VFI Executive Briefing
A weekly roundup of technology news
May 15 – 19, 2017

TABLE OF CONTENTS

HILL UPDATE

International Business Times **Your Data Privacy Could Be Endangered By Senate Bill On Overseas Servers**
The International Business Times reported on the rescheduled Senate subcommittee hearing on law enforcement access to extraterritorial data, noting that the hearing and any ensuing legislative reforms to the Stored Communications Act could have lasting impacts on "the future of data privacy."

Threat Post **PATCH Act Calls for VEP Review Board**
The bipartisan act, sponsored by U.S. Senators Brian Schatz (D-Hawaii), Ron Johnson (R-Wis.), and Cory Gardner (R-Colo.) and U.S. Representatives Ted Lieu (D-Calif.) and Blake Farenthold (R-Texas), calls for the establishment of a VEP Review Board that would consist of the highest-ranking members of the intelligence community. The board mandate would be to formalize the process rather than have it be an ad hoc activity within the Executive Branch.

ARTICLE SUMMARY

Ars Technica **Something about Trump cybersecurity executive order seems awfully familiar**

Last week, amidst the whirlwind surrounding the firing of FBI Director James Comey, President Donald Trump signed his long-promised executive order on federal government cybersecurity. While many of the other orders issued by Trump have been politically fraught, this one is not; it's possibly the least controversial document to be adorned with the president's signature since his inauguration. In fact, aside from some of the more Trumpian language in the order, this Executive Order could have easily been issued by the Obama administration. That's because it largely is based on policies and procedures that were spearheaded by President Obama's staff.

The Jackson Sun **Protecting privacy in the Internet Age**
The Jackson Sun published an op-ed by syndicated columnist Peter Roff examining the issue of lawful access to foreign-stored cloud data. Roff's article highlights the Second Circuit's ruling in Microsoft's warrant case as an example of the need for Congress to address the issue. He notes that legislators need to update the law to "permit the cloud to be more meaningful and useful to everyone while addressing concerns about data privacy and security."

Inside Sources **With Privacy Legislation, Congress Can Safeguard the Digital Domain**
Inside Sources published an opinion piece by David Williams, president of the Taxpayers Protection Alliance, urging Congress to pass ICPA. Williams highlights Microsoft's warrant case as an example of how concerns around lawful access to data stored in the cloud are "particularly acute in the international space" and notes that allowing the federal government to collect data from foreign servers jeopardizes both privacy rights and allied-nation relationships.

VFI Executive Briefing
A weekly roundup of technology news
May 15 – 19, 2017

NextGov **White House Adviser Wants to Move Cyber Risk Decisions Up the Chain**
The Trump administration's goal, he said, is to pinpoint where those outdated or risky systems exist, to make governmentwide decisions about whether those risks are acceptable and to reallocate money to update those systems when the risk is unacceptable. "If we allow individual departments and agencies to fend for themselves, we often will get the lowest common denominator as our weakest link in what is an interlinked federal network," he said.

Washington Post **FCC votes to start rolling back landmark net neutrality rules**
The Republican-led Federal Communications Commission voted Thursday to begin undoing a key decision from the Obama era that could relax regulations on Internet providers. The move highlights the uphill battle for Democrats and consumer advocates, who say that weaker rules could allow Internet service providers to abuse their position as gatekeepers between customers and the rest of the Internet. The current net neutrality rules make it illegal for Internet service providers to block or slow down websites for consumers. ISPs have argued that softening the rules would help them to continue upgrading their networks and find new ways of making money.

The Hill **Senate hearing is huge for media and its use of confidential sources**
The Hill published a contributed opinion piece by conservative columnist Brian McNicoll previewing the rescheduled Senate subcommittee hearing on law enforcement access to data stored abroad. McNicoll highlights Microsoft's warrant case as an example of the need for updated rules governing lawful access to extraterritorial data.

Foreign Policy **Report: NSA Analysts Frequently Broke Rules on Intelligence Collection**

Foreign Policy reported on the recent release of a Foreign Intelligence Surveillance Court opinion revealing that NSA analysts frequently broke compliance rules when searching data collected via the Upstream surveillance program. Just Security published a blog by Emily Berman, assistant law professor at the University of Houston, noting that questions about the legality of "backdoors searches" under Section 702 surveillance should be included in the range of questions posed to any nominee for Director of the FBI.

New York Times **Google, Not the Government, Is Building the Future**
One persistent criticism of Silicon Valley is that it no longer works on big, world-changing ideas. Every few months, a dumb start-up will make the news — most recently the one selling a $700 juicer — and folks outside the tech industry will begin singing I-told-you-sos. But don't be fooled by expensive juice. The idea that Silicon Valley no longer funds big things isn't just wrong, but also obtuse and fairly dangerous. Look at the cars, the rockets, the internet-beaming balloons and gliders, the voice assistants, drones, augmented and virtual reality devices, and every permutation of artificial intelligence you've ever encountered in sci-fi. Technology companies aren't just funding big things — they are funding the biggest, most world-changing things.

Lawfare **Foreign Intelligence Surveillance Court Approves New Targeting and Minimization Procedures: A Summary**
Lawfare published a contributed piece by multiple law fellows and students examining the recently published Foreign Intelligence Surveillance Court (FISC) memorandum order and opinion revealing that NSA analysts frequently broke the rules governing data collection.

Washington Post **The Republican push to repeal net neutrality is likely to get underway this week**
Federal regulators will likely move to roll back one of the Obama administration's signature Internet policies this week, launching a process to repeal the government's net neutrality rules that currently regulate how Internet providers may treat websites and their own customers. The vote on Thursday, led by Federal Communications Commission Chairman Ajit Pai, will kick off consideration of a proposal to relax regulations on companies such as Comcast and AT&T. If approved by the 2-1 Republican-majority commission, it will be a significant step for the broadband industry as it seeks more leeway under government rules to develop new business models.

VFI Executive Briefing
A weekly roundup of technology news
May 15 – 19, 2017

American Spectator **When Patents Are Bad, Property Rights Suffer**
While the debate over patent reform has faced something of a lull, with multiple high-profile policy issues currently eating up a large chunk of Congress's time, this lack of attention should distract nobody. The issue is still alive and well and is very much something that both sides of the aisle should be concerned about, even if the concerns over its abuse remain confined to the policy literature for the time being. That's not to say that the policy literature is all bad, though. Indeed, a new paper from the American Enterprise Institute (AEI) offers plenty of reasons why this issue could and should be a bipartisan success story and yet another jewel in the Trump economy's crown.

Wall Street Journal **Global Tech Companies Call on China to Delay Cybersecurity Law**
Trade groups representing U.S., European and Asian companies called on China to delay a cybersecurity law set to go into force June 1, saying it could discriminate against foreign businesses. The law, adopted late last year, sets up a committee to conduct security reviews of technology products supplied to the Chinese government and critical industries. Its requirements on matters such as technology disclosure and encryption could give local companies a competitive edge, the groups said in a letter reviewed by The Wall Street Journal.

The Hill **Hopes rise Trump will modernize feds' technology**
Tech groups are hopeful the Trump administration will do more to modernize the government's technology systems on the heels of a new executive order on cybersecurity. President Trump's cyber order provides new steps for agencies to boost their security and counter digital threats, and was well received by industry groups. Experts still caution that the cybersecurity changes won't be effective unless the government gets rid of outdated computer systems, which are more vulnerable to security threats.

National Constitution Center **Policing and The Cloud**
The National Constitution Center published a blog highlighting an excerpt from "Policing and the cloud," a white paper by Christopher Slobogin, director of Vanderbilt University's criminal justice program. Slobogin highlights the current state of legal rules governing law enforcement access to data and advocates for a modern regulatory framework that is reflective of constitutional protections and the needs of law enforcement and national security. He notes that until the Supreme Court weighs in on law enforcement access to cloud data, policymakers have a "clean slate" for drafting new rules.

NOTABLE QUOTES

- *"But enabling the federal government to collect wantonly such a wide swath of information on foreign servers opens the door to unintended consequences… The National Security Agency's wide net, operating in a legal gray zone, has also enabled virtual Peeping Toms in the present day. Allowing the government a carte blanche to sweep foreign communications also sets the stage for future confrontations with allied nations, whose citizens will inevitably be thrown into our surveillance net. Commercial and diplomatic relations with the European Union and China have already been harmed by revelations of the NSA's spying program, and the inferred sovereignty violations."*
  – David Williams, president, Taxpayers Protection Alliance

- *"The hearing will provide a forum to discuss legislation that has been proposed to deal with problems neither the Founders – or even Congress in the mid-1980s – could have fathomed: What happens when law enforcement seeks to look at electronic communications stored on servers outside the U.S.? Do the same rules apply as if the email had been written on paper, which the Founders could have imagined? Also, who owns the emails – the person who wrote them or the company on whose servers they exist?"*
  – Brian McNicoll, conservative columnist and former director of communications for the House Committee on Oversight and Government Reform

- *"I have long argued that strong, backdoor-free encryption is an important cybersecurity technology that the government should be embracing, not seeking to regulate or outlaw."*
  – Sen. Ron Wyden

- *"Even if you design backdoors with the goal of only allowing access by law enforcement, as a practical matter there's no way to ensure that the bad actors don't gain access."*
  – Neema Singh Guliani, legislative counsel, American Civil Liberties Union

- *"The question addressed here is when the government should be able to gain access to this wealth of personal information for law enforcement and national security purposes. In the United States, answering that question requires consulting a welter of statutes and a few Supreme Court decisions… To date, that jurisprudence has had little to say about Cloud searches. Until the Supreme Court weighs in, policymakers are working pretty much on a clean slate in this area."*
  – Christopher Slobogin, director of the criminal justice program, Vanderbilt University

- *"Sometime in May the Senate Judiciary Subcommittee on Crime and Terrorism will be holding a hearing on this issue in response to what is believed to be a request by the U.S. Department of Justice to change existing law to make it easier for the federal government to seize data stored on servers located overseas. If that were to happen, it would lead directly to data localization and the destruction of cloud computing, at least as it exists today. No one would be safe from the prying eyes of federal investigators as long as they could find a server located outside the United States where a document they wanted was stored or through which an email they wanted to read had passed."*
  – Peter Roff, syndicated columnist, Cagles Syndicate

SOCIAL HIGHLIGHTS

- **@OpenRightsGroup:** You—not @ukhomeoffice—should decide the security you need. Tell them to stop subverting security and encryption!
- **@OrinKerr:** Here's the OSG's recent extension motion in MSFT/Ireland, via @palmore_joe.
- **@usatodaytech:** The global ransomware attack is why we can't have security backdoors, privacy advocates say (EPA photo)
- **@ForeignPolicy:** The NSA's failure to report mistakes poses serious concerns for the Fourth Amendment.
- **@InformationAge:** The government is 'watching' your #onlineactivity #snooperscharter #nomoreprivacy
- **@IBTimes:** Data privacy is in danger as the senate is discussing a bill on overseas' server access

- **@mattburgess1:** Lib Dem's manifesto tech, science etc. Includes stopping surveillance laws and a Digital Bill of Rights
- **@zackwhittaker:** New on @ZDNet: As part of a wider encryption push, Senate staff can now use Signal for secure messaging.