VFI Executive Briefing
A weekly roundup of technology news
October 10-14, 2016

TABLE OF CONTENTS

HILL UPDATE

Politico Morning Tech: Gamers Back ICPA
Politico's Morning Tech newsletter reported that The Entertainment Software Association wrote a letter to leaders of the House and Senate Judiciary committees expressing support for the International Communications Privacy Act (ICPA). The group highlights Microsoft's Second Circuit Court victory in the warrant case, arguing that ICPA could establish a standard for cross-border data requests.

Morning Consult: International Privacy Bill Sponsors Ask Attorney General for Help
"The government's current position presents unique challenges for a number of industries that increasingly face a conflict between U.S. law and the laws of other countries," Sens. Orrin Hatch (R-Utah) and Chris Coons (D-Del.) and Reps. Tom Marino (R-Pa.) and Suzan DelBene (D-Wash.) wrote in the letter.

SPECIAL COVERAGE–Clinton vs. Trump: Comparing the Candidates' Positions on Technology and Innovation

Since the election is almost upon us, I wanted to share out a publication that comprehensively compares the 2016 presidential candidates' technology and innovation policy agenda. The Information Technology and Innovation Foundation (ITIF) has put together such a report for the previous two election cycles. They released this report on September 6th.

ITIF is a nonpartisan research and educational institution that focuses on innovation, productivity, and digital economy issues. It does not endorse any candidates for office. Rather, "our goal in providing a factual, impartial comparison of the candidates' technology and innovation policies is to amplify the national dialogue around the need to bolster innovation-based economic growth."

This report is based on information gathered directly from the campaigns' websites and policy documents, and from media accounts of statements the candidates have made. The report begins with an overview of each candidate's general philosophy on technology, innovation, and trade policy, and then compares the candidates' policy positions across nine specific issue areas:

- Innovation and R&D
- Broadband and Telecommunications
- Education and Skills
- Internet and Digital Economy
- Taxes and Budget
- Advanced Manufacturing
- Trade
- Life Sciences and Biotechnology
- Regulation

You can access the report here.

VFI Executive Briefing
A weekly roundup of technology news
October 10-14, 2016

SPECIAL COVERAGE–Russian Hacking

This week, there were several articles concerning Russia, hacking and what is the appropriate response from the US government. I have captured them here as this issue is broader than the current presidential campaign.

NBC News **Russia Hack of U.S. Politics Bigger Than Disclosed, Includes GOP**
"For the past two years, there has been a massive increase in hacking by the Russians," said Dmitri Alperovitch, a cybersecurity expert whose CrowdStrike firm was retained to investigate the hack of the Democratic National Committee. "Not all of it is politics. It is across the board," added Alperovitch, who is involved in the investigation. "But it got more intense this year with the election." [...] U.S. authorities believe the hacking campaign originated with direct orders from the Kremlin and is an attempt to influence the presidential election and advance the broader strategic objectives of the Putin regime.

New York Times **What Options Does the U.S. Have After Accusing Russia of Hacks?**
President Obama's options range from the mild — naming and shaming the Russians, as he did on Friday — to the more severe, like invoking for the first time a series of economic sanctions that he created by executive order after North Korea's attack on Sony Pictures Entertainment. The Justice Department could indict the Russians behind the attacks on the Democratic National Committee and the email accounts of prominent individuals, as it did with members of China's People's Liberation Army, who have been charged with stealing industrial secrets. Or Mr. Obama could sign a secret intelligence finding — similar to many he has issued to authorize Central Intelligence Agency efforts in Syria or drone strikes against the Islamic State — to attack and disable Russian computer servers or expose the financial dealings of President Vladimir V. Putin and his oligarch friends.

The Hill **Putin: Hacks in US have 'nothing to do with Russia's interests'**
Russian President Vladimir Putin told a business forum in Moscow that his nation is not responsible for the hacking of Democratic Party emails in the United States. "They started this hysteria, saying that this is in Russia's interests. But this has nothing to do with Russia's interests," Putin said, according to Reuters. The Obama administration on Friday publicly blamed Russia for stealing digital information from the Democratic National Committee (DNC) and Democratic National Campaign Committee. The hack of the DNC resulted in an embarrassing leak of internal emails just before the party's national convention in July.

CNN **Feds believe Russians hacked Florida election-systems vendor**
Federal investigators believe Russian hackers were behind cyberattacks on a contractor for Florida's election system that may have exposed the personal data of Florida voters, according to US officials briefed on the probe. The hack of the Florida contractor comes on the heels of hacks in Illinois, in which personal data of tens of thousands of voters may have been stolen, and one in Arizona, in which investigators now believe the data of voters was likely exposed.

Politico **Russians, lies and WikiLeaks**
"It is not unthinkable that those responsible will steal and release more files, and even salt the files they

release with plausible forgeries," a bipartisan group of national security experts from the Aspen Institute said in a statement July 28. More broadly, the spreading of false information by intelligence services "is a technique that goes back to Tsarist times[.]" [...] "It has to look and feel real. The whole point is, you're trying to alter reality," said Kenneth Geers, a former staffer at NATO's cyber defense center in Tallinn, Estonia, noting that Russian hackers study conversations on their targets' network before attempting to forge their communications. Estonia is frequent target of suspected Russian digital assaults.

ARTICLE SUMMARY

Washington Post **Facebook, Twitter and Instagram sent feeds that helped police track minorities in Ferguson and Baltimore, report says**
A powerful surveillance program that police used for tracking racially charged protests in Baltimore and Ferguson, Mo., relied on special feeds of user data provided by Twitter, Facebook and Instagram, according to an ACLU blog post published Tuesday. The companies reportedly provided the data — often including the locations of users — to Geofeedia, a Chicago-based company that says it analyzes social media posts to deliver surveillance information to 500 law enforcement agencies. The social media companies sought to restrict Geofeedia's access to the streams of user data in recent weeks after the ACLU discovered them and alerted the companies about looming public exposure.

The Hill **Why Yahoo's breach could turn the SEC into a cybersecurity tiger**
The U.S. Securities and Exchange Commission (SEC) has 500 million new reasons to examine the rules on when companies must disclose cyber risks and attacks. That's the number of accounts that Yahoo said were hacked in what's being called the largest data breach ever. The company on Sept. 22 blamed a "state-sponsored actor" for the theft of names, email addresses, telephone numbers, dates of birth and encrypted passwords. While Target, the U.S. Office of Personnal Management and seemingly countless other high-profile attacks have inflamed internet security fears in recent years, the unprecedented size of the Yahoo breach and the fact that it took the company two years to disclose it is drawing unusual heat in Washington.

CNET **Supreme Court grills Apple, Samsung over value of design patents**
Even the US Supreme Court justices were a little befuddled over what to do with the legal saga between Apple and Samsung. The two largest phone makers in the world squared off in the highest court in the land Tuesday over the value of design patents, marking the likely conclusion to a long-running battle that goes back to a 2012 case. One nuance of the case -- how jurors were supposed to break out the value of a design from the overall product -- was a source of most of the questions. The justices wanted to know what instructions the jury would be given when looking at damages.

Politico **Morning Cybersecurity: Could Encryption Tilt the Tar Heel State**
Politico published an article analyzing how Senator Richard Burr's controversial stance on encryption could impact his reelection campaign. The article notes that Burr has faced considerable resistance from the libertarian wing of the due to encryption legislations Burr has proposed.

VFI Executive Briefing
A weekly roundup of technology news
October 10-14, 2016

Politico **Bridging the trans-Atlantic data divide: Privacy shield and what's next**
Politico published a special working group report on the transatlantic data divide and challenges facing the EU-U.S. Privacy Shield agreement. The working group was comprised of several policymakers and stakeholders, including BSA President Victoria Espinel and New America's Open Technology Institute Policy Counsel Robyn Greene. The group provided key policy recommendations to bridge the divide, including reform of surveillance programs and engaging in global cybersecurity conversations.

Washington Post **Why Obama thinks about cybersecurity as fighting a pandemic**
After facing an unprecedented wave of cyberattacks against private and public organizations during his presidency, President Obama thinks about digital threats like a public health crisis, he said in a Wired Magazine interview published Wednesday. Instead of approaching cybersecurity as a traditional battle, he thinks about defending systems as if preparing for a pandemic.

Los Angeles Times **The government and the courts are finally getting fed up with patent trolls — and stupid patents**
Almost nobody disputes that America's patent system is a mess, or that it's been that way for an unconscionably long time. Overworked and misguided patent examiners issue patents for manifestly undeserving claims. An entire industry of patent trolls has sprung up to assemble patent rights and exploit them, not to make products or develop services, but to harass other businesses into paying them off to avoid costlier litigation.

Recode **A new generation of 5G will change everything from platforms to self-driving cars**
This week, President Obama will arrive in Pittsburgh to convene the first-ever White House Frontiers Conference. The conference will bring together innovators from across the country to focus on how science and technology is shaping the 21st century, and particularly the role of innovation in building smarter and more inclusive communities. It will be an important discussion, and a timely one, as we are on the cusp of a key technological revolution that will change everyone's lives in ways we can only dimly envision today.

Information Week **Political Positions On Cybersecurity Matter To Millennials**
Politicians of all stripes take notice: ignoring cyber issues could derail your career. A new study released today by Raytheon and the National Cyber Security Alliance (NCSA) found that 53 percent of U.S. millennials surveyed say that a candidate's position on cybersecurity will impact their level of support for that candidate. Another 50 percent say cybersecurity has not been discussed enough during the current election.

Ars Technica **Senator wants nationwide, all-mail voting to counter election hacks**
In an e-mail, Sen. Ron Wyden, a Democrat, told Ars: "We should not underestimate how dangerous... attacks on election systems could be. If a foreign state were to eliminate registration records for a particular group of Americans immediately before an election, they could very likely disenfranchise those Americans and swing the results of an election. Recent efforts by some states to make it more difficult to vote only serves to increase the danger of such attacks. This is why I have proposed taking Oregon's unique vote-by-mail system nationwide to protect our democratic process against foreign and domestic attacks."

The Hill **Google: More than 44K government requests for data**
Government requests for Google user data rose slightly in the first half of 2016, the company said on Thursday. Google said that it received 44,943 requests from government entities worldwide in the first six months of the year, up from 40,677 in the previous six month period. The requests affected 76,713 accounts — a decrease from the previous six months. The company said it had provided the authorities with some data in 64 percent of cases. That was the same rate as in the prior six months.

Notable Quotes

"Perhaps more consequential than the fact that everything is collected may be the fact that nothing is deleted. It's one thing to have to worry that anything you do online may be tracked by a corporation or government. It's another to have to worry about the possibility that your data may be exposed, whether maliciously or inadvertently, ten or twenty years from now."

– Jameel Jaffer, deputy legal director, American Civil Liberties Union

"These platforms need to be doing more to protect the free speech rights of activists of color and stop facilitating their surveillance by police. The ACLU shouldn't have to tell Facebook or Twitter what their own developers are doing. The companies need to enact strong public policies and robust auditing procedures to ensure their platforms aren't being used for discriminatory surveillance."

– Nicole Ozer, technology and civil liberties policy director, American Civil Liberties Union

"Everyone at the table agreed the U.S. must continue bringing greater transparency to the American government's surveillance practices both at home and abroad. But various parties disagreed on what further changes, if any, are needed on the scope and limits of NSA programs that, for example, permit the United States to collect foreigners' communications from American companies based on American soil without court warrants, or that collect global Internet traffic in bulk when the agency is operating outside the United States."

– Politico on the EU-U.S. Privacy Shield

"ICPA also provides improved procedures and safeguards for handling request from foreign governments for stored communications. We think this is an area worthy of attention, especially in light of the recent ruling in the "Ireland" case. The U.S. Court of Appeals for the Second Circuit makes clear that the U.S. Congress did not give the U.S. Government the authority to use warrants unilaterally to reach beyond U.S. borders. We recognize that law enforcement has legitimate needs to access stored communications, but it should do so in a way that respects fundamental rights, including personal privacy."

– The Entertainment Software Association letter in support of ICPA

"Stopping law enforcement use of social media is simply impossible in that there are so many monitoring companies out there and the government has any number of myriad contractors and shell companies it can contract services through. In short, the ACLU was able to turn up Geofeedia's contracts because

police departments purchased its services directly – in future they are more likely to use third party contractors who in turn purchase monitoring services through yet other companies, providing a much more impenetrable shroud around their monitoring access."

- Kalev Leetaru, senior fellow, George Washington University Center for Cyber & Homeland Security

Social Highlights

- **@ACLU:** .@ACLU obtains records on social media surveillance targeting activists of color, presses companies for change
- **@crampell:** Facebook, Twitter and Instagram sent feeds that helped police track minorities in Ferguson and Baltimore, ACLU says
- **@csoghoian:** Is text messaging more like email or a phone call? The answer is important. Email=court order. Phone=subpoena.
- **@FaizaPatelBCJ:** Critical issues w social media monitoring by law enforcement:
- **@JameelJaffer:** I gave the Zenger lecture at @columbiajourn last week--about surveillance, secrecy, privacy. Text posted here:
- **@Bing_Chris:** .@RonWyden on how Russia aggression in cyberspace will impact encryption policy negotiations moving forwards
- **@googlepubpolicy:** Today, we've updated our Transparency Report on government requests for user data:
- **@josephfcox:** New: British Transport Police spent £40,000 on Social Media Surveillance Software. Can monitor 'mood' of communities
- **@kashhill:** It's not just the @ACLU and @EFF. Top Verizon lawyer says it's too easy to give your location information to cops.
- **@TechCrunch:** Facebook, Twitter cut off data access for Geofeedia, a social media surveillance startup
- **@SenOrrinhatch:** Today Hatch, @ChrisCoons, @RepTomMarino and @RepDelBene urged the DOJ to work with Congress on #ICPA