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

TABLE OF CONTENTS

HILL UPDATE

Homeland Preparedness News **House Small Business Committee holds hearing on coordinating federal resources for cybersecurity**
During a hearing with the U.S. House Small Business Committee, a panel of experts said that the government must do a better job coordinating federal resources to protect the country's small businesses from various cybersecurity threats. [...] "A cyber attack can have serious consequences, not only for small businesses, but also their customers, employees, and business partners," U.S. Rep. Steve Chabot (R-OH), committee chairman, said. "Sixty percent of small businesses that fall victim to a cyber attack close up shop within six months. A 2014 survey from the National Small Business Association estimated the average cost of a cyber attack on a small business to be over $32,000."

CNN **Congressman: We need a National Guard for cybersecurity**
"I think our government should look like our country," said Will Hurd, a Republican from Texas. "We need a diversity of thought, backgrounds and experiences. The issue of the most talented folks not going into government is true, it's not just in the legislative or executive branch." A cybersecurity reservist group could occasionally be called on to protect the country against cyber threats, and strengthen national security on the digital level. That could include finding and patching bugs, upgrading outdated systems, and auditing current technology.

Politico **Senate Approves Coats As New Spy Chief**
As part of their coverage of the confirmation of Dan Coats as Director of National Intelligence, Politico and The Hill highlighted comments from Senator Wyden about Section 702 surveillance and Coats' stance on reauthorization. Senator Wyden took to the Senate floor before the confirmation vote to express his concerns that Coats still has not fully committed to providing Congress with an estimated number of Americans spied on under Section 702 programs.

ARTICLE SUMMARY

The Hill **Trump's budget proposal gives DHS $1.5 billion for cybersecurity**
The budget request, which bolsters DHS funding by 6.8 percent while making deep cuts to other agencies and departments, also calls for heightened cooperation between the government and the private sector on cybersecurity. The proposed budget "safeguards cyberspace with $1.5 billion for DHS activities that protect federal networks and critical infrastructure from an attack," according to the blueprint, which was publicly released Thursday morning.

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

Business Insider **Apple, Amazon, and Microsoft are helping Google fight an order to hand over foreign emails**
Apple, Microsoft, Amazon, and Cisco have filed an amicus brief in support of Google, after a Pennsylvania court ruled that the company had to hand over emails stored overseas in response to an FBI warrant. An amicus brief is filed by people or companies who have an interest in the case, but aren't directly involved. In this case, it's in Silicon Valley's interest to keep US law enforcement from accessing customer data stored outside the US. It isn't clear what data Google might have to hand over and, last month, the company said it would fight to the order. In the brief, the companies argue: "When a warrant seeks email content from a foreign data center, that invasion of privacy occurs outside the United States — in the place where the customers' private communications are stored, and where they are accessed, and copied for the benefit of law enforcement, without the customer's consent."

Wired **If Trump Fans Love Freedom, They Should Love Net Neutrality**
IMAGINE A WORLD where Comcast slows video streaming from Fox News's website to a pixelated crawl while boosting Rachel Maddow—who happens to star on Comcast-owned MSNBC. What if Verizon, which owns the liberal Huffington Post, charged you more to visit right-wing Breitbart. Or maybe Google Fiber bans access to the alt-right social network Gab. Today, it's illegal to impose tiered pricing on any internet content, thanks to the Federal Communications Commission's net neutrality rules. But if Republicans have their way, those rules will soon disappear, leaving companies like Comcast and Verizon free to block, throttle, or charge a toll to access your favorite websites and apps. The principle of net neutrality asserts that internet service providers should treat all internet traffic the same way, regardless of a site's content or owner—or its politics.

Ars Technica **Senate Democrats question FCC chair's independence from Trump**
US Senate Democrats have asked the Federal Communications Commission chairman for a commitment that the FCC will not try to stifle freedom of the press on behalf of President Donald Trump. The Democrats sent a letter on Friday to FCC Chairman Ajit Pai, saying he did not answer senators' questions at a Senate Commerce Committee hearing held last week. "[Y]our refusal to answer straightforward questions about how you view the media and whether you will uphold the First Amendment rights of journalists and media outlets is concerning," Sen. Bill Nelson (D-Fla.) and 12 other Democratic members of the Senate Commerce Committee wrote in the letter to Pai. As we previously reported, Senate Democrats asked Pai at the hearing if he agrees with Trump's statement that the media is "the enemy of the American people.

Ars Technica **MacroSolve: Donald Trump Jr.'s favorite patent enforcer**
Before President Donald Trump took the oath of office in January, he handed off management of the Trump Organization's business interests to his two eldest sons, Donald Trump Jr. and Eric Trump. The family-owned company has been in various lines of business over the years—most famously, there are hotels, casinos, and golf resorts, some owned and others licensed. Ties, steaks, and a controversial seminar business have also borne the Trump name. But Donald Trump Jr. has also been involved with one particular business with real implications for the technology sector: patent enforcement. Beginning in 2011, Trump Jr. worked for—and owned part of—a company called MacroSolve. While MacroSolve had supported itself selling software for more than a decade, by 2011 its focus had shifted to patent lawsuits as the company's main source of profit.

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

Consumer Affairs **Tech Companies Fight Government 'Gag Orders' On Search Warrant Cases**
Consumer Affairs published an article examining Facebook and Microsoft's recent challenges of overly broad warrants and secrecy orders. The article briefly summarizes Microsoft's secrecy order litigation as well as Facebook's lawsuit in New York challenging 381 search warrants for customer data.

Fortune **How The CIA-Wikileaks Drama Could Reignite The DC-Silicon Valley Feud**
Fortune published a contributed article by James Andrew Lewis, senior vice President at the Center for Strategic and International Studies, examining the tense relationship between Silicon Valley and Washington D.C. in light of the recent WikiLeaks disclosure. Lewis warns that the disclosure could reignite concerns over trust and government access to data, and urges the tech industry and Washington to work towards rebuilding their partnership rather than placing mutual blame.

Politico **Trump's Spying Fixation Gives Surveillance Critics Unexpected Boon**
Politico published an article examining how President Trump's wiretapping allegations have increased Congressional scrutiny of Section 702 surveillance programs. The article reports that civil libertarians and lawmakers are pushing for revisions to Section 702 should it be reauthorized later this year. The Hill reported that the alleged warrantless wiretapping of Trump Tower could have been authorized under Section 702's "backdoor" warrant loophole.

Cyberscoop **Despite open jobs, veterans face problems landing civilian cybersecurity roles**
Coming from a world that's often indecipherable to civilians, veterans face a mountain of challenges entering the cybersecurity workforce despite over a million vacant cybersecurity jobs existing as of 2015 — a number that illustrates an industry begging for new talent. In the U.S. military, career progression doesn't require the certifications and academic degrees that are highly valued in the private sector. There is often no clear cybersecurity career path available when serving.

Notable Quotes

"I'm not sure that there's a program in the national security area that has a more robust compliance regime than FISA and certainly Section 702. There's compliance requirements and review after review after review."
– Greg Brower, head of the Office of Congressional Affairs, FBI

"A replay of the San Bernardino debate won't help anyone. The tech world may have to accept that vulnerability disclosure is not a panacea. Intelligence agencies could do more harm than good if they promise to never exploit a found vulnerability and tell a company immediately when they find one. At the same time, government finger-pointing at Silicon Valley's imperfect software or new love of encryption is similarly unhelpful. Societies gain more from using buggy technology than they lose. This is why consumers continue to accept the tradeoff of less privacy for more services."
– James Andrew Lewis, senior vice president, Center for Strategic and International Studies

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

"The sheer volume of [data retained under the Investigatory Powers Act] will be huge and be incredibly revealing. It will also be a honeypot for cybercriminals. Should we be worrying about when the next hack or data leak will be?"

– Millie Graham Wood, legal officer, Privacy International

"The magistrate judge therefore erred both in looking to policy considerations and in his ultimate conclusion that there is no invasion of privacy when a service provider is compelled by the government to execute an SCA warrant by seizing and copying private communications in another country — and that the only privacy breach occurs upon the later domestic disclosure of the data to the government. The fiction that such a foreign search and seizure is a domestic act was properly rejected by the Second Circuit."

– Joint amicus of Microsoft, Apple, Amazon, and Cisco

"The way it works is, the FISA court, through Section 702, wiretaps foreigners and then [NSA] listens to Americans. It is a backdoor search of Americans. And because they have so much data, they can tap — type Donald Trump into their vast resources of people they are tapping overseas, and they get all of his phone calls."

– Senator Rand Paul

"But Vault 7 is a visceral reminder that the public can't trust the government to keep this stuff safe—hell, not even the government can trust the government to do so. And backdoors present an even more cut-and-dried case than exploits."

– Brett Max Kaufman, staff attorney, American Civil Liberties Union

"We are in a world where if the U.S. government wants to get your data, they can't hope to break the encryption. They have to resort to targeted attacks, and that is costly, risky and the kind of thing you do only on targets you care about. Seeing the CIA have to do stuff like this should reassure civil libertarians that the situation is better now than it was four years ago."

– Nicholas Weaver, professor, UC Berkeley

"Depending on what Schiff and Nunes turn up, this could be a real scandal, particularly if the names of other Trump associates picked up in incidental surveillance were unmasked and distributed widely within the government… This would mean that the Obama administration had effectively short-circuited the FISA process by checking to see if Trump associates were picked up incidentally on existing surveillance, and then disseminating the take widely within the intelligence bureaucracy. "

– Eli Lake, columnist, Bloomberg View

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

"Thanks to the third-party doctrine, the Department of Justice does not believe that people have a reasonable expectation of privacy in phone calling records, Internet transactions, financial records, hard drive backups, or other sensitive data stored with "cloud" Internet services. If they are right, searches of personal data stored online is not protected by the Fourth Amendment."

– Jennifer Granick, director of civil liberties, Stanford Center for Internet and Society

Social Highlights

- **@thehill:** Dem lawmakers want to change loophole that allowed surveillance of Flynn without a warrant
- **@bradheath:** FBI says revealing the source of its iPhone crack might prompt phone makers to adopt stronger encryption or ID other bugs gov't finds useful
- **@businessinsider:** Apple, Amazon, and Microsoft are helping Google fight an order to hand over foreign emails
- **@theintercept:** Edward @Snowden said that if Trump is concerned about wiretapping, he should fix the NSA mass surveillance programs.
- **@bradheath:** Microsoft, Apple, Amazon warn that if U.S. courts can force companies to search customers' foreign data, so can the Russians and Chinese.
- **@ggreenwald:** Rand Paul is Right: NSA Routinely Monitors Americans' Communications Without Warrants
- **@geekwire:** Amazon, Microsoft and Apple back Google in overseas data storage dispute
- **@thehill:** #BREAKING: Senate confirms GOP Sen. Dan Coats as Trump's director of national intelligence
- **@EliLake:** I credit @SalenaZito in the lede to my latest column on why you shouldn't take Trump on wiretaps literally.