VFI Executive Briefing
A weekly roundup of technology news
February 20 – 24, 2017

TABLE OF CONTENTS

HILL UPDATE

Law360 **Senator Questions Border Electronics Searches**
Law360 reported on Senator Ron Wyden's intentions to draft a bill requiring border agents obtain search warrants for electronic devices.

The Hill **House panel to hold hearing on foreign surveillance law**
The Hill reported that on March 1, the House Judiciary Committee intends to hold a hearing to discuss reform and renewal of Section 702 of FISA. The hearing will start with a classified panel featuring officials from the Justice Department, FBI, NSA, and the Office of the Director of National Intelligence, followed by an open hearing. Relatedly, FOX News published an opinion piece by Judge Andrew Napolitano criticizing the far-reaching surveillance powers authorized under FISA.

ARTICLE SUMMARY

Law360 **Google Warrant Case Vs. Microsoft Warrant Case**
As technology companies expand globally, they increasingly are storing customer electronic data on servers outside the United States. To keep apace, the U.S. Department of Justice has become more creative in adapting existing legal instruments and more persistent in advancing arguments to encourage and in some cases, to compel, companies to turn over customer data stored abroad. While courts, most notably the U.S. Court of Appeals in the Second Circuit in last year's Microsoft decision,[1] have limited government efforts to compel the retrieval and production of electronic information stored overseas, a Pennsylvania federal court has departed from Microsoft and ordered Google to disclose internationally stored customer materials.

Associated Press **Pressure Mounts For FBI To Disclose How Much It Paid To Unlock iPhone**
The Associated Press reported that a group of news organizations filed a request with the U.S. District Court in Washington, D.C. to force the U.S. government to reveal the cost of the technology used by the FBI to unlock the San Bernardino iPhone.

The Hill **It's time to reform the feds' ability to surveil Internet users**
When the Department of Justice raises "national security" as a defense in a case, should that defense trump any other argument in the case? Should the national security argument trump constitutional protections? Microsoft and Twitter sued the government regarding its secrecy practices, and both companies recently enjoyed successes in court. The Federal Bureau of Investigation served search warrants on Microsoft and National Security Letters on Twitter. The search warrants and NSLs have one thing in common: the FBI demanded the technology companies keep completely quiet about them. In

the case of Microsoft, the search warrants included court orders compelling secrecy. In the case of Twitter, federal NSL law mandates secrecy.

Associated Press **Amazon resists request for Echo info in Arkansas slaying case**
The Associated Press reported that Amazon filed a motion to quash a search warrant for Alexa recordings connected to a Bentonville murder case. In its motion, Amazon argues that the First Amendment protects Alexa's audio recordings and responses, and accordingly, "the warrant should be quashed unless the Court finds that the State has met its heightened burden for compelled production of such materials."

The News Tribune **Getting prepared for a 'cyber-Pearl Harbor'**
But the federal government can – and should – be a better partner for Tacoma and other local communities. That's why I'm working on a bipartisan bill that would establish a cybersecurity grant program within the Department of Homeland Security. It would provide states with funds to develop cyber-resiliency plans so they can outline key issues and target how to fix them. Cyber resiliency requires exceptional coordination and planning across all levels of government. [...] U.S. Rep. Derek Kilmer, D-Gig Harbor, represents Washington's 6th Congressional District.

ZDNet **Cyberattacks threaten democracy itself, warns NATO**
The hacking campaign around the US presidential election, cyberattacks against Ukraine's power grid, and even the internet crippling Mirai botnet DDoS attack all demonstrate how cyberattacks have grown to threaten the very fabric of society itself, NATO has warned. Citing the impact of high profile incidents like these, Jamie Shea, deputy assistant secretary general for emerging security challenges at NATO, suggests that hackers aren't just a threat to individuals and organisations, but to the fundamental nature of democracy as a whole. "Cyber is facilitating more advanced and more effective psychological warfare, information operations, coercion and intimidation attacks. We used to worry about [hackers targeting] banks or credit cards or inconvenience to customers, now we worry about the future of democracy, the stability and health of our institutions," he said, speaking at the European Information Security Summit in London.

Fortune **Apple Says EU Breached its Rights in Tax Case**
Apple has accused the European Commission of unfair treatment in a high-profile $13.7 billion tax case. The tech giant accused the European Union's competition watchdog of breaching its "right to good administration," according to the Financial Times, which obtained a copy of Apple's complaint on Monday. The iPhone maker added that the European Commission, or EC, did not conduct "a diligent and impartial investigation" and that it had violated its "fundamental rights."

The Hill **FCC approves devices using next wave of wireless technology**
The Federal Communications Commission is approving the first devices that use a technology intended to ease data congestion on broadband networks. The agency's Office of Engineering and Technology on Wednesday allowed the sale of Ericsson and Nokia devices that will use LTE-U. LTE-U is a type of the fourth-generation (4G) mobile communications standard but moves broadband traffic to unlicensed airwaves on the faster 5GHz spectrum. That spectrum was previously reserved for WiFi and Bluetooth, both of which will now share the 5GHz band with mobile broadband data.

VFI Executive Briefing
A weekly roundup of technology news
February 20 – 24, 2017

CNBC **Microsoft's Asia head sees 'huge' opportunity in China, the future in cloud computing**
Companies hoping to adopt new technologies for long-term growth should embrace cloud computing, according to a top Microsoft executive. Ralph Haupter, president of Asia at Microsoft, told CNBC on Monday that decision-makers in the region were looking for ways to digitally transform their businesses to tap into new technologies like artificial intelligence, the Internet of Things, mixed reality and wearable devices. "Cloud is the how in 'how to do it,'" Haupter said. In a study released by Microsoft on Monday, 78 percent of Asia Pacific decision-makers surveyed said cloud computing was crucial in their digital transformation strategy.

New York Times **How Tech Policies May Evolve Under Republicans and Trump**
WASHINGTON — With Republicans now in power across the government, Congress has moved aggressively toward undoing Obama-era tech policies. Net neutrality, the rule that ensures equal access to all websites, and broadband privacy rules are the first targets. Lawmakers also hope to play a bigger role than in the last administration on policies of particular concern to Silicon Valley and internet users, including driverless cars and the scaling back of Federal Communications Commission powers concerning broadband providers. We talked to Senator John Thune, Republican of South Dakota, who leads the commerce committee that oversees the technology and telecommunications industries, about these efforts. The interview was edited for clarity and length.

Ars Technica **Judge: No, feds can't nab all Apple devices and try everyone's fingerprints**
Ars Technica reported that a magistrate judge in Chicago rejected a government application for a warrant that would allow law enforcement to force multiple persons to attempt to unlock an iPhone with their fingerprints. Judge M. David Weisman's opinion, which quotes from a still-sealed government filing, implies that "forced fingerprinting" is part of a broader government strategy, possibly to combat the prevalence of encrypted devices. George Washington University law professor Orin Kerr analyzed the ruling for The Washington Post, expressing support for the judge's Fourth Amendment analysis while criticizing the judge's Fifth Amendment concerns.

Electronic Frontier Foundation **A Step Forward in Microsoft's Legal Battle for Transparency about Government Data Requests**
Last Friday, the Electronic Frontier Foundation published a blog by Andrew Crocker, staff attorney at EFF, analyzing Judge Robart's recent ruling in Microsoft's secrecy order case. Crocker criticized Robart's dismissal of Microsoft's Fourth Amendment arguments as unsatisfactory and urged Microsoft to consider seeking leave to appeal.

VFI Executive Briefing
A weekly roundup of technology news
February 20 – 24, 2017

Notable Quotes

"We don't just rely on companies to keep our data secure, we also need them to stand up to the government on our behalf. It's a point often missed by those who dismiss companies' growing commitments to privacy as empty marketing. If not Microsoft, Apple, Google, Facebook and all the others, then who?"

–Andrew Crocker, staff attorney, EFF

"[The Investigatory Powers Act] forces internet companies to keep bulk records of all the websites you visit for up to a year and allows the UK government to coerce tech companies to hand over your web history with a retention notice and remove encryption, upon request. If you think all of this sounds rather alarming, it's because it is."

– Gianluca Mezzofiore, reporter, Mashable

"*Unfortunately, technology has outpaced ECPA's provisions governing how law enforcement obtains electronic communications. As a result, many in Congress share my concern that this out-of-date law provides insufficient protections for Americans' privacy."*

– Rep. Bob Goodlatte, chairman of the House Judiciary Committee

"The Email Privacy Act is a carefully structured bill to improve email privacy protections. Attaching unnecessary amendments like the so-called 'ECTR fix' would be a mistake – and undermine the good-faith negotiations completed by the House and further sour already-strained relations with the tech industry."

– Nathan Leamer, policy manager, R Street Institute

"There are well-established legal rules governing how law enforcement agencies may obtain data from social media companies and email providers. The process typically requires that the government obtain a search warrant or other court order, and then ask the service provider to turn over the user's data. If the request is overbroad, the company may seek to have the order narrowed. By requesting a traveler's credentials and then directly accessing their data, CBP would be short-circuiting the vital checks and balances that exist in our current system."

– Sen. Ron Wyden

"This Court agrees that the context in which fingerprints are taken, and not the fingerprints themselves, can raise concerns under the Fourth Amendment. In the instant case, the government is seeking the authority to seize any individual at the subject premises and force the application of their fingerprints as directed by government agents. Based on the facts presented in the application, the Court does not believe such Fourth Amendment intrusions are justified based on the facts articulated."

– Judge M. David Weisman

VFI Executive Briefing
A weekly roundup of technology news
February 20 – 24, 2017

"Through secret courts whose judges cannot keep records of their own decisions and secret permissions by select committees of Congress whose members cannot tell their constituents or other members of Congress what they have learned in secret, FISA has morphed so as to authorize spying down a slippery slope of targets, from foreign agents to all foreigners to anyone who communicates with foreigners to anyone capable of communicating with them."

– Judge Andrew P. Napolitano

"With Section 702 set to expire at the end of the year, the House Judiciary Committee will work in a bipartisan fashion to reauthorize and reform this intelligence gathering program to ensure that it continues to be a critical tool to thwart terrorist attacks and that it best protects Americans' civil liberties."

– Rep. Bob Goodlatte, chair of the House Judiciary Committee

Social Highlights

- **@Big_cases:** New filing in In re Google Search Warrant: Response
- **@EFF:** A ruling in Microsoft's fight against gag orders covering government requests for user data
- **@techreveiw:** Congress can't seem to fix a 30-year-old law governing your electronic data.
- **@ACLU:** A key law giving the NSA broad spying powers is up for renewal this year. Here's how to fix it.
- **@EdFelten:** "Nuts and Bolts of Encryption: A Primer for Policymakers". Just published; as short and simple as I could make it.
- **@Nathan_Leamer:** .@RepKevinYoder and @jaredpolis led way on Email Privacy Act, now it's the Senate's turn
- **@reason:** Sen. Wyden Calls for Warrants for Tech Searches on the Border
- **@arstechnica:** "This court agrees that the context in which fingerprints are taken... can raise concerns under the 4th Amendment."
- **@BBCTech:** Amazon resists Echo murder evidence call
- **@elizbeth_joh:** In fighting warrant for Alexa info in murder case, Amazon argues it has free speech rights in Alexa:
- **@fxnopinion:** The chickens have come home to roost | via @Judgenap