Kelly defends cuts to the DHS Science and Tech budget: Secretary John Kelly defended the proposed 20 percent cut to the DHS science and technology budget in front of the House Homeland Security Committee budget hearing. Einstein, DHS’ National Cybersecurity Protection System, used to protect government agencies, would receive $74 million funding reduction. Whereas, DHS’ Continuous Diagnostics and Mitigation program, the department’s cyber operations component, would receive a proposed $4 million increase. Kelly stated that the funding reduction would be offset by leveraging research and development work done at other government labs and the private sector.

FTC announces PrivacyCon 3: The Federal Trade Commission will host PrivacyCon 3 on Wednesday February 28, 2018. The conference will focus on the economics of privacy. Topic to be discussed are: Nature and Evolution of Privacy and Security Risks; Quantifying Costs and Benefits of Privacy from a Consumer Perspective; Quantifying Costs and Benefits from a Business Perspective; and Incentives, Market Failures, and Interventions. The call for presentations ends on November 17, 2017. For more information and the scope of research visit the PrivacyCon 2018: Call for Presentations website.

Jeanette Manfra, Acting Deputy Undersecretary for Cybersecurity for DHS discussed on Wednesday some of the top challenges to implement Trump's cybersecurity executive order. One such challenge is adapting Einstein to a directive that emphasizes federal computer system upgrades. Manfra stated that DHS is “starting to move away a perimeter based security model” and “looking to the future” including the “evolution of our own programs for the adoption and encouragement on cloud and other solutions within the government.” She also said that governance will play an important role. “How do we ensure that when we do have information that CIOs and CISOs within their agencies are able to act on that?"

Uber pay algorithm used to reduce new-hire wages and reinforced gender pay gap: Uber, the ride sharing company, which is already under investigation for sexual harassment and gender bias, was accused of using an algorithm to “optimize” compensation for new-hires that also reinforced a gender pay gap. The algorithm was used to reduce new hire pay for the sake of existing shareholders stake in the company. The use of this algorithm lead to unequal pay for similar roles causing a stir inside the company. It is being reported that the algorithm is being modified.

More trouble for Uber: A top executive from Uber has been fired after he obtained medical records of a customer who was raped during a ride. Eric Alexander, the president of business for the Asia Pacific region of Uber, carried with him the medical record of a woman who was sexually assaulted during a ride in India in 2014. Alexander showed the confidential information
to Uber CEO Travis Kalanick and SVP Emil Michael. It was stated that the medical records were either discussed or shown to many other executives. The handling of this situation was one of the 215 claims reported to two law firms — Perkins Coie and Covington & Burling. —who are investigating mismanagement issues at Uber, including allegations of sexism and sexual harassment.

**Intel agencies want to make the most controversial foreign surveillance rule permanent:** Wednesday June 7, 2017 the Senate Intelligence Committee held hearing on the FISA legislation. The controversial section 702, which allows the government intelligence agencies to intercept communication of foreign intelligence targets, is set to expire on December 31, 2017 if it is not reauthorized by Congress. Both NSA Director Michael Rogers, and Director of National Intelligence Dan Coats testified in front of the committee. Questions were raised about how many U.S. citizens were caught up in the surveillance as it presents a Fourth Amendment concern.

**NSA report details Russian election hijacking attempt:** The NSA report states that just days before the November presidential elections, that Russian Military Intelligence executed a spear-phishing attack against at least one U.S. voting software supplier and more than 100 local election officials. The report suggests that Russian hackers penetrated further into U.S. voting systems than previously understood.

**Supreme Court Reenters Fray on Privacy:** On June 5, 2017 the Supreme Court agreed to review the case Carpenter v. United States addressing an individual’s expectation of privacy in his or her historical cellphone location records. In 2013 Timothy Carpenter was found guilty by a Michigan federal jury of aiding and abetting a series of armed robberies. The prosecutor applied for court orders under the Stored Communications Act (“SCA”), 18 U.S.C. § 2703(d), to obtain more than five months of historical cell phone locations records for Carpenter and other suspects. Under the SCA, a government entity may obtain such records without a warrant (or probable cause) as required under the Fourth Amendment, given that the that data have been stored for more than 180 days. The government entity must offer “specific and articulable facts showing that there are reasonable grounds to believe that” the records sought “are relevant and material to an ongoing criminal investigation.”