the form of an attractive female robot. Is this the stuff of science fiction, or is it possible that humans may transform themselves fundamentally based on human design?

Historically speaking, it was not that long ago that Homo sapiens were not the only human species walking the planet. Indeed, Homo sapiens existed contemporaneously with Neanderthals, and there were other human species along the way as well. As we of course know, Homo sapiens are the only currently surviving human species. But is that about to change? By way of our own ability to create and invent, are we about to change Homo sapiens, or at least some Homo sapiens, into yet a new form?

Since the beginning of the 20th Century, in some parts of the world, the life expectancy of Homo sapiens has been dramatically extended. This has come about as a result of the development of certain medications, medical and surgical techniques, safer water and food techniques, the provision of electricity and many other advances.

In addition, the ability of Homo sapiens to function has been improved by technological aids such as eyeglasses, contact lenses, hearing aids, and artificial limbs. At what point, however, might we become something different than true Homo sapiens? Are we getting close to the brink when intelligent design by Homo sapiens themselves (as opposed to intelligent design by a higher religious being) might replace natural selection in leading to a different and perhaps more evolved form of human species?

For example, working at the DNA level, geneticists already have been able to extend the life expectancy of certain worms by a factor of at least six. If this could be applied to current Homo sapiens, such beings potentially could live hundreds of years. Also, mice already have been engineered with greater memory and learning skills. Thus, there is the possibility that current Homo sapiens could be changed to live exponentially longer and with greater capabilities. At that point, would they still be Homo sapiens?

In addition to such biological engineering, Homo sapiens could arrange to have inorganic parts merged with their organic parts. Rather than just applying simple eyeglasses, contact lenses or even heart pacemakers that seek to perform the usual and expected bodily functions of Homo sapiens, imagine, for example, the utilization of bionic limbs that have tremendously greater power and flexible use than traditional limbs of Homo sapiens. Would these partially bionic humans still be part of the Homo sapiens species, especially when combined with biological engineering and nanotechnology?

When it comes to nanotechnology, Homo sapiens already are developing tiny nano-devices that can reside in our bodies to perform many functions, including eradicating cancer cells, battling bacteria and viruses, and opening arteries. And beyond that, nanotechnology experts are seeking to create interfaces between brains and computers; the Internet literally could be inside of these humans. Would they still be Homo sapiens?

It is possible that by way of biological engineering, the merging of inorganic with organic parts, and nanotechnology, a different, more advanced and longer lasting form of human "species" may emerge. And that species, if we are to call it that, very well could exist at the same time as Homo

sapiens as we know ourselves now. Why? Because it is very possible that only the wealthier Homo sapiens could embark down the path of further development, ultimately becoming something else, while leaving traditional Homo sapiens to continue to live as we do now – or perhaps worse off – as the gulf between the wealthier, stronger, longer living new human "species" and Homo sapiens widens over time.

Of course, many ethical and legal issues would be created if the history of the future unfolds as described above. Would all "people" really be created equal? Would the new humans be allowed to crowd out Homo sapiens by living longer and controlling more resources? The list of questions goes on and on.

Fasten your seat belts, as we move through a new history, whether as Homo sapiens, or something else!

Self-Driving Cars — Are We Ready?

JUNE 9, 2015

Many of us feel the need for control – we need to be behind the wheel when in a car. We do not like others to drive us, and when they do, we become the classic backseat drivers – constantly critiquing the technique of whoever is driving besides ourselves.

And then there is the issue of people beyond the wheel in other cars. So many people can be seen screaming in their cars and gesturing angrily at other drivers. This frustration sometimes boils over into true road rage, and unfortunately there have been instances of true violence that have erupted simply because of quarrels about getting cut off in traffic, road speed and other driving issues.

But is that all about to change? Are we willing to relinquish control and give ourselves up to self-driving vehicles? Technological efforts already are moving in that direction – but will that technology be embraced?

A good part of our American culture is built around the freedom provided by cars on the road. Perhaps we would be even more free if our cars drove themselves. Not only would we drive to and fro freely, but we also would be free from the actual task of driving. We truly could multi-task, and the idea would be that such multi-tasking would be safe. Rather than driving while dangerously texting, the car would drive itself and we could do practically anything else at the same time – be it texting, working, watching shows, or even sleeping.

What about safety, though? We certainly have witnessed many car accidents over the years, with a tremendous number of deaths and injuries resulting from human driving errors. So, the human driving baseline is not terribly high.

Would self-driving cars do better? Google's most recent Self-Driving Car Project Monthly Report indicates that its self-driving technology has made significant progress over the past six years. Since the start of the project started in 2009, Google's self-driving cars have driven in autonomous mode (meaning software is driving the vehicles) a total of 1,011,338 miles, currently averaging 10,000 autonomous miles per week on public streets. And throughout all of that autonomous driving, Google reports that there have been 12 minor accidents – none of which was caused by the self-driving car. For example, one self-driving car was rear-ended when stopped at a traffic light.

Of course, the logging of a little more than 1 million autonomous driving miles is not very much to draw from for definitive conclusions. That is tantamount to the life of only ten vehicles that log 100,000 miles apiece.

But still, these preliminary results are promising. When we realize that commercial aircraft largely fly themselves as a matter of technology, it is not beyond the realm of possibility to imagine automobiles doing the same thing. Who knows, in the future, people may look back on our current time like we view the horse and buggy days; they may find it difficult to believe that once upon a time people actually had to drive their own cars beyond simply plugging in their anticipated destinations.

Nevertheless, we get back to the issue of giving up control. It may take time for there to be such a paradigm shift that people readily will relinquish control of their automobiles to software. We already have enough trouble giving the wheel over to someone else; can we give it up to nobody in particular?

Adultery Gone Awry on the Internet

JULY 28, 2015

The Ashley Madison site declares on its home page that "Life is short. Have an affair." The home page goes on to state that "Ashley Madison is the world's leading married dating service for discreet encounters." The site also boasts "over 38,050,000 anonymous members!" But how anonymous are those members, really?

People engage in all sorts of communications and transactions on the Internet. Generally, they like to believe that their personal information is handled confidentially. For example, if someone buys an item from Amazon, she hopes that her name, credit card information, and address will not be publicly disseminated.

Once in a while, there are security breaches, and, for example, credit card information can be obtained and used by others, purchasing items for themselves and not the credit card holder. The harm in this context to the credit card holder usually is not great. Usually, the credit card company will not hold the credit card holder responsible for the purchase. The credit card holder normally will have to go through the hassle of having that credit card cancelled and a new one issued. But this simply is a hassle, and not that big a deal.

Let's now talk about a potential big deal. It has been reported that Ashley Madison, the site where millions of people go to arrange extra-marital affairs, has been hacked, possibly compromising the personal information of its many users.

A hacker called The Impact Team claimed responsibility for the attack. The Impact Team threatened to release customer information publicly unless the Ashley Madison site and another site, Established Men, are shut down on the Internet.

Undoubtedly, people who have used the Ashley Madison site are worried about public disclosure of their private information showing that they have used the site. Not surprisingly, Ashley Madison has been trying to assure its users that it is taking all deliberate steps to protect them and to take action against the hacker.

Ashley Madison has a statement on its site that reads in part as follows:

"We were recently made aware of an attempt by an unauthorized party to gain access to our systems. We apologize for this unprovoked and criminal intrusion into our customers' information. We have always had the confidentiality of our customers' information foremost in our minds, and have had stringent security measures in place, including working with leading IT vendors from around the world.

"At this time, we have been able to secure our sites, and close the unauthorized access points. We are working with law enforcement agencies, which are investigating this criminal act. Any and all parties responsible for this act of cyber-terrorism will be held responsible. Using the Digital Millennium Copyright Act (DMCA), our team has now successfully removed the posts related to this incident as well as all Personally Identifiable Information (PII) about our users published online."

Perhaps this hack attack will cause some people not to use the Internet to foster their infidelity. Maybe some will be deterred from such activities all together. Or, it is possible that some will carry on completely unfettered. And if personally identifiable information from the Ashley Madison site is disclosed, we might see an uptick in the divorce rate. It's possible that information from the hack could even be used as evidence in divorce cases.

Long story short, be careful out there in cyberspace.

Twitter Faces Copyright Infringement Allegations

AUGUST 4, 2015

Social media sites host many thousands of photos posted by people on a daily basis. An obvious issue arises as to whether and when these sites might be liable for copyright infringement with respect to any of the posted photos.

A recent case is worthy of consideration.

Kristen Pierson, a professional photographer who has won awards for her work, has filed legal action in California against Twitter, according to Wired, with respect to a copyrighted photo that was shared on Twitter.

The photograph at issue is of Herman Li, a guitarist for Dragonforce, a British power metal band based in London, England. Pierson allegedly submitted a takedown notice under the Digital Millennium Copyright Act (DMCA), and when Twitter supposedly failed to respond to the takedown notice, Pierson then filed her lawsuit.

While the account that initially shared the photograph apparently is not active any longer, the photo of Li remains on Twitter, as reported by Wired, citing TorrentFreak reports. Is this sufficient to create copyright infringement liability?

The key charging allegation in Pierson's complaint focuses on the point that her photograph was shared at all on Twitter. According to Wired: "A Twitter user or users copied the Infringing Image without license or permission from Pierson and on information and belief sent one or more Tweets publicizing or linking to it."

The case might boil down to whether Twitter actually failed to act on Pierson's DMCA takedown notice, as alleged. Under the DMCA, an Internet service provider like Twitter generally is not liable for copyright infringement with respect to content posted on its site by others to the extent that the ISP complies with a DMCA takedown notice.

Pierson's complaint reportedly seeks not only statutory and actual damages, but also a restraining order to stop Twitter in the future from hosting her copyrighted work.

It will be interesting to see how Pierson's case plays out.

Cyberwar Happening Here and Now?

AUGUST 11, 2015

Conflict has unfortunately been part of the human experience for thousands of years. In prehistoric times, rocks, sticks, and bones were some of the weapons of choice. Over time, humans became more sophisticated, utilizing knives, swords, bows and arrows, and eventually guns and cannons. Recent developments include nuclear threats and drone strikes.

There has been concern, rightly, that the Internet might provide a further means for waging war or dismantling the means of waging war by others. For example, a few years ago, Stuxnet, a computer worm, reportedly was launched by a U.S. and Israeli intelligence operation to attack and cause the tearing apart of programmable logic controllers of certain Iranian centrifuges that were designed for potential nuclear purposes.

And more recent news on this front has been quite disturbing. For example, U.S. officials reportedly have informed NBC News that Russia initiated a "sophisticated cyberattack" on the Pentagon's Joint Staff unclassified email system — a system which then was taken down for a couple weeks.

This "sophisticated cyber intrusion" happened in late July and impacted approximately 4,000 personnel employed by the Joint Chiefs of Staff. On the one hand, officials reportedly have said that it is not plain whether the attack was supported by Russia's government, but on the other hand, officials reportedly have stated that the attack "clearly was the work of a state actor." These officials emphasize that classified information supposedly was not seized, and that only unclassified accounts were compromised — hopefully, that indeed is the case.

Meanwhile, a month earlier, the Office of Personnel Management told the public that a database housing personal information relating to roughly 4 million current and former employees had been hacked. United States officials reportedly stated in private that this was the work of the Chinese government, even though the administration did not directly accuse China with respect to this attack. China has denied any suggestion of involvement.

It is true that even if Russia and China were behind these hacks, they did not perpetrate true military assaults — there was no physical harm caused to anyone that we know of at this point. However, if Russia and China so easily might be able to obtain sensitive information of U.S. government employees, this might not bode well. It is a depressing thought that Russia and China might develop the capability over the Internet to access, disrupt, or gain control of U.S. mission critical military systems and other systems that address the functions of nuclear power plants, air traffic control, the electrical grid, or water supply and distribution.

As Stuxnet demonstrated, we now live in a world where cyber attacks are real and cyberwars could cause immeasurable damage. These attacks could become greater in terms of potential harm, and thus the Internet will be a place where defensive efforts are put in place, even when defense goes on the offensive. Are these acts of war? Not in the traditional sense, but the protection of humans lives can be at stake.

Online Adultery Leads to Cyber Warfare?

SEPTEMBER 8, 2015

People who go online likely consider the risks involved with using the Internet. People who contemplate extra-martial affairs probably consider the risks of those activities, too.

And, people who go online to seek out extra-marital affairs likely are mindful of the compounded risks of such endeavors. But do they envision that online adulterous activities could lead to a type of cyber warfare? Probably not, but at times reality can be stranger than fiction.

By now, unless you have been living under a rock, you have heard of the hack attack on the Ashley Madison site. Long story short, Ashley Madison is a site that boasts many millions of "anonymous" users who can seek out sexual partners outside of their marriages, because "life is short." Unfortunately for the "anonymous" Ashley Madison users, the site was hacked, personally identifiable information was obtained, the identities of some of the site's users has been revealed, and there is the prospect that other Ashley Madison users will be unmasked going forward.

Obviously, the revelation of the identities of the Ashley Madison users can lead to negative repercussions for them. Plainly, their revealed use of the site might not stand them in good stead with their spouses and their families. Some employees could also lose their jobs for various reasons (e.g., violating the laws of their states that still make adultery an illegal activity).

But, you ask, how does all of this lead to cyber warfare?

Well, according to a recent report by CNN, foreign spy agencies, of countries such as China and Russia, are implementing huge database analyses to put together and cross-reference information obtained from cyber attacks such as the attack on the Ashley Madison site. Why would they do that? The point would be to exert leverage and to potentially blackmail U.S. federal employees.

How would this work exactly?

Apparently, thousands of federal email addresses have been leaked as having used the Ashley Madison site. If a country such as China or Russia could ascertain the identity of a federal employee whose email address was used on the site, that country could threaten to reveal that employee's seemingly adulterous behavior unless that employee did favors for China or Russia in return for not publicly disclosing his Ashley Madison usage.

Needless to say, this is troubling, especially as CNN further reports that U.S. government systems and private company systems remain vulnerable, and the Ashley Madison hack obviously is not an isolated instance.

None of this is to suggest that a foreign country is responsible for the hack attack on the Ashley Madison site. Rather, once a site like Ashley Madison is hacked and its data is out in the wild at least to some extent, that data can be leveraged by one country against another by making threats to government employees at risk of disclosure.

Hackers Are Coming After Your Private Data

SEPTEMBER 15, 2015

Is your personal data safe out there in cyberspace? This is the question so many people have been asking lately based on seemingly endless computer hacks. And, unfortunately, the answer to this question might not be what you want to hear.

In terms of recent noteworthy developments, unless you have been living in an isolated cave, you undoubtedly have heard about the Ashley Madison hacking disaster. The Ashley Madison hack does not only present a problem for the site's users who thought that their personally identifiable information would be secure, but it points to a larger problem beyond this one specific site.

How so? The passwords used on the site were encrypted and were supposed to be "uncrackable" according to the BBC. However, as further reported by the BBC, programming changes by Ashley Madison's site developers caused in excess of one-third of the site's passwords to be inadequately protected.

While the group that cracked these passwords has said that it will not share the decoded passwords, the BBC reports that this group has detailed its methods in cracking the passwords, such that other hackers could duplicate this work as to these passwords on the Ashley Madison site and elsewhere.

And, if supposedly secure passwords relating to the Ashley Madison site can be cracked, one would think that passwords used on various other sites could be hacked as well.

Hence, the answer to the original question appears to suggest that our data is not terribly safe in cyberspace, especially if even "uncrackable" passwords can be cracked.

Beyond that, Business Insider has just reported that hackers now are not only seeking data such as credit card and Social Security numbers, they also are seeking other personal information such as messages, photos, and health information for extortion and other purposes. Because of functions such as dating apps and health tracking services, not to mention social media, people now are putting all sorts of new and different kinds of personal information on the Internet. That information can be compromised by hackers.

So, the answer to the question is not a happy one. People should be careful about the information they share on the Internet and they should try to use reputable websites and apps.

But even those sites and apps can be compromised. In this day and age, we are living at least parts of our lives online, and there is no escaping the fact that our personal data can be at risk.

Rating People 1 to 5 Stars on Peeple App — Yikes!

OCTOBER 7, 2015

By now, most of us have grown accustomed to rating products on Amazon or services on Yelp, one to five stars. You might like knowing that the book you are thinking of buying on Amazon has been overwhelming rated five stars with many positive substantive reviews. And it might be helpful to learn that you probably should avoid a restaurant you were considering when most Yelp postings give only one or two stars with comments that tell you explicitly why you should go elsewhere. BUT . . .

How about websites that seek to review human beings in the same fashion as sites that address products and services???

Well, go no further. Coming this fall is an app called Peeple. The mission of Peeple, as stated on its site, is to provide "an app that allows you to rate and comment about the people you interact with in your daily lives on the following three categories: personal, professional, and dating." The purpose of such ratings and comments supposedly is to "enhance your online reputation for access to better quality networks, top job opportunities, and promote more informed decision making about people."

Wait, what? This is all about enhancement? Given that a person can receive one to five stars and comments about such star ratings, it is not hard to imagine that someone who receives a single star with comments justifying such a low rating will not find her reputation enhanced.

There certainly is room for mischief and potential liability here. Imagine a scenario in which a co-worker, an ex-"friend" or an ex-lover provides a one star rating with very negative comments about another person. If Peeple were to become the litmus test to assess human beings, that one star rating and those negative comments could cause significant reputation damage and other harm to the reviewed person. And if the negative comments backing up the one star rating were false, there could be potential defamation liability for the reviewer.

The mischief could continue in other forms — such as bullying, with concerted efforts to round up negative star ratings and negative comments to blackball a victim. There could be popularity contests, with people seeking to attract as many positive ratings and reviews for themselves.

Typically, Peeple, as an Internet service provider, would have immunity for the postings of others on its site, pursuant to Section 230 of the Communications Decency Act. However, to the extent Peeple becomes actively involved in facilitating and determining the speech to show up on its site, with editorial discretion, it is conceivable that Peeple could see its immunity diminish.

In addition, we already live in a world that can be dehumanizing. We have grown up with grades, test results, trophies, ribbons, rankings, and job titles. And now, if your essence, yourself, is summed up in a one to five star rating — well, you have been boiled down to one number to the point of possibly eviscerating who you really are as a full person.

Peeple suggests that its site should prevent online bullying because it requires users to be over the age of 21, to have a Facebook account, and to provide a true cell phone number. Still, it is not clear exactly how that would prevent all forms of bullying. This simply prevents anonymous reviews, but while that could help, some users still could engage in bullying tactics overtly or behind the scenes.

Users apparently are to be provided 48 hours to dispute negative reviews and ratings, and inaccurate reviews can be tagged for removal. But how Peeple will decide what to take off and leave on the site after a dispute is registered or a review is tagged is not clear. And again, the

more Peeple gets involved to the point of editorial discretion, it could lose its CDA Section 230 immunity.

So, all this being said, how many stars do you give to Peeple?

Government Censorship of Internet Speech

OCTOBER 28, 2015

Here in the United States, we like to think that we can speak openly and freely on practically any subject while on the Internet. But is that universally true across the globe? Not necessarily!

Indeed, headlines have made clear that certain governments are intent on blocking Internet speech when it is in the interest of those who are in power but not necessarily when it is in the interest of some members of the citizens in those countries.

For example, it has been reported that the government of Uganda has used surveillance technology to spy on and muscle opposition movements in the wake of the 2011 presidential election in that country.

And according to the BBC, the government of Uganda is on the verge of acquiring a new communications monitoring center in advance of the presidential election next year. There is fear that this center would be used by the governmental for censorship purposes.

As another example of potential mass government censorship, FOX News has just reported that Russia has been running tests to find out whether it can remove itself from the World Wide Web in order to block the information flowing to foreign countries.

The point here is that the Russian government apparently would like to be able to implement a mass online information blackout in the event of a potential domestic political crisis. The Russian government purportedly is seeking to ascertain whether the Internet would continue to work within Russia while its citizens would be cut off from the global Internet.

Of course, the Internet does not know geographic boundaries in and of itself, so it may be difficult for the Russian government to completely block out the rest of the online world. To pull this off, Russia would need to construct a back up infrastructure that creates a closed online system. Meanwhile, Russian officials deny any such effort has been taking place.

Repressive regimes have sought to quell the speech of dissidents throughout history, and long before the advent of the Internet. It therefore is not entirely surprising that attempted censorship by governments will continue in the online world. But, hopefully, the Internet will help to foster free speech and communication, and will not be a means of governmental surveillance on citizens.

Facebook: The World's Largest Nation

NOVEMBER 11, 2015

When contemplating the world's largest nations by population, China, India, the United States, and Indonesia might come to mind.

Indeed, their populations are currently estimated as follows:

- China: 1,355,692,576
- India: 1,236,344,631
- The United States: 318,892,103
- Indonesia: 253,609,643

But, are these truly the world's largest nations? Well, not if the Facebook nation is included.

Facebook, which started in a Harvard dorm only a decade ago, now reportedly boasts 1.55 billion monthly active users. Not only has Facebook surpassed China's population, given Facebook's annual growth rate of 14 percent, Facebook should have 2 billion users in less than three years from now.

And while it is true that Facebook is not a sovereign state like countries such as China, India, the United States, and Indonesia, it nevertheless is a giant to be recognized. Facebook users within states and across international boundaries can communicate, share materials and news, and can organize in many different ways.

Facebook's revenue is also formidable. In its most recent quarter, the company's revenue reportedly was $4.5 billion. This was much higher than the $3.2 billion revenue for the prior annual period. And net income increased to $896 million from $806 million from the previous year. Last but not least, Facebook reportedly has a massive $15 billion in the bank.

One definition of "nation" is "a large aggregate of people united by a common descent, history, culture or language inhabiting a particular country or territory."

Over time, perhaps Facebook truly will be recognized as the world's largest nation. Users truly are developing their own Facebook culture and way of interacting. And perhaps the common territory they inhabit will be understood as its specific social media place on the Internet.

Whether Facebook ultimately is deemed a "nation" is a matter of semantics. And while Facebook clearly is not a nation state/country, Facebook plainly is a force to be reckoned with.

Lawsuit Reveals Extent of FBI Internet and Telecom Surveillance

DECEMBER 8, 2015

While the federal government has wanted access to private electronic information pertaining individuals in its efforts to fight terrorism, the government at the same time has not wished to be transparent to the public about its information gathering techniques. This has been made fairly plain from the fruits of a legal battle that has spanned more than a decade.

The lawsuit resulted from the refusal by Nicholas Merrill, founder of hosted service provider Calyx Internet Access, to comply with a national security letter (NSL) that he received from the Federal Bureau of Investigation as far back as 2004, according to Reuters.

As reported by Reuters, a recent court filing from the lawsuit shows that the FBI has implemented secret power to force Internet and telecommunications companies to provide all sorts of customer information to the FBI. This information has included complete web browsing histories and online purchase histories of individuals.

NSLs reportedly have been in the law enforcement arsenal for some decades, but their breadth and frequency of use increased substantially under the Patriot Act that was enacted after 9/11. NSLs usually are sent along with a broad prohibition preventing companies from revealing the substance of customer information demanded.

BUT, the federal court in the Merrill case has held that the gag on the NSL he received should be removed. Hence, the revelation that the FBI has been seeking customer web browsing histories and online purchase data. Also revealed is that the FBI has been seeking IP addresses of people in certain communication chains and location information on cell-sites. The FBI reportedly responded in its court filings that it is not currently seeking location information pursuant to NSLs.

The chief industry complaint against NSLs is that they allow the government to spy on customers of Internet and telecommunications companies without sufficient transparency and judicial review. Indeed, Merrill himself has been quoted as saying that the release about government activities in his case is important because "the public deserves to know how the government is gathering information without warrants on Americans who are not even suspected by a crime."

Reuters reports that several thousands NSLs are sent out by the FBI annually and that at one point that number exceeded 50,000 NSLs in one year.

We live, unfortunately, in a world that includes terrorism. And as a result, we are learning the further extent to which our government is gaining access to our private Internet and telecommunications data in its efforts to combat terrorism. Hopefully, terrorism will be prevented while our privacy rights are not trampled to the point of causing us tangible harm.