VFI Executive Briefing
A weekly roundup of technology news
March 6 – March 10, 2017

TABLE OF CONTENTS

HILL UPDATE

The Hill **Chaffetz, Cummings question WH on digital records**
The leaders of the House Oversight Committee on Wednesday raised concerns that President Trump may be violating federal law by deleting his tweets. In a letter addressed to White House counsel Donald McGahn, committee Chairman Jason Chaffetz (R-Utah) and ranking member Elijah Cummings (D-Md.) expressed concern over the White House's digital record-keeping practices. "Many of the messages sent from [Trump's] Twitter account are likely to be presidential records and therefore must be preserved," the two wrote. "It has been reported, however, that president Trump has deleted tweets, and if those tweets were not archived it could pose a violation of the Presidential Records Act."

The Hill **Bipartisan bill would give cybersecurity grants to state and local governments**
Last week, Reps. Barbara Comstock (R-Va.) and Derek Kilmer (D-Wash.), along with Sens. Cory Gardner (R-Colo.) and Mark Warner (D-Va.), introduced the State Cyber Resiliency Act, which would fund Federal Emergency Management Agency–administered grants for cybersecurity planning and implementation. [...] "Cities manage substantial amounts of sensitive data, including data on vital infrastructure and public safety systems. It should come as no surprise that cities are increasingly targets for cyberattacks from sophisticated hackers" [...] "Cities need federal support to provide local governments with the tools and resources needed to protect their citizens and serve them best."

The Hill **Time for a cybersecurity grant program for the states**
Congress and DHS should show their seriousness about states' cyber defenses by directing some of President Trump's $1 trillion infrastructure investment toward expenditures on shoring up states' critical cyber infrastructure. This is an imperative stemming from the persistent and growing gap between the cyber threat to state governments and their ability to mitigate it. They need federal help.

SPECIAL COVERAGE – Wikileaks Year Zero

On Tuesday, WikiLeaks post thousands of documents pertaining to CIA software tools that can be used to "hack into devices." Calling its collection "Year Zero" WikiLeaks posted 8,761 documents and files. A federal criminal investigation has been opened and officials said the FBI and CIA are coordinating reviews of this matter.

New York Times **WikiLeaks Releases Trove of Alleged C.I.A. Hacking Documents**
WASHINGTON — WikiLeaks on Tuesday released thousands of documents that it said described sophisticated software tools used by the Central Intelligence Agency to break into smartphones, computers and even Internet-connected televisions. If the documents are authentic, as appeared likely

at first review, the release would be the latest coup for the anti-secrecy organization and a serious blow to the C.I.A., which maintains its own hacking capabilities to be used for espionage. The initial release, which WikiLeaks said was only the first part of the document collection, included 7,818 web pages with 943 attachments, the group said. The entire archive of C.I.A. material consists of several hundred million lines of computer code, it said.

New York Times **WikiLeaks Will Help Tech Companies Fix Security Flaws, Assange Says**
WASHINGTON — Julian Assange, founder of WikiLeaks, said on Thursday that the anti-secrecy organization would work with Apple, Google and other technology companies to fix flaws that have allowed the C.I.A. to hack into the phones, computers and other devices they produce. Speaking from London in an online news conference, Mr. Assange accused the C.I.A. of withholding information about the vulnerabilities the agency was exploiting in American technology even after it realized that documents describing the flaws had been leaked weeks ago. While some companies have already fixed the weaknesses revealed in a batch of secret C.I.A. documents made public by WikiLeaks on Tuesday, Mr. Assange said, others say they need more technical information on the hacking techniques.

New York Times **With WikiLeaks Claims of C.I.A. Hacking, How Vulnerable Is Your Smartphone?**
WikiLeaks on Tuesday released a significant cache of documents that it said came from a high-security network inside the Central Intelligence Agency. WikiLeaks called the documents Vault 7, and they lay out the capabilities of the agency's global covert hacking program. By the end of 2016, the C.I.A. program had 5,000 registered users, including government employees and contractors. And they had produced more than a thousand hacking systems. The agency's arsenal, the documents indicate, included an array of malware ranging from viruses to clandestine "zero day" vulnerabilities in the software of major companies. The files have circulated among former United States government hackers and contractors in "an unauthorized manner, one of whom provided WikiLeaks with portions of the archive," WikiLeaks said.

Wired **How the CIA's Hacking Hoard Makes Everyone Less Secure**
WHEN WIKILEAKS YESTERDAY released a trove of documents purporting to show how the CIA hacks everything from smartphones to PCs to smart televisions, the agency's already shadowy reputation gained a new dimension. But if you're an average American, rather than Edward Snowden or an ISIS jihadi, the real danger clarified by that leak wasn't that someone in Langley is watching you through your hotel room's TV. It's the rest of the hacker world that the CIA has inadvertently empowered. As security researchers and policy analysts dig through the latest WikiLeaks documents, the sheer number of hacking tools the CIA has apparently hoarded for exploiting zero-day vulnerabilities—secret inroads that tech firms haven't patched—stands out most. If the US intelligence community knows about them, that leaves open the possibility that criminal and foreign state hackers do as well.

Recode **Apple says it's working to fix security holes revealed by the WikiLeaks release of CIA documents**
Apple says it's working to fix any holes the CIA may have exploited in what appears to be a number of spying programs the agency employed. Yesterday, the whistleblowing website WikiLeaks released a cache of more than 8,000 documents that detail classified CIA cyberspying programs. According to the

leaks, the CIA has a trove of malware that can undermine security and encryption measures on Apple's iPhones, Mac OS operating system and AirPort routers, as well as Google Android phones, machines running Windows operating systems, Samsung smart TVs and other connected devices.

The New York Times **Wikileaks Reignites Tensions Between Silicon Valley and Spy Agencies**
The New York Times published an article positioning yesterday's Wikileaks release of CIA hacking techniques as the latest chapter in the ongoing feud between tech companies and the U.S. government over trust and access to data. The article highlights numerous examples of tension between the two sides, including the San Bernardino iPhone fight and pushes to reform surveillance post-Snowden.

ARTICLE SUMMARY

NBC News **Comey: FBI Couldn't Access Hundreds of Devices Because of Encryption**
NBC reported on comments from FBI Director James Comey regarding encryption and issues of U.S. intelligence. Speaking at Boston College's cybersecurity conference, Director Comey stated that "absolute privacy" does not exist in America, going on to note that ubiquitous strong encryption has "shattered" America's historical bargain on achieving both privacy and security. Comey also said that the FBI was unable to access about 43% of the 2,800 devices for which it had had lawful authority to access in the final three months of 2016.

New York Times **How Trump Became the First Silicon Valley President**
Last summer, not long after Donald J. Trump secured the Republican nomination for president, his recently installed campaign manager, Stephen K. Bannon, met with top officials from the Republican National Committee to discuss management of the general election. Mr. Trump's staff had remained unusually small throughout the grueling primaries — a compactness, his advisers believed, that had given them a nimble edge. Now most Republican officials expected the Trump team to expand as it began to oversee the thousands of Republican staff members, state officials and consultants who would be ground troops in the coming political war.

Forbes **Digital Privacy Rights Take A U-Turn, And Congress Needs To Act**
Forbes published a contributed article by Craig Newman, partner at Patterson Belknap Webb & Tyler, highlighting how two recent magistrate rulings involving SCA warrants directed at Google and Yahoo stand in opposition to the precedent set by Microsoft's warrant case victory. Newman notes that the judges' rebuke of the Second Circuit ruling mean that the "failings of the SCA have now played out in three high-profile decisions with wide-ranging implications," and are further evidence of the need for Congress and the Trump administration to update the statute. Steptoe & Johnson partners Michael Vatis and Stewart Baker briefly discussed the impact of the magistrate rulings during a segment on the Steptoe Cyberlaw Podcast, with neither expressing much optimism that Congress will move quickly on the issue.

Recode **Trump's possible pick for FTC chair might have to recuse himself in cases involving Google, Facebook or Microsoft**
Utah Attorney General Sean Reyes, considered one of the leading candidates for chairman of the Federal Trade Commission, has over the course of his campaigns received more than $60,000 in

contributions from tech companies such as Facebook, Microsoft and Google. That means if President Donald Trump appoints Reyes to the FTC, there's a chance Reyes would have to recuse himself from cases involving those companies, according to a source close to the FTC. Other FTC experts said the federal agency had little or no experience in dealing with commissioners who have received campaign contributions and if that would put him under pressure to recuse himself from cases. It's still unclear if ethics regulations would apply in the case of campaign contributions, but experts say the issue for Reyes would come down to any appearance of conflict.

Mashable **Why won't Trump talk about technology?**
Vice President Mike Pence's embarrassing use of an AOL email account is just another painful reminder of something that should be crystal clear to everyone: this administration doesn't understand or care a lick about technology. It's an especially painful reality as we come off the high of an administration's 8-year-love affair with technology and social media. They held Maker Fairs on the White House Lawn, for heaven's sake. Former President Barack Obama personally fired a marshmallow canon during the White House science fair. Obama was so enthralled by technology and innovation that he made it a centerpiece of his 2013 State of the Union Address.

The Hill **The importance of balanced patent policy**
Policy tends to swing back and forth like a pendulum before settling on the right balance. Sometimes the worst thing you can do for your cause is to overshoot your mark and set-up a bigger backswing that undoes all of your efforts. Those of us that want sound and lasting patent reform must be cautious that the pendulum doesn't swing too far and hurt legitimate patent enforcement. Not only would this hurt innovation long-term, it would also risk the policy pendulum swinging back to allow patent trolls and other opportunists to continue to take advantage of the patent system to harm main street businesses with bogus patent infringement suit threats.

Washington Post **How Foxconn's broken pledges in Pennsylvania cast doubt on Trump's jobs plan**
HARRISBURG, Pa. — For some residents of this small city, there was something familiar about Foxconn's recently announced plan to hire up to 50,000 U.S. workers, one of the many hiring pledges from companies rounded up by President Trump in the first weeks of his administration. The only difference was the scale. In 2013, Foxconn's chairman sent a jolt through this state capital when he said his company — best known for making Apple iPhones in China — would invest $30 million and hire 500 workers for a new high-tech factory in central Pennsylvania. Locals were giddy. Foxconn had a small office here, but this seemed like the start of an entire new industry. Pennsylvania's governor boasted about the deal. The Brookings Institution think tank hailed Foxconn's decision as a sign of U.S. manufacturing's strength.

Recode **Trump's administration will be making it harder to get H1-B visas starting in April**
United States Immigration and Customs Services has announced that, starting in April, it will no longer offer its 15-day "premium processing" program for applicants of H-1B visas. H-1B visas allow employers to temporarily hire non-U.S. born workers to take highly skilled positions at U.S. companies. These visas are frequently used at large technology companies to bring top engineering talent to their U.S. offices. The U.S. only allows 85,000 people per year to enter the country on H-1B visas. The announcement

means that new H-1B visa applications could take months to process. With premium processing, U.S. immigration services offered a 15-day expedited service for a $1,225 filing fee, but come April that will no longer be an option.

IPWatchdog **European Patent Office grants more patents to US companies than ever before**
Brussels/Munich, 7 March 2017 – The number of patents granted to US companies by the European Patent Office (EPO) grew by 46.7% in 2016, the highest increase in ten years, and a new record high. Last year US companies were granted 21,939 patents by the EPO (2015: 14,955). (Fig. Growth of patents granted by the EPO to applicants from the US) Patent applications from the US had enjoyed an unusual surge in 2015 (at 42,597) due to the one-off effect of a change in US patent law (America Invents Act of 2013), but have now decreased again (by -5.9%) to 40,076, which is still 9.3% higher than the 2014 figure (36,668). (Fig. Growth of patent applications at the EPO from the US).The US still remained by far the biggest patent applicant at the European Patent Office in 2016, accounting for a 25% share of all applications filed with the EPO.

Ars Technica **Industry, and Apple, opposing "right to repair" laws**
Ahead of a 2010 decision by federal regulators to legalize mobile phone jailbreaking, Apple had cautioned US Copyright Office officials that doing so would have "potentially catastrophic" (PDF) consequences because hackers wielding jailbroken iPhones might take down the nation's mobile phone networks. Clearly, Apple's scare tactics were designed to protect its own business model—as jailbroken phones can bypass Apple' App Store and get apps elsewhere. Apple is now taking a page out of that anti-jailbreaking campaign in a bid to scuttle a so-called "right to repair" law (PDF) in Nebraska, where its Legislature is scheduled to debate the measure Thursday. Eight states, including Nebraska, are considering right to repair laws that would require companies, whether they are in the tech sector or not, to make their service manuals, diagnostic tools, and parts available to consumers and repair shops—and not just select suppliers.

Associated Press **Amazon shares data with Arkansas prosecutor in murder case**
The Associated Press reported that Amazon handed over Echo data requested by law enforcement in an Arkansas murder investigation. In a stipulation filed Monday, Amazon noted that the defendant in the case consented to allow police to review the information retained on the device, and therefore their motion to quash the warrant is now moot.

Notable Quotes

"Section 702 has been a far more impactful and important counterterrorism program and tool. That doesn't mean though that we shouldn't explore whether there are ways to improve any of the protections in existing law or whether there are any changes that we need to make to the structure of the program."

–Rep. Adam Schiff

VFI Executive Briefing
A weekly roundup of technology news
March 6 – March 10, 2017

"There is no such thing as absolute privacy in America. That's the bargain. And we made that bargain over two centuries ago to achieve two goals. To achieve the very, very important goal of privacy, and to achieve the important goal of security. Widespread default encryption changes that bargain. In my view it shatters the bargain… The advent of default ubiquitous strong encryption is making more and more of the room in which the FBI investigates dark."

– FBI Director James Comey

"Yet the fact that evidence scooped up by the American surveillance state while it spies on foreign intelligence operatives might end up in a criminal case brought against an American citizen should give President Trump pause, particularly given the F.B.I.'s reported ongoing investigation into alleged contacts between Trump advisers and Russian intelligence and government officials."

– Steve Coll, staff writer, The New Yorker

"Human Rights Watch agrees with the rapporteur that many of these [U.S. surveillance programs] have not been justified as necessary and proportionate to addressing legitimate aims, and are especially problematic where states fail to respect the right to privacy of persons outside their borders. Abuse of data collected in bulk also remains a primary source of concern, particularly given the lack of independent judicial oversight of such practices in many countries."

– Human Rights Watch

"The magistrates' collective rebuke to the Second Circuit decision raises questions about the legal protections and business implications of moving vast stores of electronic data seamlessly across international borders, evolving privacy expectations, the legitimate needs of law enforcement and Congress' inexplicable failure to update a hopelessly outdated law."

–Craig Newman, partner, Patterson Belknap Webb & Tyler LLP

"We've long argued that the surveillance programs under Section 702 are not targeted, do not have sufficient oversight, and violate Fourth Amendment protections. That's why we're calling on Congress to let the authority sunset."

– Kate Tummarello, policy analyst, Electronic Frontier Foundation

"The police cannot force you to tell them the passcode for your phone. Forcing you to turn over or type in your passcode violates the Fifth Amendment privilege against self-incrimination—the privilege that allows people to 'plead the Fifth' to avoid handing the government evidence it could use against them."

– Jamie Lee Williams, staff attorney, Electronic Frontier Foundation

VFI Executive Briefing
A weekly roundup of technology news
March 6 – March 10, 2017

"I am pleased that we will have access to the data from the defendant's Echo device since the defendant consented to its release… As with any case, our obligation is to investigate all of the available evidence, whether the evidence proves useful or not. Since this case is ongoing, I cannot comment on the specifics of the recording or whether it will be used in court."

– Nathan Smith, prosecuting attorney, Benton County Prosecutor's Office

"I am deeply concerned that the right to privacy will simply not experience a full transition to the digital age. In general, laws have been drafted and rushed through the legislative process of States with clear political majorities to legitimize practices that should never have been implemented."

– Joseph Cannataci, Special Rapporteur on the Right to Privacy, United Nations

"The Foreign Intelligence Surveillance Act (FISA), which Congress passed in the aftermath of President Richard Nixon's use of the CIA and the FBI to spy on his political opponents, has unleashed demons that now seem beyond the government's control and are more pervasive than anything Nixon could have dreamed of."

– Andrew Napolitano, senior judicial analyst, FOX News

"Human rights are universal and cyberlaw should exist in such a way not only to protect privacy but also other fundamental human rights."

– Joseph Cannataci, Special Rapporteur on the Right to Privacy, United Nations

Social Highlights

- **@Law360:** Murder suspect consents to @amazon giving up Echo audio data:
- **@lawfareblog**: Stewart Baker: Steptoe Cyberlaw Podcast: Fancy Bear, Cozy Bear, and … Sneaky Bear?
- **@threatpost:** Comey: @FBI has 1,200 devices it can't crack -
- **@zackwhittaker:** Amazon was probably never going to win, anyway.
- **@EFF:** Dan Coats has a troubling history of supporting government surveillance.
- **@ggreenwald:** The U.S. government's privacy watchdog is basically dead, emails reveal by @JennaMC_Laugh
- **@realdanstoller:** Companies Can't Hide From U.S. #Surveillance Renewal Debate
- **@techreview:** National laws that restrict encryption will only push people to switch to foreign messaging apps like Line or Viber.
- **@NPR:** There are significant differences between the Snowden case and WikiLeaks' alleged CIA trove
- **@reason:** How Post-Nixon Reforms Created Today's Spy Agency Monsters
- **@SteveKopack:** Comey, in Boston cyber summit comments, says he wants "neither" weaker encryption or 'backdoors' into technology & personal devices