

VFI Executive Briefing

A weekly roundup of technology news

February 13 – 17, 2017

TABLE OF CONTENTS

Hill Update – 1
Special Coverage – 2
Article Summary – 2
Notable Quotes – 6
Social Highlights – 8

HILL UPDATE

Nexgov [Hatch's Innovation Plan: Reform H-1B Program, Protect Federal IT](#)

Sen. Orrin Hatch, R-Utah, wants to allow high-skilled immigrants to support the American tech industry as long as they want to stay in the United States, and their companies aren't abusing the system to offshore jobs.

Axios [Sen. Hatch says he'll be "bridge" between Trump and tech](#)

Orrin Hatch — the octogenarian who chairs the Senate Republican High-Tech Task Force — says he can be tech's ambassador to a White House that has taken positions Silicon Valley hates: "As one of the earliest senators to endorse President Trump, I can serve as a bridge between the president and the tech community." His comments came as part of a larger introduction of his tech agenda for this Congress.

Ars Technica [ISPs ask lawmakers to kill privacy rules, and they're happily obliging](#)

Republican senators are reportedly preparing a legislative move to overturn privacy rules that require ISPs to protect their customers' online data. Sen. Jeff Flake (R-Ariz.) confirmed "that he plans to introduce a resolution that would roll back the FCC's broadband privacy rules via the Congressional Review Act (CRA), which allows Congress to eliminate agency rules with a simple majority vote," Politico reported today. Flake had a dozen co-sponsors on board as of last week, but he hasn't said when exactly he'll submit the resolution. In the House, Rep. Marsha Blackburn (R-Tenn.), chair of the Commerce Committee's Subcommittee on Communications and Technology, "said last week she was speaking with colleagues in the Senate 'daily' about how to best utilize the CRA to undo broadband privacy," the report also said. (Blackburn is a major recipient of donations from the broadband industry.)

Ars Technica [Republican senators concerned about Yahoo's "candor" concerning data breaches](#)

Two senators have given Yahoo CEO Marissa Mayer until February 23 to answer lingering questions regarding the two massive data breaches the company sustained in 2013 and 2014. In a letter sent to Mayer last Friday, Sen. John Thune (R-S.D.) and Sen. Jerry Moran (R-Kan.) write that the company has been "unable to provide answers to many basic questions about the reported breaches." The two senators are the chairs of the Senate Commerce Committee and the Consumer Protection and Data Security Subcommittee, respectively.

The Hill [Intelligence business: Trump must keep privacy protections for US firms](#)

The Hill published a contributed blog by Zachary Goldman, executive director of the Center on Law and Security at NYU's School of Law, urging members of the Senate to press Sen. Dan Coats on the Trump

VFI Executive Briefing

A weekly roundup of technology news

February 13 – 17, 2017

administration's support for PPD-28 and the EU-U.S. Privacy Shield. The Senate is expected to confirm Sen. Coats as Director of National Intelligence after their recess.

Law360 [Tech Groups Call For Balance In Foreign Spying Renewal Push](#)

Law360 reported that a coalition of tech trade groups sent a [letter](#) to Congress urging them to engage in open debate and a "balanced" approach to reauthorization of Section 702 of the Foreign Intelligence Surveillance Act.

SPECIAL COVERAGE – DIGITAL GENEVA CONVENTION

On Tuesday, Microsoft President and Chief Legal Officer Brad Smith published a blog entitled "The need for a Digital Geneva Convention" to respond to the rise in nation-state cybersecurity attacks. In the blog, Brad defines the problem, calls for stronger tech sector responses, describes what Microsoft has done both unilaterally and collaboratively with other tech companies and calls on governments to do more. Brad also urges the tech sector to be the "trusted and neutral Digital Switzerland." In describing this concept, Brad writes

"As the Fourth Geneva Convention relies on the Red Cross to help protect civilians in wartime, protection against nation-state cyberattacks requires the active assistance of the tech sector. We need to start with a clear premise. Even in a world of growing nationalism when it comes to cybersecurity the global tech sector needs to operate as a neutral Digital Switzerland. We will assist and protect customers everywhere. We will not aid in attacking customers anywhere. We need to retain the world's trust. And every government regardless of its policies or politics needs a national and global IT infrastructure that it can trust. This commitment to 100 percent defense and zero percent offense has been fundamental to our approach as a company and an industry. And it needs to remain this way in the future."

I encourage you to read his blog [The need for a Digital Geneva Convention](#) at Microsoft On the Issues.

ARTICLE SUMMARY

LegalTech News [The Cloud Conundrum: Explaining Divergent Google, Microsoft Search Warrant Rulings](#)

LegalTech News published an article highlighting how Magistrate Thomas Rueter's ruling ordering Google to turn over emails stored abroad differs from the precedent set in Microsoft's warrant case. The article compares the two cases, and highlights how existing laws are strained by the realities of cloud computing.

Ars Technica [Twitter to judge: Let us tell everyone exactly how many secret orders we get](#)

Ars Technica, reported on comments made during a Tuesday hearing in [Twitter's lawsuit](#) seeking the right to disclose more information about national security orders directed at the company. During the hearing, District Judge Yvonne Gonzalez Rogers criticized the DOJ's responses to Twitter, accusing the government of using a generic argument about its needs for secrecy that could be "cut and paste" in response to any tech company.

VFI Executive Briefing

A weekly roundup of technology news

February 13 – 17, 2017

Reuters [Microsoft offers patent troll defense for cloud customers](#)

Microsoft Corp has thought up another way to attract potential customers to its cloud computing service: deterrent against patent trolls. Companies new to the cloud are vulnerable to non-practicing entities, which do not make any products themselves but use their arsenal of broad technology patents to sue other firms in order to extract royalties or a cash settlement. The new offering could appeal to companies new to the cloud arena, needing a service such as Microsoft's Azure to store their data or host their mobile app. It was not clear that it alone would be enough to draw customers away from the market leader, Amazon.com Inc's Amazon Web Services.

Ars Technica [A court order blocked pirate sites that weren't supposed to be blocked](#)

One week ago, the news site TorrentFreak reported that The Pirate Bay and nearly 20 other torrent and pirate sites were being blocked by Cogent Communications, an Internet backbone provider. The block had been in place for more than a week and appeared to "appl[y] to the company's entire global network," affecting customers of ISPs "from all over the world" that send traffic through Cogent. Though most Internet users were unaffected, anyone "attempting to pass requests through Cogent's network are unable to access [the sites]," the article said. Cogent CEO Dave Schaeffer yesterday confirmed to Ars that the company is complying with a court order issued recently in Spain. But The Pirate Bay was not the subject of the court order, Schaeffer also confirmed. Schaeffer would not say which site or sites the order was intended to block, but the incident demonstrates how court orders to block websites can have unintended effects. (We have not been able to track down the specific court order at this time.)

The Hill [NY state financial cybersecurity rule taking effect in March](#)

A New York state regulation intended to protect the financial services industry and its consumers from cyberattacks is taking effect in March. Gov. Andrew Cuomo (D) announced the regulation on Thursday, describing it as the first of its kind in the nation. The rule will require banks, insurance companies, and other entities regulated by the state's Department of Financial Services to establish cybersecurity programs to protect consumers' sensitive data and secure the financial services industry. "New York is the financial capital of the world, and it is critical that we do everything in our power to protect consumers and our financial system from the ever increasing threat of cyber-attacks," Cuomo said in a statement on Thursday.

New York Times [Asian Tech Titans Take a Page From Trump's Book](#)

HONG KONG — In his book on deal making, President Trump offered a key piece of advice on getting what you want: Promise big. "I play to people's fantasies," he said in 1987's "The Art of the Deal." "People want to believe that something is the biggest and the greatest and the most spectacular. I call it truthful hyperbole. It's an innocent form of exaggeration — and a very effective form of promotion." Some of Asia's biggest deal makers already understand that principle — and are making big promises accordingly. In recent months, Alibaba's founder, Jack Ma; the Japanese tech investor Masayoshi Son; and the head of Foxconn, Terry Gou, have made big, public plans to invest in America. Together, the deals proposed would help to create more than a million new American jobs and tens of billions of dollars in new investments.

VFI Executive Briefing

A weekly roundup of technology news

February 13 – 17, 2017

Forbes [Calculating The Costs Of Protectionism](#)

A few weeks ago, borne out of the twin pillars of alternative facts' whitewash (or just mendacity for shorthand) and nationalism, Donald Trump was sworn in as America's 45th president. Reality television never got so real. Already, Trump's showmanship entails such mainstays as withdrawing from multi- and plurilaterals, knee-jerk trade theatrics, the threat of scuppering NAFTA and bellicose overtures toward China and Mexico involving the proposed slapping of across-the-board, double-digit duties on imports from these countries. But the smallest common denominator behind these publicity stunts is protectionism. Negative externalities, unnatural concentration of market power and warped regulatory environment accumulate, creating growth-stifling deadweight losses—losses that far exceed any perceived benefits from protectionism.

Wired [Encryption Apps Help White House Staffers Leak—and Maybe Break the Law](#)

IN THE FOUR tumultuous weeks since President Donald Trump's inauguration, the White House has provided a steady stream of leaks. Some are mostly innocuous, like how Trump spends his solitary hours. Others, including reports of national security adviser Michael Flynn's unauthorized talks with Russia, have proven devastating. In response, Trump has launched an investigation, and expressed his displeasure in a tweet: "Why are there so many illegal leaks coming out of Washington?" The answer may have to do with uncertainty and unrest inside the administration, as well as the president's ongoing attacks against the intelligence community. But it doesn't hurt that every White House and Congressional staffer has tools to facilitate secure communication in their pocket or bag.

The Verge [Want to protect your data at the border? Delete it](#)

It's getting harder and harder to enter the United States with your privacy intact. In the wake of President Trump's executive orders on immigration, travelers have reported increasingly invasive stops by border agents. On January 30th, NASA scientist and US citizen Sidd Bikkannavar was coerced into unlocking his phone for Customs agents at the border, possibly exposing sensitive information. Homeland Security leaders are also considering more invasive requirements, like demanding social media passwords from travelers. Legally, customs agents have the right to physically inspect items as they enter the country, part of the legal mandate for keeping contraband from crossing the border. In theory, they're still subject to the Fourth Amendment prohibitions against unreasonable searches, but courts have found that the standard for reasonableness at the border is extremely low, so the prohibitions have little force.

The Register UK [Infosec pros aren't too bothered by Trump – it's his cabinet sidekicks you need to worry about](#)

The Register published an article reporting on concerns voiced by infosec professionals during the BSides conference regarding Attorney General Jeff Sessions' support of encryption backdoors.

Morning Consult [PTO, Courts and Congress Must Solve the Patent Troll Problem](#)

Like many industries, real estate is increasingly driven by innovations in technology that enable professionals to deliver services more quickly and efficiently than ever before. From functionality on websites allowing consumers to zoom in on points of interest on a map, to sending those website users alerts via email, to even providing Wi-Fi access in the common areas of buildings, real estate professionals are constantly seeking to provide consumers with improved services and information in a

VFI Executive Briefing

A weekly roundup of technology news

February 13 – 17, 2017

way that is fast, convenient and comprehensive. Unfortunately, the activities described above – which are utilized by the majority of businesses around the country – have also made them the target of patent trolls. Patent trolls use overly broad patents – for example, regarding the provision of Wi-Fi access – to threaten litigation and extort payments from real estate businesses across the country. Increasingly, these patent trolls are targeting small businesses, which are not likely to have sufficient resources to fight a long and costly legal battle and are more likely to take the trolls' settlement offers.

Wall Street Journal [Trump Takes on Tech Industry in Early Policy Moves](#) (subscription required)

In his first weeks in office, President Donald Trump has shown a readiness to take on the tech industry, clashing with Silicon Valley in ways that his tech-friendly predecessor hardly ever did. The president's executive order on immigration, which generated an outcry from the industry, was only the beginning. Trump-appointed regulators have begun scaling back net-neutrality regulations that marked one of the tech industry's most significant victories during the Obama era. That rule requires that internet service providers don't give priority to some traffic—a policy that companies like Facebook and Netflix like, because it assures them the same basic treatment that rivals would get.

Wired [Millions Need the Broadband Program the FCC Just Put on Hold](#)

EVEN BEFORE AN electrical fire burned her house down in 2014, Jennifer Sneider had trouble affording home internet. A little more than a year after the fire, she and her young son joined a program that fast-tracked them into a spot in a Sarasota, Florida, public housing complex. But the spot came with a condition: Sneider had to get a job or go back to school. She did both, landing a waitressing gig at a local pizzeria and enrolling in an online GED program in hopes of eventually getting her nursing degree. Still, getting an online degree is hard without an internet connection at home. Sneider had to do most of her work at the library, which was an hour away by bus and cost her \$5 roundtrip. Meanwhile, her son Andre, now 7, struggled to complete his online homework assignments without access to the web.

IPWatchdog [Does Patented Intellectual Property Still Matter? Yes, Depending on Who You Are](#)

The value of patents resides largely with companies like Microsoft, Samsung and IBM. If Bill Hewlett and David Packard were just starting in their garage, they might be wise not to waste money acquiring them. "To promote the Progress of Science and useful Arts, by securing for limited Times to Authors and Inventors the exclusive Right..." (Article 1, Section 8, Clause 8 of the United States Constitution). It is difficult to argue today that this applies to individual inventors or small and medium-sized enterprises (SMEs). The same is true about our elite research universities. If a patent assertion entity (PAE) – a small group of investors who buy someone else's patents and threaten others with infringement lawsuits or a "small financial contribution" – assumes ownership of patents and asserts them against an infringer, we holler "patent troll".

New York Times [What Are Your Rights if Border Agents Want to Search Your Phone?](#)

Haisam Elsharkawi was about to travel from Los Angeles to Saudi Arabia last week when, he says, he was stopped at the airport, questioned, handcuffed, questioned some more and then released without charges three hours after his flight had departed. Mr. Elsharkawi, 34, an American citizen, said in an interview on Monday that officers from United States Customs and Border Protection repeatedly pressured him to unlock his cellphone so that they could scroll through his contacts, photos, apps and social media accounts. He said they threatened to seize the phone if he did not comply. "I travel all the time, and I was never asked to unlock my phone," said Mr. Elsharkawi, an electronics salesman from

VFI Executive Briefing

A weekly roundup of technology news

February 13 – 17, 2017

Anaheim, Calif. “I have personal photos there, which I think is normal for anyone. It’s my right. It’s my phone.”

Irish Times [US Law Allows ‘Extraordinary Access’ To Private Data, Court Told](#)

The Irish Times reported on comments made in the Irish High Court by ACLU staff attorney Ashley Gorski regarding the U.S. government’s authority to obtain access to the communications data of non-Americans overseas. Gorski, who was testifying as part of the case examining the legality of Facebook’s transatlantic data transfers, argued that the Foreign Intelligence Surveillance Act and Executive Order 12333 provide the U.S. government “extraordinary access” to the private communications of people around the world.

Ars Technica [American Spies: How We Got To Mass Surveillance Without Even Trying](#)

Ars Technica published an article reviewing [a new book](#) by Jennifer Granick, director of civil liberties at the Stanford Center for Internet and Society, analyzing the evolution of national surveillance law and government surveillance practices over the past few years.

Notable Quotes

“Today, we live under a confusing, convoluted, and technologically outdated legal regime that has left American privacy with uncertain legal protection. The uncertainty is exacerbated by the fact that so much surveillance—both law enforcement and intelligence—is secretly authorized via sealed and ex parte court proceedings.”

– [Jennifer Granick, director of civil liberties, Stanford Center for Internet and Society](#)

“We have pretty readily exposed ourselves in order to get cool free services from Facebook, Google and myriad other companies. But new technologies are starting to eat away at our privacy in ways we’ve never before experienced. And now the Trump administration wants to guard your data about the way a cat might offer to guard a bird feeder. Trump apparently plans to let security organizations such as the National Security Agency (NSA)—and even scarier ones like Comcast—grab your data and use it just about any way they want.”

– [Kevin Maney, columnist, Newsweek](#)

“Such border searches of Americans’ digital devices and cloud content are unconstitutional absent individualized suspicion, specifically, a probable cause warrant. In light of the DHS secretary’s statements this week, we fear that DHS may soon take the next step down this invasive path and demand the login information for American travelers’ online accounts so that the government can peruse private, highly personal information without relying on access to a mobile device.”

– [Sophia Cope, staff attorney, Electronic Frontier Foundation](#)

VFI Executive Briefing
A weekly roundup of technology news
February 13 – 17, 2017

“The question should therefore be put sharply to Senator Coats: Will he advise the president to conduct the business of intelligence in a way that respects the privacy interests of foreigners and protects the interests of American companies? Or will he abandon PPD 28 and other privacy protections, hindering the ability of American companies to thrive in a globalized world?”

– [Zachary Goldman, executive director, Center on Law and Security at NYU School of Law](#)

“We can’t fix the surveillance problem overnight, but maybe we can build a shield that will protect anyone who’s standing behind it.”

– [Edward Snowden](#)

“Whether we approve of the motive or not, [Michael Flynn’s behavior] is an abuse of surveillance for national security officials to leverage legitimate foreign intelligence collection to reveal public information in order to damage individuals they do not believe should serve. In fact, these kind of abuses (among others) led to the passage of FISA in the first place.”

– [Timothy H. Edgar, director of law and policy, Brown University's Executive Master in Cybersecurity program](#)

“If I had five different cases, one by Twitter, one by Microsoft, one by Facebook and all the other groups that do this social media stuff that none of us judges do, [FBI Assistant Director Michael Steinbach] could have taken this exact same declaration and cut and paste the declaration, switched out the names of the company and I would have the same generic explanation for why it is that the government wants to do what it wants to do.”

– [U.S. District Judge Yvonne Gonzalez Rogers](#)

“It takes a particular bit ofchutzpah to—after insisting that average American citizens shouldn't have formalized legal protections from unwarranted data collection—declare that a person heavily connected to the incoming presidential administration should expect his conversations with high-level Russian officials to be secret. Note that I'm not arguing that it's wrong for Flynn to have had conversations or even wrong to have suggested sanctions might be eased (sanctions often suck as policy and so does the [Logan Act](#)).”

– [Scott Shackford, reporter, Reason](#)

VFI Executive Briefing

A weekly roundup of technology news

February 13 – 17, 2017

“A balanced approach will reflect the need to preserve the intelligence community's ability to collect critical information from foreign sources while also ensuring that there are essential safeguards for digital security and privacy.”

[–Joint Coalition Letter from BSA: The Software Alliance, the Computer & Communications Industry Association, the Consumer Technology Association, the Information Technology Industry Council, the Internet Association and TechNet](#)

“This idea that law enforcement can “poke around” and do anything with lawfully collected information is unreasonable and at odds with basic privacy rights. In passing Section 702, Congress created additional privacy risks for Americans; it did so for a specific foreign intelligence purpose and not with the expectation that a limited foreign intelligence tool would be used freely for domestic law enforcement, overriding stronger Congressional limits in that sphere.”

[– Jake Laperruque, privacy fellow, The Constitution Project](#)

Social Highlights

- **@arstechnica:** [American Spies: how we got to age of mass surveillance without even trying by @cfarivar](#)
- **@BloombergLaw:** [Russia Ups Fines for Data Protection Violations](#)
- **@EFF:** [DHS is embarking on a broad campaign to invade the digital lives of innocent people.](#)
- **@Newsweek:** [Snap's IPO might be a huge win for privacy](#)
- **@nxtthompson:** [You can be a citizen, and work for NASA, and Customs might still demand your phone.](#)
- **@reckless:** [This is shocking, embarrassing, and doesn't make anyone safer from anything.](#)
- **@IBTimes:** [A NASA scientist who's a U.S. citizen was detained at the border and ordered to turn over his phone](#)
- **@Snowden:** [ICYMI on Friday: @ACLU went to an Irish court to protect your rights, and @Facebook went against them to undermine those very same rights.](#)
- **@TechCrunch:** [ACLU calls for tech firms to lobby for surveillance reform](#)
- **@WIRED:** [For the past year, Edward Snowden has quietly run a nonprofit to protect reporters from government surveillance.](#)
- **@benghancock:** [Google Lawyer Says Framework Needed to Govern Cloud Data via @santaclaralaw @SCUHTL](#)
- **@EFF:** [.@DevinNunes is angry the FBI recorded Flynn's calls? Where's his outrage over NSA mass surveillance of Americans?](#)
- **@Elizabeth_Joh:** [Raises Q, @OrinKerr : what will police do in the future knowing that people will engage in cellphone data wipes in anticipation of warrant?](#)
- **@WashTimes:** [Twitter argues in federal court for right to disclose surveillance details -](#)
- **@dellcam:** [Letter from @DevinNunes defending surveillance on Americans w/o PC, which enabled NSA to monitor Flynn's call \(via @theintercept\)](#)

VFI Executive Briefing

A weekly roundup of technology news

February 13 – 17, 2017

- **@Joshgreenman:** [It's harder to make the case to crack strong encryption when you are waging war against leakers and terrorists alike.](#)
- **@KevinBankston:** [Glad to see tech groups signaling in this new letter that 702 surveillance reform is a priority for them this year:](#)
- **@ncweaver:** [The cellphone may be wiped, but basically all this data should be available with a warrant to Google in this case:](#)