VFI Executive Briefing
A weekly roundup of technology news
January 2 – 6, 2017

TABLE OF CONTENTS

Special Coverage – 1
Article Summary – 1
Notable Quotes – 5
Social Media Highlights – 7

SPECIAL COVERAGE – Russia Cyber Hacking

An unclassified report by the Intelligence community concerning Russian cyber hacking during the election is going to be released to the public soon. The articles below highlight the political debate that is happening on this issue.

- **CNN** US administration '100% certain' about Russian hacking
- **New York Times** Trump and Julian Assange, an Unlikely Pair, Unite to Sow Hacking Doubts
- **Wired** A Timeline of Trump's Strange, Contradictory Statements on Russian Hacking
- **Reuters** U.S. spy chief 'resolute' on Russia cyber attack, differs with Trump

ARTICLE SUMMARY

Wired A Few States Now Actually Help You Figure Out If You've Been Hacked

THOUSANDS OF US companies were hacked last year, and each time people's private data was taken. Was yours? You may not know because it's hard to keep track, much less do anything about it when there are so many incidents all the time. But if the data collected on breaches in the US were available to you, it would be a lot easier to check whether you've interacted with compromised businesses and institutions. That data exists. In fact, nearly every US state (47 to be exact) requires companies to disclose when a breach affects their citizens, and most track this data internally. That data is usually a public records request away from you, the consumer, who could actually use it to inform your digital habits.

The Hill Giuliani: Hacking 'biggest menace' to US

Former New York City Mayor Rudy Giuliani (R) on Thursday called hacking the "biggest menace" to the United States and the world. "It's the fastest growing form of a crime. One of the biggest fears we have is an attack on our grid," Giuliani said in an interview on Fox Business. "It's ubiquitous and we have fallen way behind. Our information systems and our gathering of information and all the wonderful things we can do, we're way ahead. And on defense, we're way behind." Giuliani was a prominent supporter of President-elect Donald Trump during the campaign.

VFI Executive Briefing
A weekly roundup of technology news
January 2 – 6, 2017

IT World **A potentially fatal blow against patent trolls**
For years, patent trolls have been the best evidence that pure evil exists. And like most evil entities, they are almost impossible to stop. Even a 2014 U.S. Supreme Court decision that was highly critical of patent trolls has done little to slow their slimy, reptilian-like existence. But a federal judge on Dec. 19 crafted a novel tactic to curb patent trolls when she slapped a half-million-dollar bill on the lawyers and said that they were personally responsible for paying it, not their client. This could truly be a game-changer. This unusual decision could make lawyers hesitate to take patent trolls as clients. Part of the patent-troll economic model is based on lawyers taking a contingency fee, meaning that they take a percentage of whatever money is extracted from victims rather than being paid an hourly fee.

The Hill **Our cybersecurity policies are failing us. It's time to fix them**
Today's criminals are fighting a 21st century war, attacking our critical infrastructure and financial systems using unconventional techniques, while we defend ourselves with antiquated methods. Pins, tokens, passwords, IP verification, device authentication, physical biometrics and even multi-factor authentication can all be bypassed. We know this because today's fraud comes from authenticated sessions that are taken over post-login. Instead of being a step ahead of the fraudsters, we are a step behind.

Wired **This Is the Year Donald Trump Kills Net Neutrality**
2015 WAS THE year the Federal Communications Commission grew a spine. And 2017 could be the year that spine gets ripped out. Over the past two years, the FCC has passed new regulations to protect net neutrality by banning so-called "slow lanes" on the internet, created new rules to protect internet subscriber privacy, and levied record fines against companies like AT&T and Comcast. But this more aggressive FCC has never sat well with Republican lawmakers. Soon, these lawmakers may not only repeal the FCC's recent decisions, but effectively neuter the agency as well. And even if the FCC does survive with its authority intact, experts warn, it could end up serving a darker purpose under President-elect Donald Trump.

The Hill **Five regulatory fights facing tech in 2017**
Tech's influence and reach is growing and pitting the industry against a new wave of regulatory challenges. In the U.S., mega-mergers are likely to face tough scrutiny in 2017, and the industry is bracing for another round in the fight over encryption. At home, President-elect Donald Trump is vowing to roll back many Obama administration regulations. But overseas, the European Union is pressing ahead with a number of high-profile cases against some of Silicon Valley's giants.

Wired **The Year Encryption Won**
BETWEEN THE REVELATIONS of mega-hacks of Yahoo and others, Russia's meddling in the US electoral system, and the recent spike in ransomware, it's easy to look at 2016 as a bleak year for security. It wasn't all so, though. In fact, the last 12 months have seen significant strides in

one of the most important aspects of personal security of all: encryption. End-to-end encryption, which ensures that the only people who can see your communications are you and the person on the receiving end, certainly isn't new.

Wired **The White House's Fix for Robots Stealing Jobs? Education**
A NEW REPORT from the White House warns that millions of jobs could be automated out of existence in coming years. But it cautions against one much discussed solution: giving away free money. The report, published this week by the President's Council of Economic Advisers, joins a growing body of work forecasting massive jobs losses due to automation and artificial intelligence. A paper published in 2013 by Oxford University researchers, for example, estimated that as many as 47 percent of all jobs could eventually be automated. The new report, likewise, forecasts millions of job losses in careers such as truck driving, as self-driving vehicles hit the roads, as well as low-skilled jobs.

The Verge **US government starts asking foreign travelers to disclose their social media accounts**
The US Customs and Border Protection has started demanding that foreign travelers hand over Facebook, Twitter, and other social media account information upon entering the country, according to a report from Politico. The new policy follows a proposal laid out back in June and applies only to those travelers who enter the US temporarily without a visa through the Electronic System for Travel Authorization, or ESTA, process. The goal, the government says, is to "identify potential threats," a spokesperson tells Politico. The new policy went into effect on Tuesday, and the request is currently "optional." It asks foreign travelers to "enter information associated with your online presence," and offers a drop-down menu allowing participants to enter in account names for most major social networks, including LinkedIn and even Google+.

The Washington Post **Obama moves to split cyberwarfare command from the NSA**
"While the dual-hat arrangement was once appropriate in order to enable a fledgling Cybercom to leverage NSA's advanced capabilities and expertise, Cybercom has since matured" to the point where it needs its own leader, Obama said in a statement accompanying his signing of the 2017 defense authorization bill. Cybercom's mission is, when ordered, to disrupt and destroy adversaries' networks. It is also to defend the nation against incoming threats to critical systems and to protect the military's computers from cyberattack.

Cyberscoop **2016: Cybersecurity becomes a political nightmare for D.C.**
Washington's attitude towards cybersecurity has drastically changed over the last 12 months. In 2016, Capitol Hill's understanding and framing of the issue evolved as major political organizations, businesses and prominent individuals were hurt by cybercrime. While the dust has yet to settle on a number of these events, we may all look back at 2016 as a watershed moment for how D.C. reacts to cybersecurity.

VFI Executive Briefing
A weekly roundup of technology news
January 2 – 6, 2017

Bank Info Security **2017 Cybersecurity Predictions: The Impact of Trump Election**
"What is most concerning to me right now is that much of U.S. critical infrastructure has been colonized by one nation-state or an adversary with backdoors and remote access terminals that would allow for them to re-enter these systems and conduct destructive attacks - like the manipulation of time or the manipulation of the integrity of data in critical systems that have a kinetic impact on society," says Kellermann, CEO of the venture capital firm Strategic Cyber Ventures.

Recode **Mark Zuckerberg's personal challenge this year is to travel all around the U.S. meeting new people**
Mark Zuckerberg is coming to a city near you. The Facebook CEO, who takes on a personal challenge for himself each January that he shares with the public, said Tuesdaythat his goal for 2017 was to "have visited and met people in every state in the U.S. by the end of the year." By Zuckerberg's estimation, that means he'll need to travel to 30 states in 2017. (He's already visited and met people in 20 of them apparently.) "After a tumultuous last year, my hope for this challenge is to get out and talk to more people about how they're living, working and thinking about the future," Zuckerberg wrote on his Facebook page. He added that he hopes to meet with teachers and scientists and visit small towns and universities throughout the year. He even plans road trips with his wife, Priscilla, for part of the challenge.

New York Times **Tech Giants Seem Invincible. That Worries Lawmakers.**
In the technology industry, the sharks have never long been safe from the minnows. Over much of the last 40 years, the biggest players in tech - from IBM to Hewlett-Packard to Cisco to Yahoo - were eventually outmaneuvered by start-ups that came out of nowhere. The dynamic is so dependable that it is often taken to be a kind of axiom. To grow large in this business is also to grow slow, blind and dumb, to become closed off from the very sources of innovation that turned you into a shark in the first place. Then, in the last half decade, something strange happened: The sharks began to get bigger and smarter.

The Verge **Mossberg: The Trump effect**
A couple of weeks ago, President-elect Donald Trump summoned the leaders of top tech companies to his New York skyscraper for a meeting. He showered them with praise. "There's nobody like you in the world," he said in the public portion of the session, adding, "we're going to be there for you." But, during his long campaign, he wasn't always so friendly or supportive of the tech industry, many of whose executives privately or publicly opposed him. He threatened specific tech companies; called for huge tariffs on China, where many tech products and components are made; strongly sided with the FBI on forcing the decryption of smartphones; and has appointed people to his transition team who have opposed net neutrality.

VFI Executive Briefing
A weekly roundup of technology news
January 2 – 6, 2017

The Verge **Mark Zuckerberg Is Sure Acting Like Someone Who Might Run for President**
MARK ZUCKERBERG HASN'T said he wants to be president. But if someone were to run for office, that someone might want to line up a few things to prepare for the possibility. A few things that Facebook's CEO has done. Uncanny, right? To be clear, setting the table doesn't mean Zuckerberg plans to sink his teeth into electoral politics. But he's made some moves in the past few days that have restarted the speculation. On Tuesday, in his annual (and annually publicized) New Year's resolution announcement, Zuckerberg vowed to travel to 30 US states to ensure he will have visited and met people from all fifty by the end of 2017. Campaigning much?

The Chicago Tribune **What's Next: Encryption, AI, fake meat and more trends ready to pop in 2017**
The Chicago Tribune published an article predicting top tech and innovation trends for 2017. The article forecasts that encryption will be a key issue of discussion this year, stating that the debate over government access to encryption will most likely gain traction during the Trump administration.

The Washington Post **Can Alexa help solve a murder? Police think so - but Amazon won't give up her data**.
The Washington Post, reported on a murder investigation in which Amazon was served a search warrant for data connected to the suspect's Amazon Echo. Amazon provided account holder information linked to the suspect but refused to provide information stored on its servers. Coverage highlighted that the case raises new privacy questions regarding electronic devices and digital assistants that are constantly listening for user commands.

The Seattle Times **Amazon Echo search warrant could spur new prosecution methods, experts says**
The Seattle Times published an interview with University of Washington law professor Ryan Calo regarding how the Amazon search warrant could spur law enforcement to utilize digital assistants to investigate crimes in unique and controversial ways.

Notable Quotes

"The Arkansas police have gotten some grief at seizing the Alexa under the idea that it's a violation of privacy. But there's no right to privacy. Amazon's not your lawyer, not your doctor, not your spouse, not your priest, so the usual protections for highly confidential information are not there. This is information you shared with a commercial vendor in exchange for certain conveniences."

- Craig Ball, law professor, University of Texas

VFI Executive Briefing
A weekly roundup of technology news
January 2 – 6, 2017

"The EWG (Encryption Working Group) report is a great place for Congress, and states, to start. It signals Congress understands how free and open encryption practices led to innovation the current, robust online-marketplace. It also signals that Congress is unwilling to disturb encryption's status quo."
- Jonathon Hauenschild, technology policy analyst, American Legislative Exchange Council

"Because the federal government relies heavily on partnerships and information sharing with state and local law enforcement agencies, passage of HB171 could potentially hinder warrantless surveillance in the state. For instance, if the feds wanted to engage in mass surveillance on specific groups or political organizations in New Hampshire, it would have to proceed without state or local assistance. That would likely prove problematic."
- Tenth Amendment Center

"I don't think there's any real dispute that for a proper criminal investigation or even for a national security matter, where there's legal authority and a judicial determination, that searches are appropriate. But if we've learned anything in the last few years, it's that these techniques can be used for the public at large. And there is a real risk right now, with the growing use of these consumer devices connected to the internet-it's not just Alexa, it's thermostats, it's, you know, connected toys-that the government will take advantage of all this personal data that's being collected for the type of mass surveillance that I don't think we could permit. So the attorney general really needs to be asked about this issue. And we need to get-I should say, in fact, the nominee to be attorney general should be asked about this issue, and we should get his views.
- Marc Rotenberg, executive director, Electronic Privacy Information Center

"It's up to the courts to protect the public against fishing expeditions by investigators seeking to examine every piece of information a smart device collects from the moment it enters a home. The courts need to make sure searches are relevant, with a clear and limited definition of what that means."
- Los Angeles Times Editorial Board

"The police request may be overbroad, in which case Amazon is fully justified in refusing to comply until it is narrowed. But Amazon is also reportedly standing on principle, claiming that the privacy rights of Echo users would justify its refusal to comply even with an appropriately tailored warrant. The difference in the principles at stake explains why Apple was right in refusing to help the FBI save lives from a potential, imminent terrorist attack, while Amazon's

refusal to help clear an isolated crime whose victim is already dead is a mistake."
- Bruce Abramson, London Center for Policy Research senior fellow

"It's not just one device, it's putting together a whole bunch of different devices to make a case that is, some would argue possibly circumstantial, some would argue is incredibly compelling. And so the question is going to be, how much data is going to be enough to make a foolproof case?...We live in the world where we really haven't settled the law or the standard of care for companies that provide in-home devices like that. The standards of care - as companies have more and more really specific information about what goes on inside the home - has got to be higher and higher."
- Nuala O'Connor, president and CEO, Center for Democracy & Technology

"As with cloud storage and webmail, the data [on Amazon Echo] lives largely on remote servers controlled by companies. In this case, Amazon provided only basic customer data, but anything held in the cloud will be susceptible to a warrant request. As a result, any request you have with Siri or Alexa will generally be treated like emails, Dropbox files or Google searches - hard for criminals to access, but available to any law enforcement officers with reasonable suspicions and an agreeable judge. That might not be the ideal result for privacy-minded Echo owners, but it's the best they're likely to get."
- Russell Brandom, reporter, The Verge

"Many innovations produced by the IoT will introduce incredible conveniences for people. People must be aware that law enforcement officials may try to obtain evidence from cloud platforms. For the most part, existing laws should protect people, as should courts. In the gray areas, federal and state legislators can easily clarify laws and protect the privacy interests of their citizens."
- Jonathan Hauenschild, technology policy analyst, American Legislative Exchange Council

Social Highlights

- **@cdt:** MUST READ: @joejerome breaks down #AmazonEcho, Arkansas murder case & #privacy implications:
- **@dvolz:** Sessions was also opponent of Email Privacy Act. Passed House unanimously and required authorities get a warrant before searching old emails
- **@elizabeth_joh:** This is a case to watch: prosecution trying to get Amazon Echo data in murder case.
- **@gonzalezseattle:** Amazon Echo search warrant could spur new prosecution methods, expert says via @seattletimes

VFI Executive Briefing
A weekly roundup of technology news
January 2 – 6, 2017

- **@GreggHoush:** "Any measure that weakens encryption works against the national interest" a bipartisan U.S. Congressional committee
- **@pressfreedom:** Transition to Trump: Why U.S. needs to be global leader in protecting strong encryption
- **@russellbrandom:** How much can police find out from a murderer's Echo? (Not much from the device, but your phone is a goldmine.)