VFI Executive Briefing
A weekly roundup of technology news
November 28-December 2, 2016

TABLE OF CONTENTS

SPECIAL COVERAGE – Rule 41

Changes to Rule 41(b) took effect on December 1. As background, in April Chief Justice John Roberts submitted to Congress, "the amendments to the Federal Rules of Criminal Procedure that have been adopted by the Supreme Court. The Supreme Court amended Rule 41(b), governing 'Search and Seizure' by expanding the scope of venue in which a warrant could apply." According to Fortune's accounting of this change, "Under certain circumstances, a federal judge could issue a warrant that would allow law enforcement to hack into a computer that may be located outside the district in which the warrant is being sought. This means that the FBI and other law enforcement agencies will be able to search multiple computers across the country with a single warrant. Until now, the government could only carry out a search of computers located in the district where the federal judge granted the warrant—typically only a few counties in a given state."

The articles below cover the range of responses to the new rule taking effect.

- **The Hill** Feds try to calm worries over new warrant rule
- **Bloomberg Technology** FBI and NSA Poised to Gain New Surveillance Powers Under Trump
- **Morning Consult** Justice Department Pushes Back on Government Hacking Concerns
- **Fortune** FBI's New Hacking Powers Take Effect This Week
- **Politico** Morning Cybersecurity: Stalling Mass Damaging Hacking
- **The Hill** Congress has one more shot to delay government hacking expansion
- **The Hill** Last-ditch effort to prevent changes to law enforcement hacking rule fails
- **BuzzFeed News** Both The US And UK Have Made It A Lot Easier Now To Spy On Their Own Citizens

Selected Quotes

"Stated another way, the Constitution already forbids mass, indiscriminate rummaging through victims' computers, and it will continue to do so if the venue rule change goes into effect. By contrast, blocking the amendments would make it more difficult for law enforcement to combat mass hacking by actual criminals."

– Leslie R. Caldwell, Assistant Attorney General of the Department of Justice's Criminal Division

"I think this debate about government hacking is far from over. My guess is that senators are going to hear from their constituents about this policy sooner rather than later, and we'll be back on the floor again."

– Senator Ron Wyden (D-OR)

"We simply can't give unlimited power for unlimited hacking."

– Senator Steve Daines (R-MT)

"This still requires the government to come forward and do what it always has to do when it seeks a search warrant"

– Senator John Cornyon (R-TX)

"We lost this fight when the rules committee decided this [Rule 41] was a procedural change and not a substantive one."

– Nate Cardozo, attorney, Electronic Frontier Foundation

ARTICLE SUMMARY

Brad Smith Blog **Responsible technology can play a crucial role in moving our country forward**
Two weeks ago, I had the chance to visit Wisconsin, where I grew up. It's a state that has obviously been in the news lately in the context of the presidential election. It's also a state with a rich history of industrial innovation that helped propel the United States to global leadership. The country's first hydroelectric power plant, built in my home town of Appleton in 1882, helped light the way towards the future that includes the electronic devices we enjoy today. Yet Wisconsin, like many states, also faces new and complex challenges due to the nonstop pace of societal and technological change and the issues that arise with it. Visiting a political battleground state whose voters helped decide the tumultuous presidential election led me to reflect on what's ahead for our country. Among other things, our recent election laid bare the struggle of many Americans who feel left out and unable to participate in the economic growth and opportunities created by our rising digital economy. This frustration is felt by more than a few of the people of Wisconsin. And what's happening their mirrors what's happening across our country and more broadly in a number of other nations.

VFI Executive Briefing
A weekly roundup of technology news
November 28-December 2, 2016

Washington Post **The surprising implications of the Microsoft/Ireland warrant case**
The Washington Post published an op-ed by Orin Kerr, law professor at George Washington University, analyzing the potential implications of the Second Circuit Court's decision in Microsoft's warrant case. Kerr states that the court was wrong in its assumption that service providers know the territoriality of customer emails. He argues that while the Second Circuit's decision creates "a sensible structure" for providers that store emails in the country or region where individual users preside, it has created challenges for providers with different network architectures.

Idaho Statesman **Why tech startups need intellectual-property plans**
Idaho has enjoyed dramatic growth in the technology sector over the last decade. It can boast of several successful tech startups. An increasing number of entrepreneurs and emerging companies call Idaho home. While those who launch startups in Idaho enjoy a low cost of living and a desirable lifestyle, they face many of the same challenges and risks faced by their counterparts in other states. One is the need to develop a comprehensive plan that addresses securing and protecting the company's intellectual property. Failure to develop such a plan could mean the difference between a successful startup and a failed one. An intellectual property plan should first identify and protect the company's IP.

Washington Post **Reddit's CEO regrets trolling Trump supporters by secretly editing their posts**
Steve Huffman, the chief executive of Reddit, knows he has some explaining to do. Huffman, also a Reddit co-founder, landed in hot water Wednesday after admitting that he used his administrative powers to secretly edit user comments that were critical of him on r/The_Donald — a popular, pro-Trump forum (or "subreddit"). He swapped all mentions of his own username with the names of the pro-Trump group's leaders, meaning that expletive-laden posts aimed at him looked instead as if they were insulting the group's leaders.

The Hill **Trump picks strike fear into net neutrality backers**
Two of President-elect Donald Trump's appointments to his transition team are sparking fears among net neutrality supporters that the internet rules are on the chopping block. Trump has tapped tech experts Jeff Eisenach and Mark Jamison, two critics of net neutrality, to head his transition team for the Federal Communications Commission. The rule, which requires internet service providers to treat all traffic equally, has been one of the most contentious issues under FCC Chairman Tom Wheeler.

WIRED UK **Snooper's Charter could be repealed after petition forces it back to the House of Commons**
Wired UK reported that over 118,000 people signed a petition requesting that the UK government repeal the Investigatory Powers Bill and engage in renewed debate about the bill. Related, in an op-ed for The Huffington Post, Jim Killock, executive director of the Open Rights

Group, urged Parliament to take a deeper look at the measures proposed in the bill, stating that the media, Members of Parliament and the public were distracted by the Brexit vote and weren't able to "consider what they have voted for." Additionally, The Global research Centre for Research on Globalization published a blog analyzing the bill and detailing its implications for personal privacy.

The Guardian **We let technology into our lives. And now it's starting to control us**
The Guardian published an op-ed by freelance writer Rachel Holmes arguing that the Internet and digital platforms have become tools of control and surveillance. Holmes contends that while the public has primarily focused on government surveillance and access to personal data, corporate control of data and the growth of social media platforms are increasingly leading to the "the demise of our privacy."

SF Gate **State wants rules to toughen utilities' cybersecurity**
Michigan Public Service Commission Chairwoman Sally Talberg says natural gas and electric providers face attempted intrusions into their computer system on an almost daily basis. She says federal and state governments need to work with utilities to create programs to deal with security issues. The rules to be crafted will require utilities to annually give regulators an overview of their cybersecurity program, staffing numbers, a description of employee training and other information such as a summary of cybersecurity incidents.

The Hill **Internet Archive putting database in Canada to keep it from Trump**
The Internet Archive, a nonprofit that saves copies of old web pages, is creating a backup of its database in Canada, in response to the election of Donald Trump. "On November 9th in America, we woke up to a new administration promising radical change," the organization wrote in a blogpost explaining the move. "It was a firm reminder that institutions like ours, built for the long-term, need to design for change." The Internet Archive is responsible for services like the Wayback Machine, a tool that allows users to access cached versions of websites long after they are pulled from the internet, and Open Library, which offers free access to millions of e-books.

IPWatchdog **Software Patents Will Survive: How Section 101 Law Is Settling Down**
Software patents have been controversial for decades. The discussion generally centers around whether software is patent-eligible subject matter. Since the Supreme Court's decisions in Bilski v. Kappos, 130 S.Ct. 3218 (2010); Mayo Collaborative Servs. v. Prometheus Labs, 132 S.Ct. 1289 (2012); Ass'n for Molecular Pathology v. Myriad Genetics, Inc., 133 S. Ct. 2107 (2013); and Alice Corp. Pty. Ltd. v. CLS Bank Intern., 134 S. Ct. 2347 (2014), much of the argument in the debate has taken one of two sides: 1) the Supreme Court has expanded the judicial exceptions to § 101 so far that nearly everything is abstract; 2) despite the Supreme Court's decisions, way too many bad patents are getting past § 101.

VFI Executive Briefing
A weekly roundup of technology news
November 28-December 2, 2016

The Verge **Will net neutrality survive Donald Trump?**
When FCC chairman Tom Wheeler passed the Open Internet Order in February of 2015, it was the culmination of decades of work. After countless advocacy campaigns and legal fights, the order classified internet providers as common carriers — falling under Title II of the Communications Act — which prohibits the companies from blocking or discriminating against traffic as it moves over their network. The move was met with cheers from net neutrality advocates and internet companies like Netflix and Twitter, who saw it as a crucial step toward keeping the playing field level for anyone trying to build things on the internet. Now, Donald Trump may be poised to undo it.

The Hill **Tech groups reach out to Trump**
More than a dozen tech groups extended an olive branch to Donald Trump on Wednesday, penning a joint letter to the president-elect congratulating him on his win and offering recommendations for working with the tech sector. “We stand ready to help your Administration tap into 21st century innovation to achieve prosperity for the nation,” read the letter from a coalition of 17 tech trade groups The letter was signed by leaders from trade associations including the Information Technology Industry Council and Internet Association, which represent companies such as Google, Facebook and Intel.

The Daily Caller **Now Is The Time To Protect American’s Privacy Abroad**
The Daily Caller published an op-ed by Andrew Langer, President of the Institute for Liberty, urging Congress to pass the International Communications Privacy Act (ICPA). Langer details that the bipartisan bill will ensure individual privacy and will create a structure for “greater transparency and accountability in how the US works with other governments in accessing individuals’ private electronic data in ongoing law enforcement investigations.”

Wall Street Journal **Microsoft, Intel, IBM Push Back on China Cybersecurity Rules**
Tough new Chinese cybersecurity rules are providing a rare, behind-the-scenes look at a regulatory skirmish between U.S. technology companies and Beijing. China is moving to require software companies, network-equipment makers and other technology suppliers to disclose their proprietary source code, the core intellectual property running their software, to prove their products can’t be compromised by hackers. Tech companies are loath to offer up their source code, saying this will heighten the risk of their code falling into the hands of rivals or malefactors—and may not guarantee it is hack-proof. Microsoft Corp., Intel Corp. and International Business Machines Corp. are among those filing objections.

Techdirt **China Files A Million Patents In A Year, As Government Plans To Increase Patentability Of Software**
Techdirt has been following for some years China's embrace of patents, loudly applauded by Western companies who believe this will give them more power there. The country has just passed a notable milestone in this area: China is driving Asian-led growth in innovation

worldwide, becoming the first country to file 1 million patent applications in a single year, the World Intellectual Property Organization (WIPO) said on Wednesday. Chinese innovators filed most of their 2015 applications in electrical engineering, which includes telecoms, followed by computer technology and semiconductors, and measurement instruments, including medical technology, the U.N. agency said.

The Hill **A political temper tantrum at the FCC**
The United States just went through a brutal election season. Politics is a nasty game. But now that the election is over, we must — in the immortal words of Abraham Lincoln — come together and embrace the better angels of our nature. Unfortunately, Federal Communications Commission (FCC) Chairman Tom Wheeler did not get the memo. Two days after the election, Wheeler announced an aggressive agenda for the FCC's Nov. 17 open meeting to push through some of his remaining high-priority items, including, among other things, mandating a massive rate reduction for Business Data Services without any economic justification for the naked benefit of select constituencies.

Lawfare **Exceptional Access in a Trump Administration**
Lawfare published a blog by Matt Tait, CEO and founder of Capital Alpha Security, challenging arguments that government should abandon efforts to obtain “exceptional access” to encryption in light of the incoming Trump administration. While Tait believes that legal safeguards and bureaucracies will prevent the Trump administration from institutional misuse of surveillance powers, he warns that preventing exceptional access will force law enforcement to rely on hacking to obtain information and make it harder to identify misconduct by the Trump administration.

Scientific American **Trump’s First 100 Days: Technology, Privacy and Intelligence**
President-elect Donald Trump’s views on technology and tech policy were not prominent campaign features on his contentious path to the White House. However, his repeated calls to dismantle the Washington, D.C., establishment provide some clues to how his first 100 days in the White House will impact the nation’s tech infrastructure and its approach to data privacy for years to come. Trump’s first major shift in tech policy will likely target the U.S. Federal Communications Commission (FCC), where he may seek to reverse key policies from Obama’s presidency that affect "Net neutrality."

Computerworld **Some tech firms welcome Trump’s H-1B reforms**
IT services firms that hire U.S. workers and don't offshore work are looking forward to President-elect Donald Trump's crackdown on H-1B visa use. This includes firms such as Rural Sourcing Inc. (RSI), an Atlanta-based domestic software development company. RSI employs about 350 people and doesn't hire workers on temporary visas. It has four development centers

in Augusta, Ga.; Mobile, Ala.; Jonesboro, Ark.; and in Albuquerque, New Mexico, where a new center opened this year.

Notable Quotes

"But what Parliament can and must do is look again at measures which constitute mass interference into people's privacy. Parliament may be forced to re-legislate several of the measures in the Bill, as a consequence of legal actions that are soon to come back, so this request for a debate gives a timely opportunity to consider the issues that will be brought up by the courts."

– Jim Killock, executive director, Open Rights Group

"Perhaps the most controversial aspect of the new law is that it will give the British government the authority to serve internet service providers with a "data retention notice," forcing them to record and store for up to 12 months logs showing websites visited by all of their customers. Law enforcement agencies will then be able to obtain access to this data without any court order or warrant. In addition, the new powers will hand police and tax investigators the ability to, with the approval of a government minister, hack into targeted phones and computers. The law will also permit intelligence agencies to sift through "bulk personal datasets" that contain millions of records about people's phone calls, travel habits, internet activity, and financial transactions; and it will make it legal for British spies to carry out "foreign-focused" large-scale hacks of computers or phones in order to identify potential "targets of interest."

– Center for Research on Globalization

"Whether the internet is a "public good" is a question that has so far focused primarily on anxiety about government intervention into our digital lives. We are rightly concerned that Donald Trump will soon get his hands on the NSA, and that Britain's snooper's charter legitimises rather than limits the vast intrusions exposed by Snowden. But just as the internet knows no international borders, neither does it recognise outmoded distinctions between state and corporate power, citizens and consumers and platforms and products."

– Rachel Holmes, freelance writer

VFI Executive Briefing
A weekly roundup of technology news
November 28-December 2, 2016

"We now live in a digital world. We are digital citizens. We have no choice about whether or not we engage online. This bill has fundamentally changed how we are able to privately and securely communicate with one another, communicate with business, communicate with government and live an online life. And that's a real, profound concern."

– Renate Samson, chief executive, Big Brother Watch

"In the run-up to the Second Circuit's decision, a lot of folks pointed to the odd results that might follow from ruling for Microsoft. But here's what I (and others) missed: I didn't expect that major domestic providers would respond to a ruling that they can't be compelled to disclose foreign-stored emails pursuant to a warrant by refusing to disclose foreign-stored contents voluntarily when the target was domestic and the only reason that particular e-mail was foreign-stored at that instant was the fluid nature of the network's architecture."

– Orin Kerr, law professor, George Washington University

"Will Trump be asking GCHQ to do more of the same? Is our government capable of resisting these requests, when they are made in secret, and the cost of resistance could be cutting off tools they rely on? Oversight of this state of dependency between the UK and USA is woeful in the UK. If we want our future to be safe, this is time to rethink how surveillance is governed and overseen."

– Open Rights Group

"The bottom line here is simple: Americans would be outraged if a foreign government forced a company to hand over our data, simply on the justification that the data wasn't being stored within that nation's borders. The same would holds true if we did the same — after all, the United States has started wars over less. Now is the perfect time to pass ICPA—it's bipartisan, it protects privacy, and it ought to be a relatively "easy lift" during the lame duck. Congress just needs to take the next step and actually pass it."

– Andrew Langer, president, Institute for Liberty

VFI Executive Briefing
A weekly roundup of technology news
November 28-December 2, 2016

"On November 9th in America, we woke up to a new administration promising radical change. It was a firm reminder that institutions like ours, built for the long-term, need to design for change. For us, it means keeping our cultural materials safe, private and perpetually accessible. It means preparing for a Web that may face greater restrictions. It means serving patrons in a world in which government surveillance is not going away; indeed it looks like it will increase. Throughout history, libraries have fought against terrible violations of privacy—where people have been rounded up simply for what they read. At the Internet Archive, we are fighting to protect our readers' privacy in the digital world."

– Internet Archive of Canada

"Even before the election we had made the decision to host at least Canadian materials in Canada. They have rigorous privacy rules because they don't particularly like patients' privacy information going to the United States."

– Brewster Kahle, founder, Archive.org

"Put simply, if President Trump wishes to illegally misuse law enforcement and to steamroll over all norms and internal safeguards, then encryption will not stop him. But his abuses will be easier to achieve and easier to hide if law enforcement uses hacking as its default, go-to investigative technique. Conversely, such abuses will be harder to secretly conduct if law enforcement's default investigative technique requires co-opting or tricking multiple organizations as part of a split-key decryption process, where each organization can demand to see and validate a judicial warrant prior to decryption, and where the illegal request will be forever, indelibly chiseled onto a public ledger."

– Matt Tait, CEO and founder, Capital Alpha Security

"This is why the Law Society of England and Wales was so deeply concerned when the Investigatory Powers Bill was first introduced without protections for legally privileged material. The final Bill that has just received Royal Assent is, in our view, far from perfect. The ability to intercept privileged communications is too wide and intrusive, and needlessly so. However, following the efforts we and others in the legal profession made, the Government has responded by making considerable improvements from where the Bill began. Proper processes to evaluate and protect legally privileged material now exist, even if the standard is not as rigorous as we would have made it."

– Patrick Bourns, President, Law Society of England and Wales

VFI Executive Briefing
A weekly roundup of technology news
November 28-December 2, 2016

Social Highlights

- **@ABC:** Sweeping UK spy bill dubbed "Snoopers Charter" becomes law
- **@glynnmoody:** German interior ministry wants 2 diminish citizens' data #privacy rights - hey, was gibt's, Germany? #dataprotection
- **@JZdziarski:** Tech Companies: You've got just shy of two months to adapt customer data privacy to take into account your own government as an adversary.
- **@mattburgess1:** Petition against #IPBill (Snoopers charter) has reached 100,000 signatures. MPs' will consider a debate
- **@OpenRightsGroup:** "With #IPBill, they will be able to hack, read and store any information from any citizen's computer or phone"
- **@politico:** Civil liberties groups want @POTUS to rein in the federal surveillance apparatus before Trump takes over | AP
- **@alantravis:** British state surveillance bill becomes law: a "world-leader" or a template for authoritarian regimes around the world?
- **@BIUK:** The Queen just approved the UK Government's mass surveillance bill
- **@ericgeller:** European ministers will discuss a proposal for an EU encryption backdoor mandate on Dec. 9:
- **@guardiannews:** The Kremlin is tightening its grip on Russia's Internet
- **@MorningConsult:** Justice Department Pushes Back on Government Hacking Concerns via @BrendanBordelon
- **@OrinKerr:** What's happening with Internet privacy after the Microsoft case? The answer may surprise you.
- **@RCalo:** @OrinKerr That's totally defensible. But note you're basically saying representatives from Google and Yahoo! confirmed how they store data.
- **@RCalo:** @OrinKerr Interesting, but: 1. Courts decide cases on facts before them, 2. Maybe companies should know where user data is...
- **@dnvolz:** FBI to gain expanded hacking powers at midnight as efforts by @RonWyden to block Rule 41 change fails... tip @Techmeme
- **@WSJ:** Microsoft, Intel, IBM push back against China's new cybersecurity rules
- **@TheLawSociety:** Investigatory Powers Act, and why confidentiality matters