

VFI Executive Briefing

A weekly roundup of technology news

March 20 – March 24, 2017

TABLE OF CONTENTS

| |
|-----------------------|
| Hill Update – 1 |
| Article Summary – 2 |
| Notable Quotes – 4 |
| Social Highlights – 5 |

HILL UPDATE

Recode [The Senate could take the first step tonight to kill the FCC's privacy rules](#)

Congress could take its first step as soon as Wednesday toward gutting the tough privacy rules imposed on Internet providers like AT&T, Comcast and Verizon last year during the Obama administration. In October, the Federal Communications Commission — then under former Democratic Chairman Tom Wheeler — began mandating that ISPs obtain consumers' permission before turning over their private data to third parties, like advertisers. Internet providers obviously loathed the rules, lambasting them as unfair and burdensome — and Republicans in Congress have heard their cries. To that end, the Senate could try to hammer the first nail in the coffin with a vote Wednesday evening on the measure, called a resolution of disapproval, that would overturn the FCC's privacy order, according to two sources familiar with the plan.

Washington Post [The Senate just voted to undo landmark rules covering your Internet privacy](#)

The Privacy Shield data transfer agreement between the U.S. and EU is likely to remain intact under the Trump administration, experts say, but American businesses can still take steps to ensure they're protected if the deal fails. European anxiety on the agreement, which enables roughly \$260 billion in trade of digital services, increased after U.S. President Donald Trump signed an executive order directing U.S. agencies to "exclude persons who are not United States citizens or lawful permanent residents from the protections of the Privacy Act regarding personally identifiable information." Extending the 1974 Privacy Act to include European citizens' data was a "long standing demand of the EU" ahead of the Privacy Shield agreement. Mr. Trump's executive order appeared to contradict EU citizens' Privacy Act protections, creating a sense of confusion in the private sector about the future of Privacy Shield.

The Hill [Lawmakers call on federal government to clearly define cyber war](#)

House lawmakers have introduced a bipartisan resolution calling on the federal government to develop and adopt a "comprehensive" cybersecurity policy that defines cyber war. The resolution, introduced by Reps. Dutch Ruppersberger (D-Md.) and Scott Taylor (R-Va.) on Thursday, asks for a policy "that clearly defines acts of aggression, acts of war, and other related events in cyberspace, including any commensurate responses to any such act or event in cyberspace." The resolution cites nine "mega-breaches" that affected the U.S. in 2015, including the one at the Office of Personnel Management (OPM) in which Chinese hackers had access to the personal information of more than 20 million Americans. After the OPM breach, former President Barack Obama and Chinese President Xi Jinping came to an agreement to tamper down the digital theft of intellectual property.

VFI Executive Briefing

A weekly roundup of technology news

March 20 – March 24, 2017

The Washington Post [House Intelligence Chair Says Trump Campaign Officials Were Ensnared In Surveillance Operations](#)

The Washington Post, reported on comments made by Representative Devin Nunes that intelligence on President Trump's campaign officials was collected legally and incidentally under FISA surveillance programs.

Networked World [US lawmakers question police use of facial recognition tech](#)

The FBI and police departments across the country can search a group of databases containing more than 400 million photographs, many of them from the drivers' licenses of people who have never committed a crime. The photos of more than half of U.S adults are contained in a series of FBI and state databases, according to one study released in October. Law enforcement agencies don't need a court-ordered warrant to search the database, members of the House of Representatives Oversight and Government Reform Committee noted during a hearing Wednesday.

ARTICLE SUMMARY

Lawfare [Gorsuch On Cyber-Related Issues: Part One](#)

Lawfare published a blog by University of South Carolina law student Sarah Tate Chambers highlighting Judge Neil Gorsuch's rulings on various issues of cybersecurity and data. Chambers notes that Judge Gorsuch's ruling in [United States v. Ackerman](#) leaves open the question of how third-party doctrine applies to email.

Wired [A Cybersecurity Arsenal That'll Help 'Protect Your Election'](#)

THE RISE OF cheap digital attacks like phishing and DDoS doesn't just endanger businesses. It also endangers democratic elections around the world, in which a well-timed data breach or site outage can meaningfully impact—and potentially destabilize—the democratic process. That's why Jigsaw and Google, both divisions of Alphabet, are launching a suite of cybersecurity tools today called "Protect Your Election." They hope to provide a set of free cyber-defenses that can support the independent news outlets, election monitoring and audit groups, activists, and human rights organizations that help elections run smoothly. The innovation here isn't the tools themselves, but packaging them in a way that makes them accessible to the people who need them most.

Courthouse News Service [National Security Letters Taken To Ninth Circuit](#)

Courthouse News Service reported that the Ninth Circuit Appeals Court heard [arguments](#) in [Under Seal v. Sessions](#), an EFF lawsuit on behalf of Credo Mobile Inc. and CloudFare challenging the constitutionality of perpetual gag orders connected to National Security Letters. The companies argued that the use of these gag orders are an unconstitutional prior restraint of speech. The Recorder article briefly referenced Microsoft's secrecy orders lawsuit as one of several attempts by technology companies to push back against gag orders.

VFI Executive Briefing

A weekly roundup of technology news

March 20 – March 24, 2017

Networked World [FBI director floats international framework on access to encrypted data](#)

Speaking on Thursday, Comey suggested that the U.S. might work with other countries on a “framework” for creating legal access to encrypted tech devices. “I could imagine a community of nations committed to the rule of law developing a set of norms, a framework, for when government access is appropriate,” he said on Thursday. Comey made his comments at the University of Texas at Austin, when trying to address a key concern facing U.S. tech firms in the encryption debate: the fear that providing government access to their products might dampen their business abroad.

Ars Technica [Feds: We’re pulling data from 100 phones seized during Trump inauguration](#)

In new filings, prosecutors told a court in Washington, DC that within the coming weeks, they expect to extract all data from the seized cellphones of more than 100 allegedly violent protesters arrested during the inauguration of President Donald Trump. Prosecutors also said that this search is validated by recently issued warrants. The court filing, which was first reported Wednesday by BuzzFeed News, states that approximately half of the protestors prosecuted with rioting or inciting a riot had their phones taken by authorities. Prosecutors hope to uncover any evidence relevant to the case. Under normal judicial procedures, the feds have vowed to share such data with defense attorneys and to delete all irrelevant data. “All of the Rioter Cell Phones were locked, which requires more time-sensitive efforts to try to obtain the data,” Jennifer Kerkhoff, an assistant United States attorney, wrote.

Foreign Policy [Trump’s Big Defense Buildup Should Include a National Cyber Academy](#)

We urgently need to build the next generation of cyberleaders to prepare both government and civil society to defend and deter in this venue. A useful model to consider is that of a national cyberservice academy, much like the dedicated national service academies at Annapolis, West Point, and Colorado Springs, which educate the human leaders to defend the nation at sea, on land, and in the air. The Pentagon should use its new windfall to establish a national cyber academy to defend America in cyberspace, in our critical infrastructure, and in the internet of things.

New York Times [In New York, Bringing Broadband to Everyone by 2018](#)

HALCOTT, N.Y. — It’s about 15 miles from here to a dairy testing facility in Roxbury, or about one hour and 20 minutes round trip if you know these dusty mountain back roads like Chris DiBenedetto, a dairy farmer. He has been going back and forth for years, ferrying a sample of fresh milk for a federally mandated drug test before he can start processing each batch. But what stressed him the most were the valuable daylight farming hours lost to the journey, while he was stuck in his car or waiting for the results. Now, Mr. DiBenedetto gives a sample to a driver heading that way to do the drop-off, letting the new fiber wiring hanging over his old route do the simple document delivery for him via email.

New York Times [A.I. Is Doing Legal Work. But It Won’t Replace Lawyers, Yet.](#)

Impressive advances in artificial intelligence technology tailored for legal work have led some lawyers to worry that their profession may be Silicon Valley’s next victim. But recent research and even the people working on the software meant to automate legal work say the adoption of A.I. in law firms will be a slow, task-by-task process. In other words, like it or not, a robot is not about to replace your lawyer. At least, not anytime soon. “There is this popular view that if you can automate one piece of the work, the rest of the job is toast,” said Frank Levy, a labor economist at the Massachusetts Institute of Technology. “That’s just not true, or only rarely the case.”

VFI Executive Briefing

A weekly roundup of technology news

March 20 – March 24, 2017

Electronic Frontier Foundation [Patents Are A Big Part Of Why We Can't Own Nice Things: the Supreme Court Should Fix That](#)

Today, the Supreme Court heard arguments in a case that could allow companies to keep a dead hand of control over their products, even after you buy them. The case, *Impression Products v. Lexmark International*, is on appeal from the Court of Appeals for the Federal Circuit, who last year affirmed its own precedent allowing patent holders to restrict how consumers can use the products they buy. That decision, and the precedent it relied on, departs from long established legal rules that safeguard consumers and enable innovation. When you buy something physical—a toaster, a book, or a printer, for example—you expect to be free to use it as you see fit: to adapt it to suit your needs, fix it when it breaks, re-use it, lend it, sell it, or give it away when you're done with it.

Wired [Trump's Budget Is Awful if You're a Worker, Great if You're a Robot](#)

WHEN THE ROBOTS rise up, they won't take your life. They'll take your job, particularly those in fields primed for automation, like manufacturing, trucking, and customer service. Technologists, economists, and policymakers believe this future is all but inevitable, and say it's time to begin thinking seriously about how to ensure artificial intelligence advances humanity—and improves the economy, without leaving the middle class behind. Two economists who recently left Washington say the answer lies in ensuring the government provides enough of a safety net to help middle class Americans navigate the coming transition. Jason Furman and Gene Sperling—former chief economic advisors to President Obama—prefer to think of it as a bridge, not a net, that will help people reach the future.

Notable Quotes

“For an issue as critical and potentially dangerous as mass surveillance, a bill reauthorizing Section 702 must be safeguarded against any such abuse. We need to know the administration has not secretly reinterpreted the law and that the will of Congress has been faithfully implemented.”

– [Daniel Schuman, policy director, and Sean Vitka, policy counsel, Demand Progress](#)

“The law governing encryption workarounds remains uncertain and underdeveloped. Whether encryption will be a game-changer or a speed bump depends on both technological change and the resolution of important legal questions that currently remain unanswered.”

– [Orin Kerr, law professor, George Washington University & Bruce Shneier, Chief Technology Officer, IBM Resilient](#)

“I could imagine a community of nations committed to the rule of law developing a set of norms, a framework, for when government access [to encrypted devices] is appropriate.”

– [FBI Director James Comey](#)

VFI Executive Briefing

A weekly roundup of technology news

March 20 – March 24, 2017

“No matter how you look at it, a perpetual gag order is inconsistent with the First Amendment... Imagine a law that does stop and frisk and says you can’t talk about this unless you go to court. That’s not something that would be allowed, but it’s allowed here. The evidence is quite strong that my clients wish to speak, and transparency reports are common in this industry.”

– [Andrew Crocker, staff attorney, Electronic Frontier Foundation](#)

“The fact that our intelligence-gathering laws leave room for politically motivated surveillance should give us pause. And it’s not enough for President Trump or members of Congress to simply express outrage that the private communications of political leaders could have been surveilled. With the expiration of Section 702 looming, they have the opportunity to push for a complete overhaul of our surveillance authorities, and ensure that they are brought fully in line with the requirements of our Constitution.”

– [Neema Singh Guliani, legislative counsel, ACLU](#)

“The FBI was unable to tell us how many people unmask names and until we get to the bottom of who has the ability to unmask names, I don’t think we’d be able to reauthorize FISA.”

– [House Intelligence Committee Chairman Devin Nunes](#)

“What happened with Trump’s folks is a perfect opportunity for Americans to understand how “incidental” surveillance of citizens’ works, what happened to the data, and the inherent risks of this level of collection for all of our privacy so at least we’re all informed about how all of this works.”

– [Scott Shackford, associate editor, Reason](#)

Judge Gorsuch’s opinion leaves open the questions of whether and how the third-party doctrine, which holds that an individual does not have a reasonable expectation of privacy in what he or she shares with third parties, applies to email.

– [Sarah Tate Chambers, Lawfare Blog](#)

Social Highlights

- **@dvolvz:** [Republicans at Monday's hearing were obsessed with surveillance "unmasking." Today showed why.](#)
- **@ericgeller:** [Great explainer by @Cory Bennett of how the IC might have collected comms involving the Trump transition team:](#)
- **@just_security:** [With this week's talk of Section 702, here's how @danielschuman & @SeanVitka think it should be reformed:](#)
- **@MikeScarcella:** [Tech, telecom companies challenge secrecy protocols for FBI national security letters Video:](#)
- **@Reuters:** [Lawmaker suggests U.S. surveillance of foreigners picked up Trump calls](#)

VFI Executive Briefing

A weekly roundup of technology news

March 20 – March 24, 2017

- **@verge:** [Prosecutors think they can extract data from phones seized during Inauguration Day protests](#)
- **@ericgeller:** [Comey on designing technical solution to encryption: "I really do think that we haven't given this the shot it deserves."](#)
- **@Gizmodo:** [Prosecutors say they are hacking over 100 phones confiscated at inauguration protests](#)
- **@kateconger:** [Alt headline: "I'm very confused by all of this right here"](#)
- **@lawfareblog:** [Sarah Tate Chambers: Gorsuch on Cyber-Related Issues: Part One](#)
- **@Slate:** [The government probably did spy on Trump, because it surveils almost all Americans:](#)