VFI Executive Briefing
A weekly roundup of technology news
August 22-26, 2016

TABLE OF CONTENTS

HILL UPDATE

Nothing new this week.

SPECIAL COVERAGE

Nothing new this week.

ARTICLE SUMMARY

Washington Post **The latest NSA leak shows why it's so hard to trust even tech designed to keep computers safe**

Leaked National Security Agency hacking tools are exposing how even the technology designed to safeguard our computer networks can put users at risk — and how poor security practices like clinging to old equipment can make things worse. The trove, which mysteriously appeared online last weekend, is full of hacking tools that can break through systems that businesses and even government agencies use to secure their digital infrastructure. In some cases, the tools can be used to attack equipment that is still being used, but so outdated that the companies that made them don't plan to release fixes.

The Hill **Voting machines should be seen as critical democracy infrastructure**

At the Open Source Election Technology Foundation (OSET), a 10-year old Silicon Valley based nonprofit election technology research institute, we are encouraged by valuable dialog underway about how to protect America's aging and vulnerable voting machinery and evolve our systems with technology for ease and confidence. Setting aside some misunderstanding about the challenges elections officials face in administering a nationwide patchwork quilt of election technology, there is a critical mass on the left and the right discussing how to protect our "critical democracy infrastructure."

The Hill **Trump gets little backing from Silicon Valley**

Election Day can sometimes feel like more of a headache than a patriotic celebration. Long lines and scheduling conflicts may leave voters wondering why there isn't an easier way to cast their ballots. Some say there already is: online voting. Why head to the polls if you can vote from anywhere using your laptop

or smartphone? But even as online voting is on the rise in the United States and elsewhere, experts warn its convenience isn't worth its costs.

CIO Dive **Continuing cybersecurity education critical as hackers hone their skills**

"While there are many industries that provide, and in fact mandate continuing education–namely the legal and financial sectors–such programs are severely lacking within the cyber-security field," Rohit Khanna, senior vice president of Customer Success at SecureAuth, told CIO Insight. "With the rapid evolution of attack tactics, the cyber-security industry must hold itself to a higher standard." Last month, an Intel Security and the Center for Strategic and International Studies report revealed that the talent shortage in cybersecurity is worse than talent deficits in other IT occupations.

Watchdog.org **A decade of court decisions has shaken the basis of patent law**

Earlier this summer, the U.S. Supreme Court made it easier for patent holders to seek larger damage awards when their patents are infringed. For patent watchers, however, the high court's ruling was only just the latest in a particularly active decade of major patent litigation. Beginning in 2006, the Supreme Court ruled that holders who license their patents cannot win an injunction to stop third parties from infringing on their patent. That lawsuit, eBay v. MercExchange, L.L.C., changed the way patent lawsuits could be waged, altering incentives along the way.

Wall Street Journal **White House Official Cozied Up to Google Before Antitrust Lawsuit Was Shelved**

When the Federal Trade Commission neared a momentous decision on whether to charge Google with violating antitrust laws in January 2013, the White House was watching closely. New emails uncovered by the Campaign for Accountability, a public interest watchdog organization, show that a White House advisor met with top Google lobbyist Johanna Shelton and top Google antitrust counsel Matthew Bye twice in the weeks before the FTC announcement.

Washington Post **Why Clinton can't shake her private email scandal**

Hillary Clinton has been tired of talking about her private email server for a long time. When a reporter asked the Democratic presidential candidate about the story's staying power as she walked away from a terse news conference in August 2015, the politician threw up her hands in exasperation. "Nobody talks to me about it other than you guys," she hollered back. But a year later — and with just over three months until the election — Clinton is still being plagued by her decision to use a personal email account for work during her tenure as secretary of state.

The Hill **Dem senator criticizes Facebook, Instagram for gun sales**

Sen. Ed Markey (D-Mass.) criticized Facebook and its subsidiary, Instagram, on Monday, saying it's too easy to purchase and sell firearms on the platforms. Facebook policies banned the sale of firearms on the website in January, but a statement from Markey's office says that according to media reports, "users are still able to pursue those sales through the social media platforms."

VFI Executive Briefing
A weekly roundup of technology news
August 22-26, 2016

New York Times **Apple Becomes a Green Energy Supplier, With Itself as Customer**

The words are stenciled on the front of the Apple Store, a glass box sandwiched between a nondescript Thai restaurant and a CVS pharmacy in downtown Palo Alto: “This store runs on 100 percent renewable energy.” If Apple’s plans play out, it will be able to make that claim not only for its operations throughout California but also beyond, as the company aims to meet its growing needs for electricity with green sources like solar, wind and hydroelectric power.

Christian Science Monitor **Can hackers sway public opinion with DNC and NSA leaks?**

"This is just an effort to confuse the issue," says James Lewis, a senior fellow at the Center for Strategic and International Studies, a Washington think tank. "If they think the US is going to come out and blame [Russia’s federal security service] for the DNC hack, they’re going to want to deflect attention and remind people they should be mad at the NSA." [...] If Moscow is trying to make that case, they have more tools to do it than ever before. Russia Today (RT), a television network funded by the Kremlin, boasts a large global audience and has developed a reputation for criticism of the West. In January, the BBC won a court case against RT after the Moscow-based network claimed it had faked a report in Syria. Russia’s latest military doctrine, released in 2014, describes the use of information warfare to cause political upheaval.

Slate **In Praise of the Private Email Server**

Slate published a contributed article by Nat Meysenburg, technologist at New America’s Open Technology Institute, arguing that enterprise and cloud service providers offer insufficient protection of private emails. Meysenburg contends that individuals should set up personal email servers, citing uncertainties around legal protection of data in the cloud. In particular, he notes that the warrant precedent set in United States v. Warshak has not been codified by new statutes or affirmed by the Supreme Court, and therefore when you use a cloud provider the “ultimate level of privacy protection for your email is uncertain, especially outside of the 6th Circuit.”

Defense One **Swing States Reject Feds’ Offer to Cybersecure Voting Machines**

[Some] battleground states, including Georgia and Pennsylvania, say they will rely on in-house security crews to maintain the integrity of voter data. “The question remains whether the federal government will subvert the Constitution to achieve the goal of federalizing elections under the guise of security,” Georgia Secretary of State Brian Kemp told Nextgov in an email. “Designating voting systems or any other election system as critical infrastructure would be a vast federal overreach, the cost of which would not equally improve the security of elections in the United States.”

Washington Times **Congress urged to investigate security concerns raised by Apple flaws used by ‘digital arms dealers’**

Rep. Ted Lieu, who has a degree is computer science, urged his colleagues Thursday to hold a hearing on mobile phone security after Apple rushed to repair critical iPhone vulnerabilities reportedly being

leveraged by state-sponsored hackers. The California Democrat was among the first lawmakers to formally weigh in this week after Apple asked its users to install an iPhones update that patches previously undisclosed security flaws affecting iOS 9.

Notable Quotes

- *"Will people eventually become desensitised to government having access to information about every single aspect of their lives? How long until the content of our emails, texts and social media message are also collected in-bulk? While no one can dispute the importance of national security, it is essential that it is not used to justify ill-considered attempts to erode the legal right to privacy."*

  – Janine Regan, associate, Charles Russell Speechlys

- *"The US houses a majority of the largest and most well-known companies in cloud data storage and software-as-a-service, so the precedent set by this ruling provides a more secure platform for Europe's enterprise to do business with the major cloud vendors in the US. They can rest easy knowing that the US government does not have access to their most sensitive data and has no sovereignty over it simply because the company that owns the servers is based in America."*

  – Brian Stafford, CEO, Diligent Corporation

- *"When companies like Facebook compromise the integrity of such platforms, they are burying our community's stories and potentially participating in police cover ups that perpetuate this cycle of violence."*

  – Rashad Robinson, executive director, Color Of Change

- *"Most large email providers require a search warrant based on probable cause before handing over your emails, consistent with a key court ruling from 2010 in which the U.S. Court of Appeals for the 6th Circuit held that the Fourth Amendment protects the privacy of your email just like the correspondence you store in your own home. However, because the Supreme Court has never ruled on the issue, that one court's decision is only technically binding on police in Kentucky, Ohio, Michigan, and Tennessee. Plus, the Department of Justice has never conceded the point that the Fourth Amendment requires it to get a warrant before seizing your emails and has over the past five years been one of the key players on Capitol Hill against legislation that would codify this clear warrant-for-emails rule in statute.."*

  – Nat Meysenburg, technologist, New America's Open Technology Institute

VFI Executive Briefing
A weekly roundup of technology news
August 22-26, 2016

Social Highlights

- **@9to5mac:** ACLU reacts to NSA hack with the perfect tweet about Apple/FBI battle
- **@business:** U.K. terror review backs case in bill for bulk data collection
- **@oliverdarcy:** The NSA hack proves Apple was right to fight the FBI
- **@ArsTechnicaUK:** French minister: Apps like Telegram must be decrypted for legal probes by @Brusselsgeek
- **@astepanovich:** French minister wants EU law to undermine encryption >300 days since we asked Obama to lead
- **@dnvolz:** Trump's sagging poll numbers threaten Sen. Burr's re-election, which could impact future debates over encryption