VFI Executive Briefing
A weekly roundup of technology news
April 25-29, 2016

TABLE OF CONTENTS

HILL UPDATE

ECPA REFORM Passed House 419-0.

The Hill Senate pressured to take up email privacy bill after overwhelming House vote
Lawmakers and tech advocates are calling on the Senate to quickly take up an email privacy bill that was overwhelmingly approved by the House this week. After years of delay, the House on Wednesday approved the bill 419-0. Lawmakers are hoping the lopsided vote will push the upper chamber to act. "Now that the House has passed this bill by a vote of 419-0, it's time for the Senate to act.

The Hill: Congress Getting it Right on Email Privacy
For thirty years, the federal government has operated under the premise that the American people do not have a reasonable expectation of privacy in their emails. What's worse, almost no one is aware of it.

SPECIAL COVERAGE

On April 26, a group of leading educators, organizations, CEOs, and 27 Democratic and Republican governors sent an open letter to Congress and the American people calling for federal funding to provide every student in every school the opportunity to learn computer science.

The development received wide press coverage, including:

The Washington Post, "Top Business Leaders, 27 Governors, Urge Congress to Boost Computer Science Education"
The Hill, "Tech Leaders Press Congress on Computer Science Funding"
Huffington Post, "Dear Congress, Give Leila the Opportunity to Learn Computer Science"
Engadget, "Tech Giants Push Congress for K-12 Computer Science Education"

ARTICLE SUMMARY

The Verge [With its retreat in New York, the FBI has lost the encryption fight](#)
As 2015 drew to a close, you might be forgiven for thinking the encryption debate was all talk. There had been a lot of speeches and it was clear the FBI didn't like Apple's default encryption system — but what could they actually do about it? They had been leaning on Congress all year and getting nowhere. Then, everything changed. On February 16th, the FBI took Apple to court over an iPhone used by one of the San Bernardino attackers, putting encryption at the center of the largest terrorism-linked shooting in the US in years.

Fortune [Supreme Court Hears Case on Bad Patents With Tech and Pharma Firms Watching Closely](#)
Patents are meant to promote innovation but, in recent years, critics say a glut of bad ones has harmed the U.S. economy. These weak patents can result in undeserved monopolies, and allow so-called patent trolls to shake down retailers and other productive companies. In recent years the Supreme Court has heard literally dozens of patent cases as part of an effort to sort out the mess. On Monday the Justices will be at it again in a major case that is being followed closely by the auto and tech industries and by intellectual property lawyers.

Politico [Report: Presidential campaign apps failing to safeguard data](#)
People who share their personal information with presidential campaign apps may be putting their privacy at risk, according to new research from the cybersecurity firm Symantec — which found that more than half of mobile apps related to campaigns for the White House "leak" user data by failing to secure it properly. The applications that fail to keep users' data safe from potential snoops include the official apps of GOP candidates Ted Cruz and John Kasich, the company said in a report released this morning.

The Hill [Five internet powerbrokers who could shape the election](#)
The presidential election is increasingly being waged online, giving an outsized influence to Internet powerbrokers. Social media has become one of the most powerful ways to reach voters, with candidates in both parties using the technology to raise money, distribute ads and win over supporters. Online news and video sites, meanwhile, have become a place where the campaigns compete to "drive the narrative" with their preferred storylines.

The Verge [Can AI fix education? We asked Bill Gates](#)

The rise of smartphones has transformed the way students communicate and entertain themselves. But the classrooms they spend so much of their time in remain stubbornly resistant to transformation. On one hand, technology has long had a home in classrooms — I learned to type on an Apple IIe in the late 1980s. But for most schools, the approach to teaching remains stubbornly one-size-fits-all: a single teacher delivering the same message to a group of about 30 students, regardless of their individual progress.

The Hill [FBI will not tell Apple how it hacked San Bernardino iPhone](#)
The FBI told Apple about a security vulnerability in its Mac and iPhone software earlier this month, the first time the agency has disclosed such a flaw under a controversial White House review process, according to Reuters. The April 14 disclosure — which involved a flaw in older devices that had already been patched by the company — came one day after a report that the agency did not believe it would be able to participate in a White House review of the hacking technique used to access the iPhone belonging to one of the San Bernardino, Calif., shooters.

Morning Consult [Complex Fight Over Patent Trolls Hits Washington TV Screens](#)
The battle between the tech community, academics, venture capitalists and scientists over reforming American patent laws is pitting groups with the similar mission of protecting U.S. invention against each other. They are fighting over two bills — the Innovation Act in the House and the PATENT Act in the Senate. The dynamic is now getting airtime on the TV sets of Washington, D.C., residents as one side pushes back against legislation aimed at stopping "patent trolls" from extorting money from companies.

CNBC Interview: [CNBC's Squawk Box](#) aired an interview with Brad Smith discussing Microsoft's recent lawsuit challenging indefinite secrecy orders. Smith detailed Microsoft's reasons for filing suit, explaining that the government's use of gag orders "goes too far and really infringes on people's constitutional rights." Asked about who customers should trust with access to their data, Smith said that "people should trust themselves," noting however that to do so, people need and deserve more information about how their data is accessed.

Ars Technica [Rule 41 would make it easier for the government to carry out hacks](#)
Privacy activists and at least one senator are up in arms over a proposed change to a section of the [Federal Rule of Criminal Procedure](#) that would allow any magistrate judge to issue warrants authorizing government-sanctioned hacking

anywhere in the country. If the proposal does go forward, it would mark a notable expansion of judicial power to sign off on "remote access" of criminal suspects' computers. As Ars has reported previously, [for more than two years now](#), the Department of Justice has pushed to change Rule 41 in the name of being able to thwart online criminal behavior enabled by tools like Tor.

NOTABLE QUOTES

- *"As we have said previously, these cases have never been about setting a court precedent; they are about law enforcement's ability and need to access evidence on devices pursuant to lawful court orders and search warrants. In this case, an individual provided the department with the passcode to the locked phone at issue in the Eastern District of New York. Because we now have access to the data we sought, we notified the court of this recent development and have withdrawn our request for assistance. This is an ongoing investigation and therefore we are not revealing the identity of the individual."*
  - [Emily Pierce, spokeswoman, Justice Department](#)

- *"Congress is voting today to pass my Email Privacy Act. With 315 additional House cosponsors, the most-widely supported bill in Congress extends the same Fourth Amendment probable-cause protections afforded our physical mail to our digital communications and storage. It would require government agencies to obtain a warrant to search your Gmail account, just as it would at your home. Lawmakers in 1986 should be commended for attempting to codify privacy protections for a ground-breaking new technology. Unfortunately, they got it wrong. Not through their own fault, but through an unforeseen evolution of the technology and how it is utilized by our society. Today, Congress is getting it right."*
  - [Rep. Kevin Yoder](#)

- *"These amendments will have significant consequences for Americans' privacy and the scope of the government's powers to conduct remote surveillance and searches of electronic devices. Under the proposed rules, the government would not be able to obtain a single warrant to access and search thousands or millions of computers at once; and the vast majority of the affected computers would belong to the victims, not the perpetrators, of a cybercrime."*
  - [Sen. Ron Wyden](#)

- *"For the government to unlock everything there has to be a key to everything. Every other person in the world can find that key and use it too. It's a fundamental problem of science. Encryption is not an unbreakable as well. Or if it is, it is one we can get around, if we are patient, if we are careful, if we think and plan how to go about our investigations."*
    - [Edward Snowden](#)

- *"I've said on many occasions that I agree that this law needs to be updated to better protect privacy. Members of this committee on both sides of the aisle have expressed concerns about the details of this reform, and whether it's balanced to reflect issues raised by law enforcement. I plan on taking a close look at the bill that passed the House, and talking with interested stakeholders and members of the committee to try to find a path forward for ECPA reform here in the Senate."*
    - [Sen. Chuck Grassley](#)