VFI Executive Briefing
A weekly roundup of technology news
May 8 – 12, 2017

TABLE OF CONTENTS

SPECIAL COVERAGE – DIGITAL PRIVACY

The postponed Senate Judiciary Hearing looking at U.S. law enforcement's ability to access data stored overseas had some coverage on the topic this week. **The Hill** published an op-ed by Michael Chertoff, former Secretary of Homeland Security, calling for the U.S. government to pursue new evidentiary rules and bilateral agreements with nations around the world to create mechanisms for law enforcement to legally access data stored abroad. Chertoff highlights the reciprocal agreement with the UK currently pending in Congress as a common-sense model for this global framework. **Politico Morning Cybersecurity** and **The Hill** reported on the delay of the Senate Judiciary subcommittee hearing.

Unrelated, The National Constitution Center launched **A Twenty-First Century Framework for Digital Privacy: Balancing Privacy and Security in the Digital Age.** The series features leading experts who consider the future of the Fourth Amendment in the digital age, reflect on the challenges that new technologies pose to privacy and security, and tackle one of the most important legal challenges of the digital age—how to protect privacy and security in the era of cloud computing. The series features an overview by **Jeffrey Rosen**President and CEO of the Constitution Center and white papers by the following experts:

- Jennifer Daskal, Associate Professor of Law at American University

Whose Law Governs in a Borderless World? Law Enforcement Access to Data Across Borders
Jennifer Daskal explores the challenges posed by data mobility and considers how best to resolve cross-border data disputes in a way that promotes privacy, security, and sovereignty.

- Jim Harper, Vice President of the Competitive Enterprise Institute

Administering the Fourth Amendment in the Digital Age
Jim Harper critiques current Fourth Amendment doctrine and calls on courts to adopt a new approach that hews closely to the Fourth Amendment's text and protects data, information, and communications as a key form of property.

- David Kris, former Assistant Attorney General for National Security

Digital Divergence
David S. Kris challenges the view that balancing privacy and security in the digital age is a zero-sum game. Instead, he explores how advances in digital technologies are threatening both privacy and security.

- Neil Richards, Thomas and Karole Green Professor of Law at Washington University

Secret Government Searches and Digital Civil Liberties
Neil Richards tackles the issue of "secret government searches"—namely, instances of government surveillance that remain secret to the search target.

- Christopher Slobogin, Milton R. Underwood Chair in Law at Vanderbilt University

Policing and The Cloud
Christopher Slobogin explores how best to construct legal approaches that will allow the government to harness The Cloud's investigative potential, while also limiting the opportunities for government abuses.

VFI Executive Briefing
A weekly roundup of technology news
May 8 – 12, 2017

HILL UPDATE

The Des Moines Register **Grassley faces privacy test over our data**
The Des Moines Register published an op-ed by contributor Steve Sherman previewing the postponed Senate Judiciary Subcommittee hearing on cross-border data issues and urging Congress to act quickly to modernize the laws governing the cloud. Sherman highlights the risks and challenges posed by U.S. efforts to use a warrant to reach across borders to access data, including promoting data localization and infringing on personal privacy rights. Sherman closes with a warning against using the hearing to overturn the Second Circuit decision in Microsoft's warrant case.

The Hill **Senators press Trump for cyber deterrence, response strategy**
The issue has taken center stage in Washington in the wake of high-profile cyber intrusions and attacks in both the public and private sectors, and has been amplified by Russian interference efforts in the presidential election. Sen. John McCain (R-Ariz.), chairman of the Armed Services Committee, expressed frustration on Tuesday over the Trump administration's lack of a strategy to address cyber threats despite his pledge to deliver an anti-hacking plan within 90 days of taking office.

ARTICLE SUMMARY

Wired **Microsoft Is Right: We Need a Digital Geneva Convention**
STATE-SPONSORED HACKERS MAY have meddled in political campaigns from the US to France to the Netherlands. And while nations are finding it tough to cooperate on the issue, Microsoft is pushing for more global cooperation, not less, in proposing a Digital Geneva Convention to prevent cyberwarfare. By invoking the Geneva Convention, Microsoft appears to want to learn from the past. And history shows that while the company is right to propose action, international agreements alone won't fix our vulnerabilities in cyberspace. Our best chance of success starts with voluntary industry standards. Microsoft's president and chief legal officer, Brad Smith, pitched Microsoft's ideas for international cooperation at the RSA security conference in February.

Daily Caller **Congress Must Act Quickly To Protect Americans' Safety And Privacy**
The Daily Caller published an opinion piece by Drew Johnson, national director of the Protect Internet Freedom, urging Congress and the Department of Justice to work together to support and pass the International Communications Privacy Act (ICPA). Johnson highlights how ICPA will enable legal authorities to gather information stored abroad using warrants that apply extraterritorially while respecting the sovereignty of foreign nations. Johnson warns that letting the courts decide the issue of extraterritorial access to data poses risks to law enforcement and personal privacy.

The Hill **Trump signs cybersecurity executive order**
President Trump has signed an executive order on cybersecurity, homeland security adviser Tom Bossert announced Thursday at the press briefing. The order was long awaited by the cybersecurity community. Drafts of the executive order have leaked since the first days of the Trump administration. The White House once even scheduled a signing ceremony, which was latter scrapped.

Bloomberg BNA **Can You Hear Them Now? Robbers Ask SCOTUS for Phone Privacy**
Bloomberg BNA reported on three potential Supreme Court cases (*Carpenter v. United States*, *Graham v. United States*, and *Jordan v. United States*) in which the defendants seek to impose a requirement for law enforcement to obtain a warrant for historical cell site location information. The piece notes that the cases offer the Supreme Court an opportunity to weigh in on the validity of the third-party doctrine in the digital age.

VFI Executive Briefing
A weekly roundup of technology news
May 8 – 12, 2017

IPWatchdog **Patents as property rights: What will it take to restore sanity to the narrative surrounding US patents?**
On Monday, May 8th, the U.S. chapter of the International IP Commercialization Council (IIPCC) held an event entitled Promoting Innovation, Investment and Job Growth by Fixing America's Patent System. The event, held in the basement of the U.S. Capitol, featured many speakers and panelists who discussed various issues with the current state of the U.S. patent system and how those issues were reducing the nation's overall investment into research & development (R&D) and overall innovation. Although many of the industry insiders at the event held similar opinions on the current state of the U.S. patent system, bringing their message to a mainstream audience has been difficult. Much of this has to do with the "patent troll" narrative that has been forwarded by the efficient infringement lobby.

Washington Post **The future of net neutrality might rest on this obscure court case**
There's a huge court case you need to hear about. It might not be on your radar yet because, frankly, some of it gets pretty technical. But the outcome is likely to have enormous repercussions for online privacy, net neutrality and the economy. For months, policymakers have been struggling with the implications of this case, FTC v. AT&T, in part because it overturned about a century's worth of established legal practice and also, analysts say, because it appeared to open a wide loophole that businesses might use to evade most federal oversight. On Tuesday the federal appeals court responsible for the ruling announced that it has agreed to rehear the case, potentially opening the door to a different result. Here's everything you need to know.

The Hill **Take the first step toward good global data sharing rules**
Recent events remind us that terrorism and crime are now global phenomena. Attacks in Paris, and here in the U.S. metastasize from rhetoric and calls for violence that begin overseas in the Middle East. Criminal theft at the Bangladeshi national bank has its origins (probably) in North Korea. When I first began my career as a prosecutor back in the 1980s most crime was local. The greatest jurisdictional challenge we had was that physical evidence of a crime in New Jersey might be somewhere in New York City, or Philadelphia. Today, that same crime (or terrorist attack) in New Jersey more often involves digital evidence that is overseas. And that's a problem. Cross-border law enforcement cooperation is hampered by inadequate laws and conflicting jurisdictional demands. As a result, evidence overseas is often, in practice, unavailable to prosecutors.

Washington Post **Trump's FCC chairman has wasted no time enacting a conservative agenda in his first 100 days**
Last week, President Trump celebrated his first 100 days in office without a major legislative achievement to his name. But even as the administration made some headway Thursdaywith a deeply controversial health-care bill, some of Trump's allies in Washington are moving even more swiftly. Few have acted as decisively as Ajit Pai, the Republican chairman of the Federal Communications Commission. Elevated by Trump to the role in January, the Indian American telecom regulator has worked to reduce his agency's profile. He has proposed transferring some of the FCC's authority over Internet providers to other regulators, for example, and has questioned the need for key policies enacted under the Obama administration.

The Hill **Five key players for Trump on cybersecurity**
Profiles of the top people for cybersecurity in the Trump Administration.

- Rob Joyce
- Jared Kushner
- Chris Liddell
- Homeland Security Secretary John Kelly
- Defense Secretary James Mattis

VFI Executive Briefing
A weekly roundup of technology news
May 8 – 12, 2017

NOTABLE QUOTES

"Delays like this are frustrating. Failure to act and clarify when and how law enforcement may access data stored abroad disadvantages American companies operating in the cloud and impedes the protection of consumer privacy."

Morgan Reed, president, ACT | The App Association

"We seem to understand how the technology threatens privacy, but I think we have not yet understood as well how it threatens security. We need that understanding to find a real equilibrium, to make informed judgments about how best to strike the balance between privacy and security. We need it also to identify technological and legal approaches that may enhance both security and privacy, reversing the trend of the past several years."

David S. Kris, executive vice president and general counsel, Intellectual Ventures

"[Riley] was the first time the Supreme Court explicitly recognized that mobile phones are like computers and homes and thus deserve full Fourth Amendment protection. The court could build on Riley….and hold that discovering historical location data is like searching the content of a cell phone and thus is a Fourth Amendment search requiring a warrant."

Christopher Slobogin, director of the criminal justice program, Vanderbilt University

"Cross-border law enforcement cooperation is hampered by inadequate laws and conflicting jurisdictional demands. As a result, evidence overseas is often, in practice, unavailable to prosecutors. Congress has an opportunity to take the first steps toward fixing the problem; it should seize that chance."

Michael Chertoff, former Secretary of Homeland Security

"The ICPA gives Congress the opportunity to protect our personal information from unnecessary snooping, while working with our allies to obtain valuable data that can protect American citizens. Leaving the issue to the courts will ultimately damage the speed and efficiency needed by law enforcement to obtain sensitive data that could thwart terrorism, while unnecessarily violating the privacy of innocent, honest Americans."

Drew Johnson, national director, Protect Internet Freedom

"Courts rarely follow the full analysis Justice Harlan's formulation suggests. They rarely inquire into a defendant's "actual (subjective) expectation of privacy," for example, or how it was "exhibited." … Against litigants importuning about privacy, courts after Katz *have found as often as not that the Fourth Amendment does not protect the security of sensitive and revealing information*."

Jim Harper, vice president, Competitive Enterprise Institute

"But there are several reasons why the simple translation of the traditional rules governing searches and seizures to the world of digital evidence does not make good sense. There are, after all, key—and highly relevant—distinctions between digitalized evidence and its more tangible counterparts. Our failure to adequately account for these differences is having increasingly negative consequences for our security, our privacy, and our economy."

Jennifer Daskal, professor of law, American University

"This [Senate Judiciary subcommittee hearing] will serve an important purpose, yet it should not be used as a means to overturn the Microsoft decision with a new statute that violates our privacy.

Allowing warrants to reach overseas, without applying the laws of the nation where the data resides, would lead to less privacy. Taking away more of our privacy in this manner will not solve the problem: We need a complete modernization of our current law to address both privacy and law enforcement concerns."

Steve Sherman, contributor, The Des Moines Register

"Richards tackles the growing problem of secret government searches – such as when law enforcement compels production of a target's emails from a service provider and simultaneously obtains a gag order indefinitely prohibiting the service provider from giving its customer notice of the search. (Microsoft is challenging these gag orders in a lawsuit in the Western District of Washington; although the court recently dismissed the Fourth Amendment challenge, it has permitted Microsoft's First Amendment challenge to proceed.)"

Jennifer Daskal, professor of law, American University

SOCIAL HIGHLIGHTS

- **@BlogsofWar:** Will Comey's encryption legacy at FBI go dark?
- **@ConstitutionCtr:** .@TheParallax talks to @ConstitutionCtr's Tom Donnelly about digital privacy & new white paper series w. @Microsoft.
- **@dnvolz:** NSA Rogers says much of intelligence community's insight on Russian interference during election was gleaned from Section 702 surveillance
- **@ericgeller:** Wyden slams Cotton for saying IC shouldn't produce a report on Americans swept up in 702 surveillance b/c it would compromise their privacy.
- **@astepanovich**: Trump's ousting of Comey may open the door for expansion of gov surveillance powers
- **@CenDemTech:** .@Richardson_Mich: "If you just build a backdoor, ...[it's] sitting there & can be exploited by bad guys too:"
- **@ConstitutionCtr:** .@jendaskal discusses @ConstitutionCtr's newly launched white paper series on digital privacy. @just_security
- **@engadget:** Senator confirms FBI paid $900,000 to unlock San Bernardino iPhone
- **@Jim_Harper:** Nice @jendaskal summary of my @ConstitutionCtr paper on the Fourth Amendment.
- **@BobLoeb**: The Senate Judiciary Committee, Subcommittee on Crime & Terrorism, is having hearings today on law enforcement access to data stored abroad
- **@ChertoffGroup**: NEW: Michael Chertoff authors an opinion editorial in @thehill on global data sharing rules.
- **@ITIFdc**: Ahead of tomorrow's @SenJudiciary hearing on law enforcement access to data, here's an innovation-friendly approach
- **@BlogsofWar**: New White Paper Series: 21st Century Framework for Digital Privacy
- **@ConstitutionCtr**: On May 10, CEO @RosenJeffrey & panelists discuss digital privacy, #4thAmendment, Brandeis & more. #AmericasTownHall
- **@DailyCaller**: SCOTUS Weighs Seizure Of Cell Tower Data Without Warrant
- **@DavidKris**: My paper on "Digital Divergence," for the National Constitution Center, with a short summary on Lawfare