VFI Executive Briefing
A weekly roundup of technology news
November 14-18, 2016

TABLE OF CONTENTS

HILL UPDATE

Forbes **In The Lame Duck, How Congress Makes Cybersecurity A Non-Partisan Priority**
With a lame duck session of Congress looming, federal lawmakers are scrambling to push key legislative items through last-minute. One key area of concern is cybersecurity. Recent headlines have exposed a wide array of victims, ranging from both corporate to government entities. Stoking concerns is the ongoing controversy surrounding Russian hacking of Democratic presidential candidate Hillary Clinton's campaign emails and the DNC, in a perceived effort to influence the outcome of the U.S. presidential election. Against this backdrop, several members of Congress have introduced amendments to the National Defense Authorization Act (NDAA) to strengthen cybersecurity. Yet, is this enough?

The Hill **Russian hacking of election infrastructure 'curtailed' after US statement**
Russian scanning of state election infrastructure was "curtailed" after the U.S. publicly blamed Moscow for hacking several U.S. political organizations, the nation's top intelligence official says. "The issuance of the statement and communication between our government and the Russian government seemed to have curtailed the cyber activity the Russians were previously engaged in," Director of National Intelligence James Clapper said during a House Intelligence Committee hearing Thursday.

CNN **Regulate cybersecurity or expect a disaster, experts warn Congress**
The hearing, held Wednesday by members of the House Energy and Commerce Committee, examined how millions of infected internet-connected devices took down parts of the internet on October 21. [...] Experts blame poor practices by low-end manufacturers making devices like internet-accessible baby monitors, cameras and thermostats. [...] Asking for regulation is a rare move for cybersecurity experts. They usually want fewer government rules, which tend to stifle innovation. But the panel of experts on Wednesday said this time it's different. "We're not going to be laughing when the lights go out," Fu said.

VFI Executive Briefing
A weekly roundup of technology news
November 14-18, 2016

ARTICLE SUMMARY

The Salt Lake Tribune **Op-ed: Hatch bill clarifies what is private in the digital world**
The Salt Lake Tribune published an op-ed by Microsoft President Brad Smith urging congressional leaders to support the International Communication Privacy Act (ICPA). In the op-ed, Smith highlights how the legislation, introduced by Senator Orrin Hatch, provides a legal framework that respects people's right to privacy while enabling law enforcement to obtain data necessary to their investigations.

Morning Consult **The Next Unknown in Intellectual Property: President Trump**
The U.S. Patent and Trademark Office's decision to host a series of roundtables on subject matter eligibility issues starting today and extending into next month comes at a uniquely interesting time. For one, no one really knows the Trump administration's vision or plans for intellectual property. This uncertainty casts a shadow over what's already been a particularly disruptive period in IP. The post-Supreme Court Mayo-Alice landscape casts into question what is and what is not a patentable invention.

The Register **Encrypted email sign-ups instantly double in wake of Trump victory**
ProtonMail has published figures showing that as soon as the election results rolled in, the public began to seek out privacy-focused services such as its own. [...] "Given Trump's campaign rhetoric against journalists, political enemies, immigrants, and Muslims, there is concern that Trump could use the new tools at his disposal to target certain groups," Yen said. "As the NSA currently operates completely out of the public eye with very little legal oversight, all of this could be done in secret."

CNET **iPhone sales will 'suffer' if Trump targets China, officials warn**
As the world watches to see how President-elect Donald Trump handles his new responsibilities, China's state-run press has readied something of a warning: start a trade war with the country and American companies could suffer. "China will take a tit-for-tat approach" if Trump were to declare China a currency manipulator -- as Trump claimed he could do -- the Global Times wrote in the column. "US auto and iPhone sales in China will suffer a setback, and US soybean and maize imports will be halted."

The Hill **Google CEO to meet with EU antitrust head**
Sundar Pichai, the CEO of Google's parent company Alphabet, will meet with the European Union's antitrust commissioner on Friday, The Wall Street Journal reports. Pichai's meeting with Margrethe Vestager Alphabet formally rejected the European Commission's accusation that Google violated antitrust policies. The executive arm of the European Union charges that Google's Android operating system and its advertising and comparison shopping services clashed with those regulations.

Washington Post **How Donald Trump could dismantle net neutrality and the rest of Obama's Internet legacy**

VFI Executive Briefing
A weekly roundup of technology news
November 14-18, 2016

President-elect Donald Trump could eviscerate some of the most significant tech policies of the 21st century, all but erasing President Obama's Internet agenda and undoing years of effort by lawmakers, tech companies and consumer advocates to limit the power of large, established corporations, analysts say. In particular danger are key initiatives of the Obama years, including net neutrality and a pivotal series of Internet privacy regulations that came along with it.

Wired **Trump's Presidency Could Upend the Way Silicon Valley Works**
DURING THE PRESIDENTIAL campaign, Silicon Valley leaders all but uniformly rejected Donald Trump. Now they're struggling to come to terms with what his presidency will mean for their industry. Under President Obama, Silicon Valley became very friendly with Washington—and the relationship went both ways. Tech companies spent millions to lobby Congress, while former political strategists often left the White House for Bay Area tech jobs. After his term is over, President Obama himself is reportedly likely to stay linked to tech, with much of the work of his charitable presidential foundation tied to the progress of innovations in Silicon Valley. The reality of a Trump presidency is likely to be vastly different for tech.

IPWatchdog **Death to All Patents? Really? Why Inter Partes Review Shouldn't Be Controversial**
I'll be speaking on November 17, 2015 at IAM's Patent Law and Policy event. (It looks to be a really interesting day.) My panel has the provocative title, Death to all patents! The realities of the USPTO's review procedures, which expresses a point of view I hear all too often. It amazes me that a procedure like inter partes review has become so controversial, with the Patent Trial and Appeals Board being called a "patent death squad" and people talking about patent "kill rates."

New York Times **Automated Pro-Trump Bots Overwhelmed Pro-Clinton Messages, Researchers Say**
SAN FRANCISCO — An automated army of pro-Donald J. Trump chatbots overwhelmed similar programs supporting Hillary Clinton five to one in the days leading up to the presidential election, according to a report published Thursday by researchers at Oxford University. The chatbots — basic software programs with a bit of artificial intelligence and rudimentary communication skills — would send messages on Twitter based on a topic, usually defined on the social network by a word preceded by a hashtag symbol, like #Clinton.

IT Business Edge **Why Cybersecurity Must Be a Priority Post-Election**
Now that most of the election dust has settled, I think it is safe to say that this was the most cybersecurity-aware election season that we've ever witnessed. Clearly, not all of it was good cybersecurity awareness, as most of the talk was about hacked emails and the potential for hacked voting machines with little to no conversations about solutions or prevention. I wanted cybersecurity to be a front-and-center issue and talking point, and I believe it needs to continue to be a talking point. Some, in fact, think the focus on cybersecurity needs to be not only a high priority but take on a sense of urgency. In fact, there are predictions that cybersecurity will

become a national crisis in a matter of months and must be a focal point of the new president's first 100-days agenda.

Wall Street Journal **U.S. Workers to Lose in China Trade War**
Nobody wins in a trade war. If Donald Trump sparks one with China, among the losers will be some of his most ardent supporters: blue-collar workers who helped sweep him to election victory. In fact, they'll stand to lose twice. They've already endured stagnant incomes for decades amid withering trade competition from China. Mr. Trump's threatened tariffs of 45% on all Chinese imports would hit their pocketbooks again by raising the price of pretty much everything on sale in Wal-Mart, from sneakers to microwave ovens. Nor is there convincing evidence that punitive tariffs would bring back jobs lost to China. The march of technology has altered the employment landscape. American factory workers are threatened more by automation than Chinese sweatshops.

ZDNet **From Brexit to Trump: How organizations and data prepare for and respond to political events**
As the Big Data London event coincided with a new development in the Brexit story, back-stage discussions could not possibly have remained unaffected. In some cases they even took to the center stage, going as far as panelist Kim Nilsson from Pivigo who has been quoted to say that "if we have a hard Brexit, the data industry is going to die". The newly elected US president has drawn parallels between himself and the Brexit movement, so even though comparing leaving a federated union of nations and changing head of state is like comparing apple pie to Marmite, looking at what organizations can do using data to cope with political change may be of relevance.

CNET **Here's what 40 internet companies want Trump to do**
In July, 145 tech leaders called Donald Trump "a disaster for innovation." But now that he's been elected president, some of those companies are trying to appeal to his good graces. The Internet Association -- a group of 40 top internet companies including Airbnb, Amazon, Facebook, Google, LinkedIn, Netflix, Twitter, Uber and Yahoo -- issued an open letter on Monday that congratulates Donald Trump on his victory and offers a long list of policy positions they hope he'll consider during his time as president.

Forbes **Law Prof Says FTC Report On Patent Assertion Entities Is 'Totally Flawed'**
A new Federal Trade Commission report that looks at patent assertion entities — some of which are referred to as patent "trolls" because of their penchant for filing lawsuits — and their business practices is "totally flawed," says a Virginia law professor who has been studying patent licensing firms for years. Kristen Osenga, a professor at the University of Richmond School of Law, teaches and writes in the areas of intellectual property, patent law, law and language, and legislation and regulations. She is a frequent speaker at symposiums on patent law and intellectual property.

VFI Executive Briefing
A weekly roundup of technology news
November 14-18, 2016

Washington Post **Web users' online rights are on the decline worldwide as governments target messaging apps**
Messaging apps are facing increased pressure from government authorities as online rights around the world are slipping, according to a Freedom House report released Monday. Internet freedom declined for the sixth year in a row, the pro-democracy think tank's "Freedom on the Net" report shows. The report looks at online access, censorship and surveillance in 65 countries around the world. "In a new development, the most routinely targeted tools this year were instant messaging and calling platforms, with restrictions often imposed during times of protests or due to national security concerns," the report says.

Wall Street Journal **China's Xi Jinping Opens Tech Conference With Call for 'Cyber Sovereignty'**
WUZHEN, China—China's President Xi Jinping called for "more fair and equitable" governance of the global web, as the country opened a state-run internet conference aimed at pushing its alternative vision of the web. Mr. Xi said in video remarks played at the conference opening Wednesday that China would work to uphold "cyber sovereignty," the idea that countries have absolute control over their corners of the internet. In its third year, the Wuzhen World Internet Conference remains an anomaly: a convocation of the world's biggest tech companies in a rustic tourist village, organized by the world's most sophisticated internet censorship bureau, the Cyberspace Administration of China.

Just Security **US Transparency Regarding International Law in Cyberspace**
Last Thursday, State Department Legal Adviser Brian Egan, delivered an important speech at Berkeley Law School on the relationship between international law and cyber activities. It was significant in two regards. First, it added granularity to the US positions regarding how international law in such areas as IHL, sovereignty, and State responsibility applies in cyberspace. Second, and perhaps more importantly, Mr. Egan came out strongly in favor of transparency vis-à-vis State legal views on the matter. His stance has the potential to engender greater, and desperately needed, transparency on the part of other States.

American Thinker **Winning the Cyber-War Under Trump**
Turning the NSA into a Cabinet office of the National Information Security (NISD) Department would not only help the unite our cyber defense, but would help to cut down on bureaucracy. The NIS should ensure that policies and definitions of cyber include timing and location services, such as GPS (Global Positioning System). This classification would help coordinate the efforts to increase resiliency capabilities and would help minimize, and possibly prevent, purposeful interference with our cyber infrastructure, and enhance our defense capabilities. The NIS would be in charge of uniting and overseeing the necessary actions needed to secure the nation's cyber infrastructure from any interruptions.

Forbes **UK Joins Russia And China In Legalizing Bulk Surveillance**
Forbes reported that the UK's House of Lords passed the Investigatory Powers Bill, clearing the way for the bill to be made law. Outlets highlighted concerns from numerous privacy advocates

regarding the UK's new surveillance capabilities, as well as their fears that other governments could mirror the UK and enact similar laws. Jim Killock, executive director of the Open Rights Groups, heavily criticized the bill, calling it the "most extreme surveillance law ever passed in a democracy." The bill will soon undergo Royal Assent, and could be enacted before the end of the year.

Notable Quotes

"At Microsoft, we are doing everything we can to protect the privacy of our customers in Utah and around the world. But we also need strong leaders in Congress, like Hatch, to advance strong solutions that provide clear and necessary rules-of-the-road to move technology forward while ensuring no one is left behind."

– Microsoft President Brad Smith

"With Trump eager to misuse his power and get revenge on his perceived enemies, it's reasonable to conclude there will be a parallel increase in abuse of power in law enforcement and the intelligence community. Activists who put their bodies on the line trying to protect basic rights — freedom of religion, freedom of speech, civil rights, reproductive rights, voting rights, privacy rights — will face the brunt of it."

– Micah Lee, reporter, The Intercept

"It's very much within the authority of the president to make changes [changes under Executive Order 12333]…There could be a significant expansion of those activities without the public having any knowledge of it."

– Elizabeth Goitein, co-director, Brennan Center for Justice's Liberty and National Security Program

"Secrecy is crucial because it enables more invasive and disruptive forms of surveillance, according to University of Washington Professor Ryan Calo, who has written extensively on the topic. As long as surveillance programs are secret, it's nearly impossible to hold them in check — and without a steady stream of whistleblowers, any new programs are likely to stay secret.

– Russell Brandom, reporter, The Verge

"Strong encryption is critical to national and individual security. Encryption is key to national defense, and it also protects our nation's financial system and critical infrastructure. It also protects users from repressive governments looking to stifle speech and democracy, and it shields users from nefarious actors seeking to steal their sensitive data. Laws that require

companies to engineer vulnerabilities into products and services harm personal privacy and endanger national security. Support for strong encryption makes America more secure."

– Internet Association letter to President-elect Donald Trump

"Twitter is used extensively by terrorist organizations and other criminals to communicate, recruit, and raise funds for illegal activity. With increased use of Twitter by subjects of FBI investigations, it is critical to obtain a service which will allow the FBI to identify relevant information from Twitter in a timely fashion."

– FBI Contract with Dataminr

"Because encryption protects us in so many ways, it is important that technology policies around the world do not mandate built-in flaws that would undermine its effectiveness. Weakening encryption by requiring companies to intentionally undermine the integrity and the security of their products and services will eventually lead to less *security for our society as a whole. Compromised encryption may help law enforcement investigate specific crimes, but it can also make the internet and our lives much less secure. There is no way to weaken encryption only for law enforcement. Mandated weak encryption lowers our defenses in every sector that depends on software. And today,* every *sector depends on software."*

– Victoria Espinel, President and CEO, BSA | The Software Alliance

"If the U.S. acts in its own interests without regard to the legitimate needs of its allies, they will do the same. Nations will act unilaterally to protect their own citizens, making it collectively harder to investigate crime and cutting the internet to pieces. We are already seeing this reaction — many nations (even our friends) are writing laws that say that data about their own citizens — Germans, say — must be stored in Germany and subject only to German law. The trend toward a fractured network in quickening before our eyes."

– Paul Rosenzweig, senior advisor, The Chertoff Group

"The passing of the IP Bill will have an impact that goes beyond the UK's shores. It is likely that other countries, including authoritarian regimes with poor human rights records, will use this law to justify their own intrusive surveillance powers."

– Jim Killock, executive director, Open Rights Group

"While the risks to the reputation of UK companies whose services might be backdoored by state agencies is another concern. How can UK-based tech companies promise a trusted service

to users when the law can compel them to pre-bake weaknesses into systems on-demand? Perhaps only by moving their businesses elsewhere."

–Natasha Lomas, reporter, TechCrunch

Social Highlights

- **@BradSmi:** We need strong leaders like @SenOrrinHatch to advance #privacy solutions that move #tech forward. via @sltrib #ICPA
- **@EFF:** Stand up for your right to encrypt.
- **micahflee:** Here's how to begin surveillance self-defense preparations for the long fight ahead against the Trump Administration
- **@rcalo:** Every single communications platform needs to adopt end-to-end encryption by January 1
- **@SenOrrinHatch:** Op-ed: Hatch bill clarifies what is private in the digital world, via @BradSmi #icpa #ecpa #Tech @Microsoft
- **TechCrunch:** Trump surveillance fears could lift privacy tech in Europe by @riptari
- **@TheRegister:** Encrypted email sign-ups instantly double in wake of Trump victory
- **@verge:** Donald Trump is about to control the most powerful surveillance machine in history
- **@yaelwrites:** Can you Trump-proof your electronic communications? I spoke w/@micahflee @harlo about steps to take @FutureTenseNow
- **@FortuneMagazine:** These tech giants are banding together and reaching out to Donald Trump
- **@josephmenn:** WhatsApp adds secure video calling, spreading the appeal of strong encryption. Exclusive interview with Jan Koum.
- **@russellbrandom:** In May, Twitter shut off the CIA's Dataminr access, citing surveillance concerns.
- **@dnvolz:** Sen. Warner, who favors an encryption commission, to be top Dem on Senate Intel Cmte. Replaces Sen. Feinstein, who advocated backdoor access
- **@evadou:** China's Xi repeats call for "cyber sovereignty" at third annual state-run internet conference
- **@BSAnews:** BLOG: #encryption is a complex issue. Debate solution must consider arguments from govt, business & individuals
- **@RosenzweigP:** Paul Rosenzweig commentary: Let's not build border walls in cyberspace | The Columbus Dispatch via @DispatchAlerts
- **@TechCrunch:** FBI will receive 'limited' Twitter firehose access through Dataminr, but has to watch its step