

VFI Executive Briefing

A weekly roundup of technology news

May 29 – June 2, 2017

TABLE OF CONTENTS

Hill Update – 1
Article Summary – 1
Notable Quotes – 3
Social Highlights – 4

HILL UPDATE

The Hill [Trump's pick to lead antitrust division raises concerns over vertical mergers](#)

President Trump's nominee to run the Department of Justice's antitrust division said that vertical mergers, such as the proposed AT&T-Time Warner deal, can "raise competitive concerns." "I think every transaction should be reviewed based on its particular facts and circumstances," Makan Delrahim wrote in response to questions submitted by a group of Democratic senators. "Thus, just because a transaction or particular types of transactions have been approved in the past does not mean that they could not raise competitive concerns in the future." The comment was made in response to a question submitted to the record by Sen. Al Franken (D-Minn.), a member of the Senate Judiciary Committee, about how Delrahim sees vertical mergers, which are deals between companies in different sectors of an industry.

ARTICLE SUMMARY

The Verge [Supreme Court says companies can't use patent law to sue resellers](#)

The Supreme Court has ruled that patent holders can't sue people for reselling or refurbishing a product that's based on those patents. Today, it passed down a decision in Impression Products v. Lexmark International, declaring that printer company Lexmark can't sue companies selling refilled toner cartridges for patent infringement. This reverses a two-part federal court ruling from 2016, affirming that patent law doesn't justify eroding ownership rights. Lexmark International, like many companies that sell printers, makes a lot of its money from customers buying a steady stream of toner cartridges after their initial purchase. But "remanufacturing" companies like Impression Products can take exhausted cartridges, refill them, and independently sell them at lower costs.

Fed Tech Magazine [Trump's 2018 Budget for DHS Emphasizes Federal Network Protection, Cyber Monitoring](#)

The budget requests \$971.3 million "to improve security of the U.S. cyber infrastructure in collaboration with public, private, and international partners." However, some programs are getting shortchanged. As CyberScoop notes: "Despite these increases, not every tech element of the department got its funding goosed. Research and development in the DHS Science and Technology Directorate was slashed by \$100 million and the allocation for the CIO office was also down \$60 million."

Ars Technica [To kill net neutrality rules, FCC says broadband isn't "telecommunications"](#)

The Federal Communications Commission's plan to gut net neutrality rules and deregulate the Internet service market may hinge on the definition of the word "broadband." In February 2015, the FCC's then-Democratic leadership led by Chairman Tom Wheeler classified broadband as "telecommunications," superseding the previous treatment of broadband as a less heavily regulated "information service." This was crucial in the rulemaking process because telecommunications providers are regulated as common carriers under Title II of the Communications Act, the authority used by the FCC to impose bans on blocking, throttling, and paid prioritization.

VFI Executive Briefing

A weekly roundup of technology news

May 29 – June 2, 2017

DefenseNews [NATO might trigger Article 5 for certain cyberattacks](#)

NATO will not rule out invoking Article 5 of its charter should one or more member nations find themselves under a serious cyberattack that threatens critical military and civilian infrastructure. NATO officials told delegates at the International Conference on Cyber Conflict, or CyCon, in Estonia that the Western alliance would deliver a robust response in the event of a serious and prolonged attack on a member state in cyberspace. Article 5 provides for a united response by NATO states should a member nation come under attack.

Wall Street Journal [EU Cheers Tech Giants' Commitment to Tackling Online Hate Speech](#) (subscription required)

Alphabet's YouTube, Facebook, Twitter and Microsoft Corp. MSFT 0.37% have doubled their efforts over the past six months to remove hate speech and other information that incites acts of terror from their platforms, the European Union said Thursday. The assessment is welcome news for the companies, which face growing pressure from Europe's national governments to do more to address racist and xenophobic content. The EU report evaluates the impact of a common code of conduct that the four tech companies agreed on a year ago. They pledged to review precise and substantial complaints regarding users' behavior within 24 hours of receipt and cut off access to the content, if required. The European Commission, the bloc's executive, said the tech companies removed illegal hate-speech content 59% of the time when it was flagged for review, up from a rate of 28% that the commission reported six months ago.

New York Times [China's New Cybersecurity Law Leaves Foreign Firms Guessing](#)

BEIJING — As China moves to start enforcing a new cybersecurity law, foreign companies face a major problem: They know very little about it. The law — which was rubber-stamped by the country's Parliament last year — is part of wide-ranging efforts by Beijing to manage the internet within China's borders. Those efforts have been stepped up in the years since Edward J. Snowden, the whistle-blower and former American intelligence contractor, revealed that foreign technology firms could help governments spy. And while Chinese officials say the new rules will help guard against cyberattacks and prevent terrorism, critics, many of them from businesses, have their concerns..

Washington Post [Your face or fingerprint could soon replace your plane ticket](#)

Headed on a trip? You may soon be able to ditch your boarding pass in favor of your fingers or face. Delta announced, on Wednesday, a new biometric identification pilot program that will eventually let you use your fingerprints instead of a plane ticket. That followed a JetBlue announcement hours earlier that it is testing a program in Boston that will match pictures of customers' faces with the passport database maintained by U.S. Custom and Border Protections. Delta's program, which kicked off at Washington's Reagan National Airport, is in partnership with Clear, a company that already lets customers skip to the front of security lines without identification. To be eligible for the program, one must be a member of Delta's frequent-flier SkyMiles program and a Clear subscriber.

The Hill [How did Obama's massive surveillance state fail to defend Americans against Russia?](#)

The Hill published a contributed opinion piece by former Rep. Lynn Westmoreland criticizing the Obama administration for conducting illegal electronic surveillance under Section 702. Westmoreland states that he was a "big supporter" of Section 702 surveillance while in Congress, but changed his mind on the programs after finding out the Obama administration failed to follow Section 702 minimization procedures.

Forbes: [That Time The FBI Phished A Cop With Poisoned Microsoft Docs](#)

Forbes published an article exploring an investigation in which the FBI was granted a warrant to lawfully use targeted phishing attacks, some of which involved Microsoft products, to unmask and arrest a New York cop accused of stalking and harassing an ex-girlfriend.

VFI Executive Briefing

A weekly roundup of technology news

May 29 – June 2, 2017

NOTABLE QUOTES

- *"Instead of limiting searches to foreign agents who were targets of investigations, the administration searched for communications about those people—meaning Americans who only mentioned a foreign agent would have their communications accessed and analyzed without any warrant or probable cause. This is an obvious violation of the Fourth Amendment."*
[-former Rep. Lynn Westmoreland](#)
- *"The [China cybersecurity] law is both extremely vague and exceptionally wide in scope, potentially putting companies at risk of regulatory enforcement that is not related to cyber security."*
[-Carly Ramsey, associate director, Control Risks](#)
- *"[Section 702] is not limited to counter terrorism... The broad application undermines the moral authority to operate invasive surveillance programs and unnecessarily impugns the rights of people around the world."*
[-Access Now](#)
- *"Government intrusions do raise some 4th amendment legal search concerns. For something like this, we'd want them to have a warrant... This shows a way that police can obtain digital information without using zero-days. It further highlights there's not much of a reason for governments to hoard computer exploits... Even dead simple social engineering works."*
[-Cooper Quintin, security researcher and programmer, Electronic Frontier Foundation.](#)
- *"Technology presents challenges to governments like almost never before. It is a realm that we cannot simply legislate or regulate to control -- we must work with the industry who have their hands on the levers, and invariably, they are in the private sector... Prolific growth in the use of encryption technology is an everyday reality for investigators and we cannot afford for this to remain an obstacle."*
[-Andrew Colvin, Australian Federal Police Commissioner](#)
- *"Following the Snowden disclosures and amid questions about western law enforcement access to data, popular support for data localization has grown in China. There is now a widespread—though inaccurate—belief that geographic location matters for data security and that demanding data stay in China affords a higher level of protection."*
[-Samm Sacks, adjunct fellow, Center for Strategic and International Studies' Technology Policy Program](#)
- *"EFF has long been concerned about law enforcement using private actors, such as Best Buy employees, to conduct warrantless searches that the Fourth Amendment plainly bars police from doing themselves... The key question is at what point does a private person's search turn into a government search that implicates the Fourth Amendment."*
[-Electronic Frontier Foundation](#)
[Lee Tien, senior staff attorney, Electronic Frontier Foundation](#)

VFI Executive Briefing

A weekly roundup of technology news

May 29 – June 2, 2017

SOCIAL HIGHLIGHTS

- **@FinancialTimes:** [China's cyber security law rattles multinationals](#)
- **@ITI_TechTweets:** [Quantum computing's potential for cracking #encryption worries the NSA so it is developing new encryption standards](#)
- **@jimwaterson:** [We've got a problem: We're about to have a national debate over encryption and most politicians/journalists/public don't know what it is.](#)
- **@Lawfareblog:** [Lawfare Editors: June 1 Hoover Event: The Future of Section 702 of the Foreign Intelligence Surveillance Act](#)
- **@PoliticalShort:** [FBI illegally shared spy data on Americans with private parties while NSA illegally searched American's data](#)
- **@verge:** [Facebook, Google, and other tech companies ask lawmakers to reform NSA surveillance law](#)
- **@accessnow:** [#US: Tech giants to Congress: Please change how NSA spies on people #Section702 via @CNET](#)
- **@EFF:** [A former mayor explains from experience why California needs to pass surveillance transparency legislation](#)
- **@govtechnews:** [Apple sees massive increase in national security requests for user data](#)
- **@iblametom:** [Key takeaway? This is probably the way the FBI should be hacking if they're going to do it at all: Warrant + targeted + no 0days required.](#)
- **@ReutersWorld:** [China says controversial cyber law not designed to cripple foreign firms](#)
- **@WashTimes:** [Barack Obama's spy games ignored by yawning media - @washtimes](#)
- **@CNBC:** [China's new cybersecurity law takes effect today, and many are confused](#)
- **@EFF:** [We're suing the FBI to learn how it uses Best Buy Geek Squad informants to search devices without a warrant](#)