VFI Executive Briefing
A weekly roundup of technology news
August 15-19, 2016

TABLE OF CONTENTS

Hill Update – 1
Special Coverage – 1
Article Summary – 1
Notable Quotes – 4
Social Media Highlights – 5

HILL UPDATE

Nothing new this week.

SPECIAL COVERAGE

Nothing new this week.

ARTICLE SUMMARY

Wall Street Journal **U.S. Companies Slow to Adopt European Data Transfer Agreement**

U.S. companies have been slow to sign on to a new international data-transfer agreement with the European Union for reasons that include uncertainty that the terms will survive legal tests in the EU, experts said. The agreement, called Privacy Shield, allows businesses to transfer personal data on European citizens to the U.S. About 40 companies have been certified under the new rules since Aug. 1, when the U.S. Department of Commerce began accepting applications, the agency said on Friday.

Christian Science Monitor **Opinion: NSA hack reveals flaws in White House zero-day process**

Now, the dump is raising serious questions about the nature of the US government's cyberweapons arsenal. Chief among those questions is whether or not the US government should withhold information about potentially damaging flaws in software programs widely used by American companies. One of the most potentially damaging exploits that the Shadow Brokers revealed is a so-called "zero-day" vulnerability in a Cisco security product common in many American critical infrastructure facilities. Zero-days are security flaws that the affected company doesn't know about. Is that the kind of flaw that the NSA should keep secret from American businesses? Should it have told Cisco?

Wall Street Journal **EU Looks to Level Regulatory Playing Field With Apps, Telecoms**

BRUSSELS—The European Union's executive body is set to propose more rules for so-called over-the-top telecommunications services such as Microsoft Corp.'s Skype or Facebook Inc.'s WhatsApp, in a bid to level the regulatory playing field with the bloc's big telecom operators. The European Commission plans to require internet communications companies to meet stricter privacy and security protections and make

it easy for consumers to move their information when switching to other services, according to an internal document obtained by The Wall Street Journal.

Recode **Russia fines Google less than what the company makes in an hour**

Antitrust authorities in Russia hit Google this morning with a fine of around $6.8 million — what the company brought in, roughly, in the time it took me to make my coffee and write this post. Google reported $21.3 billion in gross revenue last quarter. Still, Russia's gesture is more damning to Google than the fine. It's another dent from an onslaught of regulatory probes into the web giant for anticompetitive behavior. Russia's case, like one (of three) in Europe, hinges on Google's practice of installing its Play store apps and services on Android devices.

Huffington Post **5 Cyber-Security Myths We Need To Ditch**

1. Software Will Protect You
2. Cyber-Crime Is Mostly About Credit Card Fraud
3. Cyber-Crime Is Only About Making a Buck
4. Cyber-Criminals Don't Target Small Businesses
5. There Is No Way to Stop a Cyber-Attack

Washington Post **The privacy debate is personal to Tim Cook**

Apple CEO Tim Cook has said he developed his "moral sense" growing up in rural Alabama in the '60s and '70s – a period of incredible social upheaval. Today, at Apple headquarters in Cupertino, Calif., Cook keeps in his office photos of two men who pushed the South to change: Robert F. Kennedy and Martin L. King Jr. In recent years, Cook appears to have been inspired by Kennedy and King as he pushed for the South to change again, this time on the issue of gay rights.

Wired **The Baltimore PD's Race Bias Extends to High-Tech Spying, Too**

THIS SPRING, AN appeals court ruled that Baltimore police systemically misused "stingray," a powerful surveillance device that spoofs cell sites to track cellphones. Last week, the Department of Justice issued a damning report detailing Baltimore PD's history of racial discrimination. As it turns out, those two issues aren't just related; they're intertwined. That's what a new FCC complaint, filed by the Center for Media Justice, ColorOfChange.org, and New America's Open Technology Institute, alleges. The report goes further than just detailing Baltimore's stingray indiscretions; it agues that the city's use of cell site simulators disproportionately impacts minority communities, with serious repercussions.

Wall Street Journal **Group Claims to Have U.S. Government Hacking Tools for Sale**

A previously unknown hacking group claims to have broken into a cyberespionage organization linked to the National Security Agency and is offering to sell what it says are U.S. government hacking tools. The group, calling itself the "Shadow Brokers," said in an internet post on Saturday that it had access to a "full

state sponsor tool set" of cyberweapons. To back up its claims, the group posted what appears to be attack code that targets security software on routers that direct computer traffic around the internet.

The Hill **DHS offers states cybersecurity help for voting machines**

Homeland Security Secretary Jeh Johnson is offering state election officials his department's help to shore up the cybersecurity of voting machines. On a conference callMonday, Johnson said the Department of Homeland Security National Cybersecurity and Communications Integration Center will help states audit machines, provide actionable intelligence and assist in other general ways.

Bloomberg **When a Tech Patent Is Neither**

Two years ago, when the U.S. Supreme Court invalidated Alice Corp.'s handful of patents on the concept of an electronic escrow arrangement, it ruled that taking abstract ideas—apparently including established methods of doing business like escrow—and implementing them on a computer doesn't meet the standard of intellectual property. In its unanimous decision, written by Justice Clarence Thomas, the high court refused to precisely define what makes something an "abstract idea." "We tread carefully," Thomas wrote of the new standard for patents. Since then, however, lower courts, and the U.S. Patent and Trademark Office, have been using some pretty heavy boots.

New York Times **Tech Giants Gobble Start-Ups in an Antitrust Blind Spot**

Walmart's $3.3 billion acquisition of Jet.com can be expected to sail through antitrust review, eliciting barely a peep of objection from the federal government. Like Facebook's acquisition of WhatsApp, the Walmart deal will probably end up being another example of an upstart internet company being swallowed up to preserve the stranglehold of a giant. This happens because antitrust regulators are stuck in an outdated view of the world, while the internet giants are more attuned to their nascent competitive threats. The deal for Jet.com is just the latest defensive internet acquisition of an emerging start-up that will preserve the hegemony of a select few.

Washington Post **We asked experts to compare Trump's and Clinton's cybersecurity policies. Here's what they said.**

Cybersecurity is now a top national security problem — some officials even call it a bigger threat than terrorism. But both major presidential candidates have hit hurdles on the campaign trail that raised questions about how they would try to keep U.S. computers safe if elected. Just last month, Democratic nominee Hillary Clinton escaped criminal prosecution for using a private email server for work as secretary of state — but got a tongue-lashing from the director of the FBI for being "extremely careless" by using it. Then emails from the Democratic National Committee were released by WikiLeaks, exposing politically embarrassing information.

Forbes **American Economic Activity Is Rooted In Global Flow Of Information**

Forbes published a contributed article by Jim Pflaging, principal and technology sector lead at The Chertoff Group, analyzing the Second Circuit Court ruling in Microsoft's warrant case and underscoring

the importance of an open Internet to the American economy. Pflaging highlights that although the Second Circuit ruled in Microsoft's favor, the government's argument in the case remains a threat given the possibility of a Supreme Court appeal or new legislation could enable the DOJ to obtain the emails in question.

Notable Quotes

- *"Honestly? I was shocked that they [FBI] would even ask for this. That was the thing that was so disappointing that I think everybody lost in the whole thing. There are 200-plus other countries in the world. Zero of them had ever asked this."*

  – Tim Cook, CEO, Apple

- *"Facebook, Google, Microsoft, Twitter and Yahoo unanimously expressed their opposition in a written statement to the British Parliament. Their primary concern is the legal conflicts [the Investigatory Powers Bill] would create when tech companies seeking to comply with the law take measures that have extraterritorial effect. For example, it is not inconceivable that UK authorities could ask a company like Microsoft to hand over customer data held in another country whose laws forbid such disclosure. Apple also expressed concern over the bill's "technical capability notices" and their consequences on encryption, noting that "companies should remain free to implement strong encryption to protect customers."*

  – James Pooler, intern, Council on Foreign Relations Digital and Cyberspace Policy program

- *"True, 'we have never had absolute privacy' guaranteed by law in this country. But it's also true that the government has never had an absolute guarantee that it could find everything it looked for—sometimes all it can do is penalize noncompliant people."*

  – J.D. Tuccille, former managing editor, Reason

- *"A successful appeal to the Supreme Court, or the adoption of legislation codifying this argument, would accelerate a breakdown of trust between nations and increase the risk of internet "balkanization."*

  – Jim Pflaging, Principal and Technology Sector Lead, The Chertoff Group

- *" When the top hacking outfit on the planet is itself hacked, we should be concerned that keeping backdoors secure isn't going to work."*

  – Kevin Bankston, Director, New America Foundation's Open Technology Institute

VFI Executive Briefing
A weekly roundup of technology news
August 15-19, 2016

Social Highlights

- **@matthew_d_green:** Is Apple's Cloud Key Vault a crypto backdoor?
- **@rhhackett:** very very provocative argument from @pwnallthethings on how apple just opened a can of worms
- **@simonlporter:** U.S. Companies Slow to Adopt European Data Transfer Agreement
- **@washingtonpost:** Tim Cook discussed his first five years in one of Corporate America's most glaring spotlights
- **@WIREDUK:** A Microsoft golden key blunder means you can install any OS on Windows hardware at the moment
- **@JD_Tuccille:** FBI investigations reveal that encryption is increasingly important, and officials can't be trusted with a backdoor.
- **@PaulNemitz:** Tim Cook: #Privacy Is Worth Protecting - InformationWeek via @tame_it
- **@ChertoffGroup:** Principal & Tech Sector Head Jim Pflaging in @Forbes "Technological innovation relies upon the global network"
- **@adctweets:** Cross-Border Law Enforcement Demands: Analysis of the US Department of Justice's Proposed Bill