

TABLE OF CONTENTS

Hill Update – 1
Article Summary – 2
Notable Quotes – 4

HILL UPDATE

PCWorld [Senators want warrant protections for US email stored overseas](#)

A new bill in Congress would require U.S. law enforcement agencies to obtain court-ordered warrants before demanding the emails of the country's residents when they are stored overseas. The International Communications Privacy Act, introduced Wednesday by three senators, would close a loophole that allows law enforcement agencies to request emails and other electronic documents without warrants.

Morning Consult [Hatch Introduces Bill Clarifying Rules for Accessing Online Communications Overseas](#)

American law enforcement would be permitted to access messages of U.S. citizens, by way of a warrant, regardless of where they are in the world under legislation introduced Wednesday by Utah Sen. Orrin Hatch (R). The measure, which is co-sponsored by Sens. Chris Coons (D-Del.) and Dean Heller (R-Nev.), would also allow investigators to obtain warrants for the online communications of foreigners if they are from or located in countries that have law-enforcement agreements with the United States.

InsideSources [Senate Stalls on House-Passed Email Privacy Bill](#)

A Senate committee stalled legislation Thursday to reform a 30-year-old law granting the government warrantless access to Americans' six-month-old emails, one month after the House unanimously passed similar legislation. Sponsors of the Electronic Communications Privacy Act (ECPA) Amendments Act on the Senate Judiciary Committee agreed to hold the bill over to address concerns and potential amendments posed by their colleagues.

CNET [Senate bill would let FBI read your emails without a court order](#)

CNET reported that the Senate Intelligence Committee approved the 2017 Intelligence Authorization Act, which would enable the FBI to obtain email records using only a National Security Letter. Committee Chairman Richard Burr and Vice Chairman Dianne Feinstein expressed their support, noting that it makes it easier for the government to keep Americans safe, while Sen. Ron Wyden, who was the lone dissenter, stated that it would take "a hatchet to important protections for Americans' liberty."

ARTICLE SUMMARY

Wired [The Oracle-Google Case Will Decide the Future of Software](#)

THE LEGAL BATTLE between Oracle and Google is about to come to an end. And nothing less is at stake than the future of programming. Today lawyers for both companies are set to make their closing arguments in the fight over whether Google's use of the Java application programming interface (API)—an arcane but critically important part of the Android mobile operating system—was legal. Regardless of how the jury rules, the case has already had a permanent effect on the way developers build software.

CBS News [Jury sides with Google in \\$9 billion intellectual property battle](#)

Google's Android software just dodged a \$9 billion bullet. A federal jury found Thursday that Google didn't need permission to use a rival's programming tools as it built Android - now the world's leading smartphone operating software and a key part of Google's multi-billion dollar Internet business. Software competitor Oracle claimed Google had stolen its intellectual

The Hill [Microsoft to explicitly ban 'terrorist content' on its services](#)

Microsoft is updating its terms of use to specifically ban the posting of "terrorist content" on its services. The company is also considering whether to prominently display "positive messaging" in its Bing search results when users look for terror-related materials. However, it will not hide results for terror content on its search engine unless it is banned by local governments. "Terrorism is one of the truly urgent issues of our time," the company announced Friday. "We are committed to doing our part to help address the use of technology to promote it or to recruit to its causes."

The Hill [Supreme Court shows the way on privacy regulations](#)

In a recent 6-2 decision, the Supreme Court struck a blow for a more rational and consumer-friendly privacy regime by coming down in favor of a "harms-based approach." Although the opinion focused on standing rather than regulatory policy, agencies that enforce privacy regulations, such as the Federal Trade Commission (FTC) and the Federal Communications Commission (FCC) — the latter of which has proposed major new privacy regulations for internet service providers (ISPs) — should take a lesson from the *Spokeo, Inc. v. Robins* decision.

The Hill [Lawmakers urge colleagues to use encryption](#)

A bipartisan pair of lawmakers are encouraging their colleagues to use end-to-end encryption to communicate. "There are a number of easy-to-use applications that have end-to-end encryption for mobile communications. While this method is not foolproof, the use of these apps constructs a huge barrier to your communications being deciphered," Reps. Ted Lieu (D-Calif.) and Will Hurd (R-Texas) wrote in a "Dear Colleague" letter sent Monday.

New York Times [Microsoft Awards First Grants to Help Expand Global Internet Access](#)

VFI Executive Briefing

A weekly roundup of technology news

May 23-27, 2016

Microsoft has largely stood by as other technology giants like Facebook and Google have begun work on grand plans for balloons, satellites, drones, simplified apps and even bicycle hot spots to deliver Internet access to the four billion or so people around the world who are not yet online.

The Wall Street Journal [Should Law Enforcement Have to Get a Warrant to Obtain Stored Emails?](#)

The Wall Street Journal published a joint op-ed from law professors Fred Cate and Stephen Saltzburg arguing counterpoints about whether law enforcement and civil agencies should have to get a warrant to obtain stored emails. Cate argues that the legal protections for the contents of our communications should not depend on the method we use to transmit them, and therefore, warrants should be required to gain access to all email. Saltzburg suggests however that subpoenas and court orders protect privacy better than a warrant since notice is given to affected parties before any data is turned over.

Cybersecurity Caucus [Schools and Universities Must Make Cybersecurity Education a Priority](#)

Cyber-attacks have increasingly become the chosen method of attack against the United States by enemies of our country. Yet despite this, our efforts to educate students to prepare for careers as computer experts are severely lacking. Our schools and universities must embrace change immediately to begin preparing more of our young people to fill the roles needed to defend our national security from cyber-attacks from threats coming from China, Russia, North Korea, and other countries. [More than 209,000](#) cybersecurity jobs in our country are unfilled, and the number of postings for such jobs has increased 74 percent in the last five years. This is expected to grow another 53 percent by 2018.

Washington Post [What's driving Silicon Valley to become 'radicalized'](#)

SAN FRANCISCO — Like many Silicon Valley start-ups, Larry Gadea's company collects heaps of sensitive data from his customers. Recently, he decided to do something with that data trove that was long considered unthinkable: He is getting rid of it. The reason? Gadea fears that one day the FBI might do to him what it did to Apple in their recent legal battle: demand that he give the agency access to his encrypted data. Rather than make what he considers a Faustian bargain, he's building a system that he hopes will avoid the situation entirely.

The Hill [Tech companies warn senators not to 'weaken' email privacy bill](#)

The largest names in the tech industry are pressing senators to approve the House's widely supported email privacy bill without changes. The letter from nearly 70 prominent tech companies and advocates urges the Senate to approve the "carefully negotiated compromise" immediately and without any amendments to "weaken" the legislation. The letter comes as the Senate Judiciary Committee plans to vote on reform during a Thursday markup. The committee already plans to take up the exact text of the House bill, in the form of a substitute amendment.

VFI Executive Briefing

A weekly roundup of technology news

May 23-27, 2016

Washington Times [ACLU asks to join Microsoft in Fourth Amendment fight against DOJ](#)

Attorneys with the American Civil Liberties Union asked a federal judge Thursday for permission to take part in a Fourth Amendment lawsuit brought by Microsoft last month concerning the U.S. government's use of gag-orders, the likes of which have prevented the tech titan from telling thousands of customers annually that their accounts are under surveillance.

The Hill [State aide thought Clinton email was for 'family and friends'](#)

A State Department official who once offered to arrange a "stand-alone" computer for then-Secretary Hillary Clinton said he believed she was only emailing with friends and family — not using it for official work business. Lewis Lukens believed his suggested work-around was "for ease of access," he said during a two-hour deposition with a conservative legal watchdog looking into Clinton's private email server setup. But he assumed that her efforts to access her BlackBerry weren't related to her job as the nation's top diplomat.

Wired [Peter Thiel's Gawker Suit Is Another Free Speech Debacle for Facebook](#)

BILLIONAIRE INVESTOR PETER Thiel has admitted to secretly funding wrestler Hulk Hogan's lawsuit against Gawker Media. In an interview with The New York Times, Thiel called the suit "one of my greater philanthropic things that I've done." The news raises thorny questions about litigation financing and whether wealthy individuals ought to be able to use our court systems as a tool for revenge. (The site revealed in 2007 that Thiel is gay.) But what makes the situation even more complicated is the fact that Thiel sits on the board at Facebook.

Notable Quotes

- *"It makes no sense that the legal protection for the contents of our communications depends on the medium we use to transmit them—or, in the case of email, when it was sent or where it is stored. The weaker standard for the contents of older email made little difference when adopted. Email was in its infancy, and very few Americans had an account. Storage was expensive, and most service providers limited how many emails could be stored and for how long. Customers typically stored email in their computers, which required a warrant to search. Proponents of the weaker protection for older email assumed, not unreasonably, that such email was effectively abandoned and therefore not the subject of a 'reasonable expectation of privacy.'"*

- [Fred Cate, distinguished professor of law, Indiana University](#)

- *"The bill passed by the House does not achieve all of the reforms we had hoped for. Indeed, it removed key provisions of the proposed bill, such as the section requiring notice from the government to the customer when a warrant is served, which are necessary to protect users. However, it does impose a warrant-for-content rule with limited exceptions. It represents a carefully negotiated compromise which preserves existing exceptions to the warrant requirement, provides a new ability for civil agencies to obtain access to previously public commercial content, and maintains the government's ability to preserve records and obtain emails from employees of corporations."*

- [Letter from tech companies and advocacy groups urging the Senate to approve the Email Privacy Act](#)

VFI Executive Briefing

A weekly roundup of technology news

May 23-27, 2016

- *"A basic promise of our Constitution is that the government must notify you at some point when it searches or seizes your private information. Notice serves as a crucial check on executive power, and it has been a regular and constitutionally required feature of searches and seizures since the nation's founding. The government has managed to circumvent this critical protection in the digital realm for decades, but Microsoft's lawsuit offers the courts an opportunity to correct course."*

- [Alex Abdo, senior staff attorney, ACLU](#)

- *"This bill takes a hatchet to important protections for Americans' liberty. This bill would mean more government surveillance of Americans, less due process and less independent oversight of US intelligence agencies. Worse, neither the intelligence agencies, nor the bill's sponsors have shown any evidence that these changes would do anything to make Americans more secure."*

- [Sen. Ron Wyden on 2017 Intelligence Authorization Act](#)