DuaneMorris®

ERIC SINROD

THE YEAR IN **TECH LAW 2017**

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

JANUARY – NOVEMBER 2017

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.

Supreme Court Will Not Consider Backpage.com CDA Section 230 Case

JANUARY 18, 2017

https://blogs.duanemorris.com/techlaw/2017/01/18/supreme-court-will-not-consider-backpage-com-cda-section-230-case/

Section 230 of the Communications Decency Act (CDA) generally grants broad immunity to Internet Service Providers (ISPs) with respect to third-party content posted on the ISP sites. The legislative history behind CDA Section 230 makes plain that Congress intended for the Internet to flourish for businesses and the US economy, and that intent would be thwarted if ISPs had the onerous duty to police and somehow regulate information and communications posted on their sites by others the ISPs do not control.

Nevertheless, there have been efforts in legal cases to chip away at the broad immunity afforded to ISPs by CDA Section 230. One such effort is the recent legal case Jane Doe No. 1 v. Backpage.com, LLC.

This case was filed in federal court in Boston in 2014 by several young women who accused Backpage.com of having facilitated their forced prostitution. How? The allegation was that this happened via classified advertisements posted within the "escorts" section of the Backpage.com site. The plaintiffs alleged that they were "repeatedly forced as minors to engage in illegal commercial sex transactions" in Massachusetts and Rhode Island when they were as young as the age of 15 by pimps who advertised on Backpage.com, according to a Reuters article.

The case made its way up to the the United States Court of Appeals for the First Circuit. The First Circuit sided with Backpage.com, agreeing that the ISP was immune from liability under CDA Section 230 as to the classified advertisements posted by others on its site.

Undeterred, the young women plaintiffs, then sought review by the United States Supreme Court. They took the position, according to Reuters, that in this context CDA Section 230 improperly is relied upon to prevent enforcement of federal and state statues designed to thwart human trafficking, and that Section 230 even could be used to get in the way of attempts to stop racketeering and terrorism. The plaintiffs also argued that that Backpage.com is profiting from all of this, and thus should be responsible for this type of content on its site.

Nevertheless, the United States Supreme Court very recently declined to review the case, leaving intact the decision by the First Circuit in favor of Backpage.com under CDA Section 230. Had the Supreme Court accepted the case and then later ruled in favor of the young women and against Backpage.com, the ruling could have had potentially broad implications for ISPs. But, that did not happen, and this particular attack against Section 230 immunity for ISPs did not succeed.

Still, it is worth noting that Backpage.com has been in the cross-hairs of the United States Senate and has faced various civil lawsuits relating to alleged facilitation of sex trafficking, and in particular with respect to children, according to the recent Reuters article.

Protection of Climate Change Data

FEBRUARY 1, 2017

https://blogs.duanemorris.com/techlaw/2017/02/01/protection-of-climate-change-data/

The vast majority of scientists who have studied the issue have concluded that global warming is happening and that such warming has been caused to a large extent by humans. For that reason, not long ago, many countries signed onto the Paris Agreement on Climate Change in an effort to deal with this threat to life on the planet.

However, there is concern that plans to deal with global warming may be halted. Why? Because it appears that President Trump is bringing into US government people who reportedly have expressed doubt about climate change, or at least who have been in favor of less environmental regulations for businesses. Indeed, according to a recent report by Public Radio International, a Trump transition team member has said that new studies and data by EPA scientists will be put on hold.

In this context, some people are worried that environmental data and documents from the EPA and other government agencies may become no longer be available to the public. The Public Radio International report refers to Michelle Murphy, a Professor at the University of Toronto, as saying "we're worried that the incoming administration is going to remove data sets that are available now and make the inaccessible offline." And, "once they're offline, we don't know what's going to happen to them."

The Public Radio International report states that data sets have not yet been removed from government web sites, but that the word "climate change" has been removed from the White Houses official web site.

Based on the worry that important environmental information may become unavailable from the US government, Murphy and other academics in Canada and the US have begun attempts to back up data and documents from the EPA, as well as information from additional government agencies that address environmental and climate issues.

Murphy also has contributed in founding the Environmental Data and Governance Initiative that last month hosted a data archiving event at the University of Toronto. This reportedly is just one of other data archiving efforts, including such efforts in Philadelphia, PA and Ann Arbor, MI, that have sprung up in the wake of the Trump presidency.

Murphy has stated that she is concerned about a "war on science."

Stay tuned to learn whether her concern is well-founded and whether data preservation efforts were worth it to help protect the planet.

Subsidized Internet Use for Low-Income Customers to Be Stopped by the FCC?

FEBRUARY 9, 2017

https://blogs.duanemorris.com/techlaw/2017/02/09/subsidized-internet-use-for-low-income-customers-to-be-stopped-by-the-fcc/

Changes keep coming fast, and now nine companies that recently have been part of a program intended to offer subsidized internet access to low-income users have been informed by the Federal Communications Commission that they must not offer this service, according to a recent article by the International Business Times. This position by the new leadership of the FCC represents a complete pivot from a ruling only weeks before by prior FCC Chairman Tom Wheeler.

The explanation for this about-face, provided by Ajit Pai, the new head of the FCC, is that Wheeler's decision to give the green light for the provision of low-cost internet access constituted a "midnight regulation" passed during a lame duck session, as reflected in the IBT article. Indeed, Pai is quoted as stating that "these last-minute actions, which did not enjoy the support of the majority of commissioners at the time they were taken, should not bind us going forward."

Pai's decision arguably thwarts the FCC's Lifeline program. This program, initiated in 1985, offers $9.25 per month for low-income households toward the subscription of home internet service, and it offers a credit for mobile phone subscriptions. The Lifeline program serves 13 million low-income people, according to the IBT article.

Just two days before President Trump's inauguration, Wheeler, on January 18, granted approval for nine specific carriers to be part of the Lifeline program. And in 2016, under Wheeler, the FCC passed the Lifeline Modernization Order. This order extended financial benefits with respect to broadband internet. When the order was being considered, Pai opposed it, taking the position that it created uncertainty with respect to potential fraud.

In now reversing Wheeler when it comes down to the Lifeline program, Pai is quoted as saying that this reversal "would promote program integrity by providing the [FCC] with additional time to consider measures that might be necessary to prevent further waste, fraud and abuse in the Lifeline program," as reflected in the IBT article. Furthermore, the reversal is not necessarily final; there is a 30-day period for the FCC potentially to reconsider its decision.

Social Media and Attacks on Traditional, Investigative Journalism

FEBRUARY 21, 2017

https://blogs.duanemorris.com/techlaw/2017/02/21/social-media-and-attacks-on-traditional-investigative-journalism/

Once upon a time, we received news in traditional formats from finite media sources by way of newspapers, television, and radio. And the news we received from those sources did not vary tremendously one from another. The news just seemed to be the news. As Walter Cronkite closed on his CBS nightly newscast, "And that's the way it is" — in essence meaning, "Those are the facts."

Times plainly have changed. There are many sources of news. People can choose a news outlet that suits their own political preferences. For example, for someone of a conservative, Republican persuasion, Fox News might be the news outlet of choice. Fox tends to present the news more in line with that end of the political spectrum. And, of course, there are other news outlets that favor the liberal, Democrat end of the political spectrum. So what are the "facts" when the reporting of the same events can be interpreted very differently?

Social Media as "News"

The answer to this question is all the more important when we factor in the influence of social media when it comes to the news. Many millions of people now get their news from social media streaming. Facebook alone has more than 1.5 billion users. A substantial number of those users obtain their news from the daily Facebook feed. They also get their news from what is posted by their Facebook "friends." Practically anyone now can act as a newscaster — posting information and interpretations on events as they happen.

Is the "news" as posted on social media reliable? Not necessarily. This "news" is not vetted as it would be via traditional journalism. Often times, people just vent their opinions and create facts from those opinions. And worse, "fake news" truly occurs — for example, a number of intelligence agencies have reported that Russia and others attempted to influence our most recent presidential election by leaking or using social media to post less than credible information online. It probably goes without saying that this can have huge ramifications.

Plus, by being able to choose our own designer news — having the choice of what version of the news we want to receive based on our political stripes — there can be a greater divide between people of different political persuasions. We see what we believe and we are not aware of how others think and experience the world.

The Attack on Traditional Journalism

On top of all of this, traditional journalism is under attack. We have seen that a simple tweet from the President can send the world scurrying to ascertain whether what has been tweeted is truth or made-up "facts." And when it is pointed out that a tweet actually is not factually correct, the President accuses traditional media outlets as being "fake news" and his administration has

declared that the press is the "enemy" or the "opposition." The press is seriously undermined when it seeks to correct factual inaccuracies and then is accused of being the "fake news."

The press serves as one of the important checks and balances to protect democracy. But now traditional press must compete with social media, which allows people to live in their own bubbles and which thrives on immediate and sensational postings. And the traditional press is under attack by the executive branch of government.

Traditional, investigative journalism is time-consuming and labor-intensive. Such journalism with persistence and digging uncovered and reported on the Watergate scandal in the early 1970s. Such journalism is imperative now too, to make sure that those who are governed are governed properly by those in government. Indeed, without the press, it would not have been revealed that former National Security Advisor Michael Flynn communicated with Russia during the presidential campaign about the issue of sanctions against Russia imposed by former President Obama.

To get back to the original question of this piece, as a country we need to support the efforts of traditional journalism to make sure that we receive and digest true facts. We need to step out of our own social media "news" bubbles to see what is really happening and to learn the views of others with whom we do not always agree. Social media companies also should take efforts to provide news from reliable sources. And we should not tolerate attacks on the press by the government.

Rush Hour Traffic: Telecommuting Is Looking Better!

MARCH 1, 2017

https://blogs.duanemorris.com/techlaw/2017/03/01/rush-hour-traffic-telecommuting-is-looking-better/

Getting to and from work can be a time-consuming, irritating and productivity-sucking endeavor. Indeed, time wasted in the car certainly could be used for more enjoyable and productive activities than countless annual hours behind the wheel. Where rush hour traffic consistently is bad, telecommuting should be actively explored for appropriate employees.

TomTom has collected data in an effort to measure the worst rush hour traffic in 48 countries, and specifically within 390 cities in those countries. So what are the most recently measured worst cities for rush hour traffic?

Well, if you live in Los Angeles, you probably are not surprised to find out that your fair city ranks in the top 15 worst rush hour traffic cities in the world. To point a fine point on it, Los Angeles is the 14th worst city on the globe for rush hour traffic.

Perhaps that is bad news here in the US, but the good news domestically is that no other US city makes the top 15 list of worst rush hour traffic cities.

So, guess which city is at the top of the list of worst rush hour traffic cities? Drum roll please … Bangkok, Thailand!

Coming in at second, third, fourth and fifth are Mexico City, Mexico; Bucharest, Romania; Jakarta, Indonesia; and Moscow, Russia. The eighth spot also belongs to Russia — St. Petersburg.

Istanbul, Turkey comes in as the seventh worst city for rush hour traffic, and Santiago, Chile comes in at tenth.

What about the other spots, sixth, ninth, eleventh, twelfth, thirteenth, and fifteenth? They all belong to China! These poor rush hour traffic cities are: Chongqing, Zhuhai, Guangzhou, Shijiazhuang, Shenzhen, and Beijing.

The aggravation and loss of human potential, not to mention the expense of fuel and other costs, plainly warrant a deep dive into methods to have employees telecommute from home or from more locally convenient locations at least part of the time.

Obviously, efforts are being made in this direction in some areas; indeed, telecommuting practically was unheard of not that too far into the past. But more can be done.

Vote with your feet — keep them working from home or nearby if you can, to the extent you are living in a city where rush hour traffic is a burdensome and time-consuming ordeal.

Internet Freedom and Security Statistics Across Countries

MARCH 22, 2017

https://blogs.duanemorris.com/techlaw/2017/03/22/internet-freedom-and-security-statistics-across-countries/

All countries are not the same when it comes to online freedom and security issues. This is borne out by recent statistics published by Richard Patterson of Comparitech.

When it comes to the amount of freedom offered by countries on the internet, a scale of 1 to 100 is implemented, with 1 being the absolute best possible, and with 100 being the worst. While the United States comes in with a relatively low score of 18, the US is not ranked the most free. Indeed, both Iceland and Estonia have a very low score of 6, with Canada next at 16, then the US at 18. Other relatively free countries include Germany at 19, Australia at 21, Japan at 22, the UK at 23, and South Africa and Italy both at 25.

The countries that rank most poorly when it comes are internet freedom are: China at 88, Iran at 87, Syria at 87, Ethiopia at 83, Cuba and Uzbekistan both at 79, Vietnam at 76, Saudi Arabia at 72, Bahrain at 71 and Pakistan at 69.

While the United States offers a fair degree of internet freedom, that freedom does not necessarily translate to online security. For example, a whopping 66% of global web application attacks had US targets. Germany and Brazil are next, while each receiving only 5% of such attacks.

Along the same lines, the US, by far and away, is the country most affected by cyber espionage. The US had the highest rate of such espionage at 54%, with South Korea next, at only 4%.

And the United States is not as pure as the white driven snow when it comes to sources of of global denial of service (DDoS) attacks. Indeed, the second highest percentage of such attacks, 21.59%, originate from the US. And China is not far ahead in terms of being the highest attacks source, at 29.56%. The UK comes in as the third worst offender at 16.17%, and France is the fourth worst offender at 8.72%.

Obviously, the global internet is dynamic, and how countries handle their online presence can vary over time, so the picture painted above is subject to change. Hopefully, the United States will remain and even improve in terms of internet freedom, while protecting itself better from outside attacks and while becoming less of a source of attacks.

Human Rights in the Digital Age

APRIL 5, 2017

https://blogs.duanemorris.com/techlaw/2017/04/05/human-rights-in-the-digital-age/

Should you have human rights specific to the new digital age? The answer is a clear YES, according to Gerd Leonhard, the author of the new book titled "Technology vs. Humanity." Indeed, Leonhard sets out five potential human rights in what he calls a Digital Ethics Manifesto. So, what are these proposed rights?

5 Potential Human Rights

The first right is to "remain natural." What does this mean? This is the right to be simply "biological and organic." This translates into having the ability to work and function in society without the need to "deploy technology with, on or — most importantly — inside our bodies."

The second right is to be inefficient "when and where it defines our basic humanness." Here, Leonhard believes that we should have the choice to be "slower and less capable than technology." Why? Because we should "never make efficiency more important than humanity."

The third right is to be able to disconnect. This means that we should be allowed the choice to "switch off connectivity." Further, we should be able to "go dark" on networks and to be allowed to pause communications, tracking, and monitoring.

The fourth right is to be able to remain anonymous. Thus, we should have "the option of not being identified and tracked" by technology. Leonhard believes that "anonymity, serendipity, and mistakes are crucial human attributes we should not seek to remove by technological means." Leonhard's point here seems to tie into the notion of the "right to be forgotten" that is gaining traction at least in Europe.

The fifth right is to engage with people instead of machines. Here, Leonhard believes that companies/employers should not be penalized if they decide to use real people instead of machines in certain contexts, even if that is less efficient and more expensive. In fact, he posits that companies that utilize humans over machines should receive tax credits for doing so.

It is important to look at the adverse impact on humanity stemming from the rise of machines in the digital age. Leonhard's work is thought-provoking. But will the marketplace embrace his notion? The answer is probably not if the marketplace is left to its own devices – competition and efficiency/cost savings will drive decisions. However, if the human rights he asserts are embraced and supported by governments such that companies are not disadvantaged by employing humans over machines, there may be a chance. As of this writing, we are nowhere close to Leonhard's ideal.

Watch Out for Your Job — Artificial Intelligence Is Coming

APRIL 12, 2017

https://blogs.duanemorris.com/techlaw/2017/04/12/watch-out-for-your-job-artificial-intelligence-is-coming/

Artificial Intelligence (AI) sounds exciting in terms of what AI can do for humans; however, a more fully automated world comes with a price — many jobs lost that were previously performed by humans. This is especially true in specific employment sectors: sales, customer service, transportation, shipping/logistics and healthcare/legal paraprofessionals.

A recent article posted on Futurism.com walks through each of these sectors and how they will be impacted by AI.

Sales, Customer Service, and Transportation Go First

When it comes to sales, lead generation is critical in terms of profiling online behavior to discover viable opportunities. AI likely will take over to reveal the optimum leads for sales teams to follow.

As far as customer service, by 2020, it is predicted that 85% of customer service transactions could be handled by AI. This would happen because AI transactions would feel more human based on more advanced personalization.

Transportation could be revolutionized by AI. Every years millions of people are injured and many thousands are killed in traffic accidents caused by humans drivers. Self-driving cars will be available for consumers within the next year or two, and it is believed that they will be programmed better to avoid accidents. Moreover, delivery and long-haul drivers, as well as public drivers, ultimately may lose their jobs to self-driving vehicles.

As far as shipping and logistics, the handling of the management of route systems and delivery speeds, as well as warehousing and space allocation for containers and trucks, likely will be powered by AI — with humans losing jobs.

And when it comes to healthcare and legal paraprofessionals, they could lose jobs as AI robots become more capable of searching databases for potential legal and medical solutions.

So yes, AI is exciting in terms of what can be done for humans; however, along the way some humans will be forced out of jobs that they previously performed.

What You Might Not Know About Amazon

APRIL 19, 2017

https://blogs.duanemorris.com/techlaw/2017/04/19/what-you-might-not-know-about-amazon/

Sure, sure, like most of us, you use Amazon often to buy things online and have them delivered to your home without the hassle of actually having to go out to the store. So, given your buying familiarity with Amazon, you might think you know quite a bit about the company. But perhaps there is much more to know.

Indeed, in a recent book by Brad Stone, titled "The Everything Store: Jeff Bezos and the Age of Amazon," profiled by Business Insider, much is revealed that you might not know. (And yes, big surprise, you can purchase the book on Amazon).

So, you might know that when Amazon launched in 1995, it was a web site that only sold books. And you may know that from that early start, founder Jeff Bezos wanted Amazon to become the "everything" online shopping experience. But getting on to more obscure facts: Bezos originally wanted to name the company "Cadabra." Ultimately, he was convinced otherwise, because that sounded too much like "cadaver."

In the beginning, whenever a purchase was made on the site, a bell would ring. Could you imagine that happening now? The Amazon office workers would go deaf from constant bell ringing.

Here is an ironic surprise — early on, Bezos, his wife, and the third company employee held meetings in a local Barnes and Noble.

Bezos back in the day, believed that employees should work at least 60 hours per week. This one may be a bit less of a surprise. But suffice it to say, the concept of work-life balance was not embraced.

Amazon was caught flat-footed by Christmas season 1998 — not having enough hands on deck to deal with online orders. Going forward, it was vowed that there never again would be insufficient labor to deal with demand; and hence, the later hiring of seasonal workers.

Did you know that Amazon tried to launch its own "auction" site to compete when eBay came into its own? This represents one of Amazon's failures.

Prior to Google's Street View, Amazon started a project called Block View. Amazon dropped this project in 2006, and then Google ran with Street View starting in 2007. This is another failure of Amazon, among many successes.

Here's one for you — in the early 2000s, Amazon's operations manager encouraged employees who had reached important goals during the tense holiday season to let rip primal screams to ease tension.

You may use a Kindle, but that was not the originally contemplated name for the device, which instead was "Fiona," based on a character in a futuristic novel. However, "Kindle" prevailed given its suggestion of starting a fire.

Finally for now, apparently Bezos was very harsh at times with employees and could be quite explosive. Accordingly, it is rumored that he hired a coach to help him with his tone.

Did you learn anything new?

Busted by a 'Textalyzer'?

MAY 3, 2017

https://blogs.duanemorris.com/techlaw/2017/05/03/busted-by-a-textalyzer/

Let's face it — many of us are addicted to our tech gadgets. We constantly have to check our smart phones for all sorts of communications and updates. Of course, this can be problematical, especially when we might want to reach for our handheld devices while driving our cars. Indeed, texting while driving can be rather dangerous; it is difficult to focus on your driving while looking down into your phone to text.

But if you manage to text while driving without causing an accident, are you out of the woods? Not necessarily. And what if you are involved in an accident? Well, you may be busted by a "textalyzer."

So, what Is a Textalyzer?

A textalyzer reportedly is modeled after the Breathalyzer and is to be used to ascertain whether a person has been using a phone illegally while driving. And according to NPR, legislators in New York and a few other states and cities are weighing whether to implement the device to "crack into phones" because far too many people are texting while driving and causing many accidents as a consequence.

Without a textalyzer, it can take months to obtain phone records through the legal process to pinpoint when and how a particular phone was being used at the same time as a person was driving and may have caused an accident.

Enter the textalyzer, developed by a company called Celebrate, as a potential solution. This is how the textalyzer is used: a police officer simply approaches the driver of a vehicle, the officer connects the textalyzer to the driver's phone, and with the tap of one button in about 90 seconds the textalyzer will show that last activities on the phone with time stamps. Thus, in theory, the textalyzer could show right away whether someone was texting on a phone while driving and possibly causing an accident.

Apparently, the textalzyer is not yet ready for prime time, and efforts will be made to tailor the textalyzer to applicable driving laws in different jurisdictions. Importantly from a privacy standpoint, the textalyzer should not download the actual content of communications; instead, it will show which apps and functions were in use at specific points in time. And it should detect if the hands-free function was in use, which may satisfy certain legal requirements.

So, stay tuned to find out if textalyzers will be coming to law enforcement near you. But rather than wait to adjust your driving habits — please do not text or use your smartphone in an unlawful manner.

Global Internet Access for Everyone?

MAY 10, 2017

https://blogs.duanemorris.com/techlaw/2017/05/10/global-internet-access-for-everyone/

Since the internet expanded beyond the narrow confines of the military and a few educational institutions and became a more general phenomenon, there has been concern about the internet haves and have-nots. There has been talk about the digital divide — meaning those who already have greater resources will get further ahead by virtue of internet access, leaving those without resources and access even more behind and in the dust. Well, is that about to change?

In a recent Senate committee hearing, SpaceX explained plans for building a global internet network. The foundation of the plan is the deployment of in excess of 4,000 satellites into orbit. And this is not just idle talk by SpaceX. Indeed, the company completed an application to the FCC in November and reportedly is motivated to proceed with its plan, according to an article by Futurism.com.

Yes, many people around the world already are connected to the internet — more than 3.77 billion people. But we have a long way to go, as approximately 3 billion people still do not have internet access, as set forth in the article.

To add more detail with respect to the plan for global connectivity, SpaceX, Elon Musk's company, filed an application with the FCC to create a high-speed, global internet network by launching as many as 4,425 satellites — more than all satellites presently in orbit. SpaceX would like to launch the satellites between 2019 and 2024; they would be launched into space in batches using the company's own Falcon 9 rockets.

SpaceX certainly is ambitious and Musk is a known innovator. We shall see what happens next with this plan.

Meanwhile, as the article points out, SpaceX is not the only company interested in increasing global internet service. Facebook reportedly is implementing tremendous, solar-powered drones to expand internet access to otherwise unreachable parts of Earth. And AT&T seeks to send WiFi via existing power lines.

We may be in the brink of substantially closing the digital divide. Given that so much of global activities now take place online, it is important to ensure internet access for all who are interested.

Are You Dealing With a Real Person or AI?

JUNE 15, 2017

https://blogs.duanemorris.com/techlaw/2017/06/15/are-you-dealing-with-a-real-person-or-ai/

Perhaps you saw the movie "Ex Machina" a couple years ago. In that movie, a male internet coder was drawn into an unusual experiment, as he engaged with an Artificial Intelligence (AI) being provided in the form of a very attractive female robot. Is this the stuff of science fiction, or are we already dealing with AI, even when we do not know that is the case?

Generally speaking, we hopefully know that we are not dealing with a live human being when we talk to Apple's Siri or when dealing with Amazon's Alexa. However, according to a recent article by Forbes, we often interact with AI unbeknownst to us. For example, we probably do not think about the fact that AI controls Google's searches for answers to our questions, and AI also controls how Gmail and Outlook know which emails to put in our spam folders.

And you probably have received phone calls when the "person" on the other end of the line sounds like a live human, only to realize that you are talking to an AI system with a life-like human voice. Indeed, when we call businesses of various types these days, we first are directed through a number of prompts by automated voices before we might be able to get to a live human.

As the Forbes article points out, a recent study of 6,000 consumers by Pegasystems revealed that when asked the question "have you ever interacted with Artificial Intelligence technology," 34% responded yes, 34% responded no, and 32% said that they did not know. BUT, the actual fact is that 84% had interacted with AI. This means that practically a whopping half of respondents had interacted with AI without having such knowledge. This appears to show how seamless AI has become in our lives.

Is this a good thing? Well, 70% of respondents have a fear of AI, and 25% of respondents even fear that AI might "take over the world."

At this point, AI assists us in various aspects of our lives. Whether AI actually will become a true threat to humans in the future, we might have to stand vigilant to make sure that AI does not become so intelligent that it someday might seek to further its own interests ahead of the interests of humans.

We do not want a situation like in the 1968 movie "2001 A Space Odyssey," when Hal, the artificial brain behind spaceship created by humans, locked the human Dave out of the craft, because Hal feared that Dave was planning to shut down Hal. Was that movie of almost 50 years prescient or just Sci-Fi?

The History of the Future and Back

JUNE 27, 2017

https://blogs.duanemorris.com/techlaw/2017/06/27/the-history-of-the-future-and-back/

It is natural for us to ponder the future and to wonder what is coming next. For example, right now we are considering how far will Artificial Intelligence (AI) go. Will more and more of our lives be facilitated positively by AI? Or, will AI robots ultimately work toward their own superiority and survival over that of their human creators? But let's also consider the history of the future. What were past predictions of the future? And what about future look backs to this present time?

Centuries ago, it is unlikely that most humans contemplated that not too long in the future that their descendants would talk to one and other over the telephone and would travel great distances by planes, trains and automobiles. Indeed, they would have struggled to even imagine lighting up the night with electricity and the many other functions that would be moved forward by electricity.

As recently as the New York Worlds Fairs in the mid-1960s, there were grand predictions about how by now we would be flying around in our own flying cars. Well, that prediction proved wrong, obviously. And while there were many grand future predictions at those Worlds Fairs, one major development was missed — the internet!

So, future predictions at times just don't get it right — either by way of over-predicting or under-predicting.

How about look backs? How will future humans view what is taking place presently? Will we be viewed favorably for all of our technological advances that are bringing the world closer by way of many different types of communications mediums? Will future humans live better because of AI that is starting in this era?

Or, assuming humans are still on Earth for the foreseeable future, will we be viewed very badly by future humans for destroying much of the planet and mankind because of environmental destruction, or biological or nuclear warfare — the roots of which could be traced to this time period?

What are your predictions for the future? Will they be correct? Let's stick around and find out!

Are Nuclear and Energy Sectors at Risk of Hacking?

JULY 6, 2017

https://blogs.duanemorris.com/techlaw/2017/07/06/are-nuclear-and-energy-sectors-at-risk-of-hacking/

Most of us are aware that our personally identifiable information, like our credit card numbers, are at risk when retailers are hacked. However, there may be even greater risks. Indeed, the U.S. government has issued a recent warning about a hacking campaign targeting nuclear and energy sectors.

According to a Reuters article, in recent months hackers have utilized phishing emails in an effort to "harvest credentials" in order to gain access to networks at nuclear and energy targets. Reuters cites a joint report from the U.S. Department of Homeland Security and Federal Bureau of Investigation as its source. The report indicates that at least in some instances hackers already have succeeded in gaining entry to certain networks, but the report did not identify specific targets that were compromised.

Why do hackers have designs on the nuclear and energy sectors? The report states that "cyber actors have strategically targeted the energy sector with various goals ranging from cyber espionage to the ability to disrupt energy systems in the event of a hostile conflict," as cited by Reuters.

On top of this, Reuters reports that E&E News, an energy industry news site, has revealed that U.S. investigators are investigating apparent cyber intrusions at multiple nuclear power generators. While no safety systems reportedly were compromised, this is not a positive development.

It is not comforting to think that our energy and nuclear industries could be vulnerable to cyber attacks. We have seen what can happen; in late 2016, hackers were able to cut electricity in Ukraine. According to Reuters, two cybersecurity firms stated that they had identified malicious software implemented in the Ukraine attack, and which also stated that it would not be difficult to modify such software to come after utilities elsewhere, like in the United States.

Plainly, in this new internet era, warfare and attacks can take place in cyberspace as well as traditionally on land, on the sea and in the air. Absolute best efforts must be made to protect our nuclear and energy sectors. We need to avoid being put in the dark by energy disruption, we must protect the integrity of mission critical systems, and we must be certain that there is no risk of danger caused by interference with nuclear and other energy systems.

We Need Internet Stop Signs

JULY 20, 2017

https://blogs.duanemorris.com/techlaw/2017/07/20/we-need-internet-stop-signs/

Has our ability to stay present in the real world largely been destroyed by the internet? If so, how has that happened? If we erected internet "stop signs" would we be better off?

While we were saturated with different sources of information, news, and entertainment as recently as the Twentieth Century, those sources had naturally occurring stop cues that allowed us to pause and consider disengaging from the sources.

For example, when we reached the end of a section of the newspaper, or even the entire newspaper, we stopped, and likely decided to move onto something else.

While reading a book, we came to the end of a chapter, or the completed book, and then we were done, freeing ourselves up for something different in the world.

When we played a record album, we had a natural stop built in when we finished the side of the album.

As we watched television, there were limited channels and shows to choose from, and when our selected show ended, we often used the break and decided to go do another activity, and frequently not a passive activity.

When we wanted to watch a movie, we went out to the theater, saw the movie, and then got up and left to return to our real lives.

But now the sources of information, news, and entertainment are bottomless. What is meant in this context by the word "bottomless"?

By virtue of the ultimate saturation provided by the internet, we have lost stopping cues. For example:

- We can check ever-updated news sites constantly.
- There is no dearth of constant updates provided by social media sites.
- Even when reading books, by doing so electronically we can move seamlessly and endlessly from one book to another.
- We can stream music non-stop without even coming to an end.
- We have numerous online ways to watch a multitude of television shows and movies without ever having to stop; there is more content than we can ever handle.

So, What Do We Do to Build in Stop Signs on the Internet?

Some of the stop signs can be mandated by employers, for example.

Indeed, one company toward the end of the work day has all desks automatically raised to the ceiling. The workplace is transformed into a yoga and dance studio. Obviously, the employees do not have the option to continue working at their desks on their computers. Rather, they are provided the choice on certain days to engage in yoga, and on other days to participate in dance.

Another company, when an employee is on vacation, provides automatic email replies that tells email senders that the employee is on vacation and that the email will be deleted. Thus, the email sender has the choice of waiting to contact the employee once the employee is back from vacation, or to contact a different employee who is not on vacation. The point is to treat as sacrosanct the vacation of the employee so that the employee truly can get away.

And at home, certain stops signs can be put in place. Rules can be agreed upon; for example, it can be decided that smart phones must be placed far away from the dining table during meals. The same thing can be true when it is agreed that in-person conversations are going to happen.

We all must find ways to protect ourselves from the ubiquity of the internet. The internet can become omnipresent, but we can take steps to build internet stop signs.

Tech Acumen: Many Companies Falling Behind

AUGUST 15, 2017

https://blogs.duanemorris.com/techlaw/2017/08/15/tech-acumen-many-companies-falling- behind/

Corporate America and companies around the globe are spending vast amounts of money trying to keep up with all sorts of threats in this new digital age. So, how are companies really doing?

Unfortunately, not so well. Indeed, according to PwC's 2017 Digital IQ Survey, as reported by PR Daily, barely more than half of IT executives from the US and 52 other countries reported that their companies have a "strong digital IQ." This is down from 67 percent so reporting in 2016, and 66 percent in 2015.

What is going on? The problem is not that corporate employees somehow have become less tech competent during the last year. Rather, they are struggling to keep up with many different demands — from IT, to social media, to a company's online culture.

PR Daily notes that as business processes become more digital, there is greater complexity, and there is increased risk and uncertainty with respect to potential privacy violations, data breaches, and various types of hacks. On top of this, there are further and constant innovations; for example, like the "internet of things," as to which 42% of executives report it to be "disruptive to their business model."

According to PwC, there are an "essential eight" quickly developing technologies to grapple with effectively. These include not only the internet of things, but also artificial intelligence, robotics, 3-D printing, augmented reality, virtual reality, drones and blockchain. Yes, indeed, there truly is much to grapple here.

If you already are awake at night pondering all of this, you are not alone, as respondents reported that their companies were spending only 18% of their tech budgets on emerging technologies.

The Harvard Business Review, cited by *PR Daily*, asserts that companies must raise the digital IQ of their employees. To do that, they must invest in the technological tools to accomplish that goal.

And there must be constant training and flexible planning to deal with the ever-changing digital landscape. Very true!

What to Do About Social Media Bullying and Hate

AUGUST 29, 2017

https://blogs.duanemorris.com/techlaw/2017/08/29/what-to-do-about-social-media-bullying-and-hate/

Social media outlets now connect billions of people around the globe on a constant basis. Facebook, by headcount, has become the largest nation on the planet, with approximately two billion users. A tremendous number of these users communicate with others via their social media accounts many times a day. Of course, there are many positive aspects of social media communications; but, regrettably, there are palpable negatives as well.

Cyberbullying is one of those negatives. All too often, for example, a minor or a group of minors bullies another minor, with disastrous consequences. The victim can be ostracized, humiliated, and driven to anxiety, depression, and even self-destruction. This can even happen with adults. We learned in the news recently of a woman who was prosecuted for egging on her boyfriend via text messages to commit suicide. She ultimately was found guilty of manslaughter.

And social media has made it easy for people and groups with different opinions to engage not only in civil political discourse, but to also voice extreme accusations, to make racist and sexist remarks, and to even suggest potential violence. It seems that social media has made it simple to reach out to a vast audience while demonizing others who are not truly known on a personal, individual basis.

So, what is to be done about all of this?

It is not realistic to expect that social media companies will ensure that these types of communications never will appear on their outlets. Why? First, under Section 230 of the Communications Decency Act, internet service providers generally are immune for the content of third-parties posted on their sites.

And second, it just is not practical to assume that social media companies could police the many billions of communicates that appear on their sites daily. These companies could not possibly hire an army big enough to get this job done while also remaining economically viable. Sure, in extreme instances, social media companies can be informed of truly horrifying posts so that they can be removed, and these companies do employ some level of resources to find and address such posts. But more needs to be done.

We really need to take this on individually as people dealing with real people.

Parents need to be involved in the Internet activities of their children and teenagers. It is true that technology advances at warp speed, and often children and teenagers know more about cyberspace than their parents. It is up to parents to become educated in the first instance so that they can educate their children as their children first go online. Parents should inform their kids about the specific risks on the Internet, and how properly to treat other people when online. They also should know that they can come to their parents when they become concerned about anything that they encounter online.

And as adults, we need to treat people in cyberspace as we would in a face-to-face communication. And on top of that, we should get out from behind our computers and actually see people in the real world; and not just people who share our beliefs, but people outside of our respective bubbles so that we can understand that people with different points of view are still human beings deserving of respect and civility.

Perhaps these recommendations may seem like only a start and not enough. And that is probably true. Further ideas to bring people together are welcome and should be considered.

How to Respond to the Huge Equifax Hacking

SEPTEMBER 12, 2017

https://blogs.duanemorris.com/techlaw/2017/09/12/how-to-respond-to-the-huge-equifax- hacking/

By now, you likely have learned that Equifax suffered tremendous hacking. Specifically, as Equifax recently announced, hackers took advantage of a website application vulnerability to access records during a several-month period from May through July of this year. Not only did these hacking activities take place over an extended period of time, but as many as a whopping 143 million consumers in the United States may have been impacted. How so? Their personally identifiable information may have been compromised, including Social Security numbers, addresses, drivers license numbers, and birth dates.

So, what should U.S. consumers do in response to the Equifax hacking?

A recent article by Forbes.com provides some solid guidance in terms of a five-point plan.

First, find out if you are affected. Go to this site that has been set up to provide further details relating to the hack: EquifaxSecurity2017.com. To ascertain whether you have been affected, click on the Potential Impact link in the top navigation. After you have gone there, you are directed to the Check Potential Impact button. From there, enter the last six digits of your Social Security number and last name. Hopefully, you can find out your status. But there can be some vague responses. If you get a vague response, you can call the response line at 866-447-7559 for clarification.

Second, enroll in TrustedID Premier. Equifax is offering a complimentary monitoring service, which includes an Equifax credit report, three-bureau credit file monitoring, Equifax credit report lock, Social Security monitoring, and up to $1 million in identity theft insurance.

Third, monitor your accounts. This means you should be active in reviewing your account statements, checking for any irregular activity or any changes in your personal information.

Fourth, visit the FTC Identity Theft site for additional recommendations on protecting yourself from identity theft. This site gives guidance regarding types of information stolen and exactly what to do in response. Some of this advice includes explaining when to place a credit freeze, suggesting to file taxes early (so hackers won't have as much time to use your Social Security number to file for you to get your tax refund), explaining not to trust anyone who calls saying you must pay taxes or debts promptly, and stating when to change passwords and login information.

Fifth, in the unfortunate event you have been a victim of identity theft, you should complete a form on the FTC Identity Theft Recovery site. This will give you a specific identity theft report as well a recovery plan to do list.

Hopefully, you were not a victim of the Equifax hacking. However, given how many U.S. consumers probably have been affected, you or someone close to you may have been impacted and should take defensive steps for protection.

The Rise of Uber Dealt a Current Blow in London

SEPTEMBER 27, 2017

https://blogs.duanemorris.com/techlaw/2017/09/27/the-rise-of-uber-dealt-a-current-blow-in-london/

Once upon a time not that long ago, we generally took taxis for ground transport from one specific location to another within and around cities. At times, it was difficult to obtain a taxi when desired, or to avoid a wait, a taxi would need to be reserved quite a while in advance. But, then along came Uber as a ride-sharing game-changer with many positive advantages. However, Uber also has taken some recent hits, including losing its license to operate in London.

Uber is fantastic in many respects. By using an app on a smartphone, we can track the closest Uber driver, and in many urban areas an Uber car will come to us within just a couple minutes. No longer are we tied to taxis, or even the need to rent or own cars in Uber-friendly cities.

In addition, Uber has provided employment opportunities for thousands of people who want to provide rides on the side of their primary jobs, or for people who desire to drive for Uber on a more full-time basis. Uber's worth has been estimated to be as high as $70 billion.

Of course, the taxi industry has not been happy with Uber, as Uber has made major inroads into what was the taxi market. And Lyft has joined Uber as part of the new ride-sharing model.

While Uber's rise has been relatively meteoric, it has been facing a variety of current problems. For example, while there have been many hundreds of thousands of rides without any incidents, there have been some reports of sexual assaults on passengers, including assaults allegedly perpetrated by drivers. To be clear, this has been the very rare exception.

Moreover, different criticisms from diverse voices such as some regulators, customers, unions and investors led to the removal of Uber's founder and CEO, Travis Kalanick. He was just replaced by Dara Khosrowshahi, previously of Expedia.

These problems have been significant, and they were just compounded by London's transportation agency's decision late last week to decline to renew Uber's license to operate in London — Uber's largest European market, according to a recent New York Times article.

In making this decision, the agency said that Uber's "approach and conduct demonstrate a lack of corporate responsibility in relation to a number of issues which have potential public safety and security implications." Among issues troubling the agency are how Uber conducts background checks on its drivers, and how Uber has dealt with criminal offenses. Uber asserts that its methods are the same as those of black-cab drivers.

This decision by the agency occurs within a year of a British tribunal ruling that Uber could not characterize its drivers as self-employed contractors; meaning that Uber would have to comply with labor standards requiring pensions and holiday pay.

According to the New York Times article, Uber's London license will expire on September 30, but Uber has been afforded 21 days to appeal. Uber has declared that it indeed will appeal, and it is permitted to continue to operate in London during the appellate proceeding.

If Uber is stopped in its London tracks, there will be a huge impact, as there are 40,000 drivers, and 3.5 million customers who use its app at least once every three months, as reported in the article. Also, some have suggested ethnic and class issues, as the majority of black-cab drivers are white native-born Britons, whereas many London Uber drivers are immigrants, as reported by the New York Times.

Stay tuned to see whether the decision by the London transportation agency will stick, or whether it will be overturned on appeal and Uber will be allowed to continue to operate in London. Perhaps if Uber can show that its methods truly are not different than those of black- cabs, or even that it can measure up to those methods very soon, it could continue to live on in London.

Private Government Emails in the FOIA Era

OCTOBER 12, 2017

https://blogs.duanemorris.com/techlaw/2017/10/12/private-government-emails-in-the-foia-era/

The Freedom of Information Act (FOIA) was enacted to shine light on government activities for public review. Indeed, for our democracy to function effectively, those who govern must be accountable to those they govern. Along those lines, the Supreme Court has held that our citizenry is entitled to know "what the government is up to." And in the wake of Watergate, the FOIA was given greater enforcement teeth.

In a nutshell, the public can make FOIA requests to the government seeking government records pertaining to all sorts of government affairs. The government is required to produce or make available such government records, unless a narrow exemption applies, such as exempting the production of records that could compromise an ongoing law enforcement investigation, or records that would reveal classified state secrets. But the presumption is that requested government records must be produced.

As we heard about during the most recent presidential campaign, Hillary Clinton, when serving as the Secretary of State, engaged in governmental communications while using a private email server. The problem with this is that if FOIA requests are made for government records, those communications housed on a private email server could escape revelation to the public. This could mean that government could operate in secret — undercutting the core purpose of the FOIA and the functioning of an open democracy.

Hillary Clinton admitted that it was a mistake that she used a private email server for some governmental communications. She explained that nothing consequential was kept secret, and she endeavored to produce these email communications. Nevertheless, on the campaign trail, Donald Trump whipped up his base, and there were repeated chants of "lock her up" when referring to the Clinton email debacle.

Fast-foward, Donald Trump is President, and now it has reportedly has come to light that Jared Kushner, Ivanka Trump, others in government have been using private email servers with respect to governmental communications. What does this mean?

Does this mean that Donald Trump was not truly serious when accusing Hillary Clinton of criminal conduct regarding her private email server communications? Does this mean that Trump's people should be prosecuted for private email server government communications, as he strongly suggested should happen to Hillary Clinton? Or does this mean that there should be a pox on the houses of both sides, and we truly have to be concerned about the open running of government, as these lessons seem not to be learned and there appears an ongoing desire to keep some government communications away from public scrutiny?

At this point, one can reasonably suspect that Trump will not continue as strongly to proclaim that Clinton engaged in criminal conduct, as that could boomerang back on his people. One can also guess that there will be further investigation into how Trump's people handle their government emails — as Hillary was similarly investigated. It remains to be seen what

enforcement or prosecutorial action, if any, will be taken in response to Trump administration emails that were communicated via private email servers.

Using Fiber Optic Cables to Predict Earthquakes

OCTOBER 24, 2017

https://blogs.duanemorris.com/techlaw/2017/10/24/using-fiber-optic-cables-to-predict-earthquakes/

Earthquakes can be devastating in terms of their destructive impacts. For decades, there have been scientific efforts seeking to predict earthquakes. If an earthquake could be predicted reliably in advance, people could be warned and they potentially could move toward safety before the earthquake strikes.

Unfortunately, earthquake prediction efforts generally have not met with success. But what about fiber optic cables — the very cables that deliver internet connectivity: can they help when it comes to earthquake detection?

As we know, and as explained in a recent article in PopularMechanics.com, fiber optic cables carry information almost at the speed of light. These cables are used by telecommunications companies all across the globe. And they also are implemented by oil and gas companies to detect tiny quakes that result from drilling equipment. These companies use the "backscatter property" of the cables to monitor the actual movement of cables and to detect seismic events.

Following on, researchers at Stanford University have put in place a three-mile optical fiber loop around the Stanford campus. And by employing this fiber network they have been able to detect 800 seismic events, including 1.6 and 1.8 Richter scale local earthquakes as well as a recent earthquake as far away as Mexico, according to PopularMechanics.com.

This could translate to mean that scientists potentially could piggyback on existing fiber optic cables that telecommunications companies already have put in place around the U.S. to detect earthquakes.

It is important to note that these cables would not be as sensitive as traditional seismometers, but but they are less expensive and provide a broader detection network, as pointed out by PopularMechanics.com.

It remains to be seen how much advance warning of earthquakes fiber optic cables would provide if they are employed to detect earthquakes. Yet, even a warning of a matter of minutes could save many lives in an urban area.

Immunity for Internet Service Providers Under Siege?

NOVEMBER 8, 2017

https://blogs.duanemorris.com/techlaw/2017/11/08/immunity-for-internet-service-providers-under-siege/

Long ago in internet time, back in the mid-1990s, Congress considered how closely to regulate Internet Service Providers (ISPs). Congress determined that it was in the best interests of the United States not to burden ISPs with restrictions, so that the Internet could grow and flourish in the areas of commerce, communications and education. Thus, Section 230 of the Communications Decency Act was enacted and it provides broad immunity for ISPs with respect to third-party content posted on their sites. Generally speaking, ISPs have not been saddled with publisher-type liability — it is not their job to police their web sites to ensure that posted content is not false or malicious.

The high water mark of Section 230 ISP immunity probably was best represented by the late-1990s case of Zeran v. AOL. In that case, the Fourth Circuit Court of Appeals basically held that AOL did not have liability even though Zeran established that third-party content on the AOL site sought to connect Zeran with the Oklahoma City federal building bombing (the worst terrorist attack on US soil up to that time). These posts led to death threats, the loss of Zeran's business, and the needed for 24/7 protection. He also alleged that AOL did not take down these extremely offensive and damaging posts in a timely fashion even after having been notified. Notwithstanding, the Fourth Circuit held that AOL had no liability pursuant to Section 230 immunity.

Since the Zeran case, there have been judicial efforts to whittle down the broad immunity afforded ISPs by Section 230. But Section 230 still stands as a substantial barrier in efforts to pin liability on ISPs for third-party content. And in part because of Section 230, ISPs truly have flourished since the enactment of this statute. Indeed, companies like Facebook, Google and Twitter now are some of the most highly-valued companies in the world.

But, just last week these three companies were on Capitol Hill testifying about what happened during the 2016 Presidential Election. Facebook alone revealed that one Russian group posted about 80,000 times during the campaign and reached over 126 million Facebook users. And, of course, Congress is concerned that Facebook purportedly did not endeavor to ascertain the true identities of the posters, nor did Facebook allegedly seek to ascertain whether the information posted was true or false.

Apparently, efforts now are being undertaken by Facebook and perhaps other ISPs, especially in the election context, to try to ensure identity transparency and accuracy via fact-checking. However, how far do these efforts go, can ISPs on their own ensure the truth, and will Congress be satisfied by such self-regulation?

Some members of Congress do seem deeply concerned, and the legislative machine may be gearing up. Will Congress explicitly eliminate, at least to some extent, the heightened immunity afforded to ISPs under Section 230? If so, will such efforts require ISPs generally to police third-party content much like a traditional publisher, especially now that some ISPs are all grown up

and our internet truly has matured? Or, will legislation be tied primarily to election context? Or further still, can the ISPs convince Congress that they truly can handle such problems on their own and that legislation is unnecessary?