Cyber Update
12 February 2019
By Michael Kans

Trump Administration Finds "No Material Impact" on 2018 Elections

The Departments of Justice (DOJ) and Homeland Security (DHS) submitted a classified joint report to the President "evaluating the impact of any foreign interference on election infrastructure or the infrastructure of political organizations, including campaigns and candidates in the 2018-midterm elections" according to a joint press release. DOJ and DHS "have concluded there is no evidence to date that any identified activities of a foreign government or foreign agent had a material impact on the integrity or security of election infrastructure or political/campaign infrastructure used in the 2018 midterm elections for the United States Congress." The agencies added that "[t]his finding was informed by a report prepared by the Office of the Director of National Intelligence (ODNI)."

The DOJ-DHS report was required by "Executive Order on Imposing Certain Sanctions in the Event of Foreign Interference in a United States Election" (Executive Order 13848). On the basis of this assessment, the Department of Treasury must impose all appropriate sanctions, which is not to say sanctions must be imposed. Likewise, the Departments of Treasury and State are required to determine whether they will advise the President to impose additional sanctions.

Also last week, "[i]n preparation for the 2020 elections, the Office of the Director of National Intelligence (ODNI); its National Counterintelligence and Security Center (NCSC) and Cyber Threat Intelligence Integration Center (CTIIC); along with the Department of Homeland Security and the Federal Bureau of Investigation (FBI), today held a classified election security workshop for state election officials from across the country" according to a press release. ODNI explained

> Discussions focused on foreign adversary intent and capabilities against states' election infrastructure, as well as threat mitigation efforts. The goal of this collaborative event was to enhance existing partnerships to ensure the sharing of timely, substantive information on threats to our nation's critical infrastructure. Similar classified workshops were held last year for state election officials and election vendors in connection with the 2018 elections.

Michael Kans, Esq. | mdk@michaelkanslaw.com | @michael_kans

These efforts may be discussed at a House Homeland Security Committee hearing that has been announced for this week "on election security entitled *Defending Our Democracy: Building Partnerships to Protect America's Elections*...[that] will be part of series of hearings the new House Democratic majority is holding on H.R. 1, the *For the People Act*." Cybersecurity and Infrastructure Security Agency Director Christopher Krebs is among the invited witnesses.

U.S. Policymakers Continue To Focus on Huawei and ZTE

Officials in the executive and legislative branches continue to argue that Chinese technology firms, Huawei and ZTE, pose dangers to U.S. national security. Moreover, the Trump Administration has continued pressing allies to forgo the firms when looking to upgrade to 5G wireless networks.

This week, Senators Marco Rubio (R-FL), Chris Van Hollen (D-MD), Susan Collins (R-ME), Mark Warner (D-VA), Jerry Moran (R-KS), Elizabeth Warren (D-MA), and Doug Jones (D-AL) reintroduced the "ZTE Enforcement Review and Oversight (ZERO) Act" that would require the Secretary of Commerce to ensure ZTE's compliance with its July 2018 agreement for the entirety of the ten year period. A failure to comply would result in the immediate forfeiture of $400 million currently held in escrow by the U.S. government. The Department of Commerce's settlement with ZTE arose from "a multi-year conspiracy to supply, build, and operate telecommunications networks in Iran using U.S.-origin equipment in violation of the U.S. trade embargo, and committing hundreds of U.S. sanctions violations involving the shipment of telecommunications equipment to North Korea."

This legislation was introduced during a week in which the United States pressed its allies and other countries to forgo using Huawei technology and products in upgrading to 5G and word has leaked from the White House that an executive order banning Huawei from U.S. wireless networks could be issued next week. To allies Department of State officials have made the case that Huawei technology may be compromised by security risks. Nonetheless, Germany announced that it would not summarily ban Huawei from bidding to build the country's 5G networks. In the same vein, the French Senate rejected legislation that would require telecommunications companies operating in France to receive permission to use certain types of equipment supposedly susceptible to espionage. However, a number of Senators made clear their votes against such legislation were more on procedural grounds as the government tried to tack this language onto a different bill.

Additionally, it has been reported in the media that President Donald Trump will sign an executive order banning both companies from U.S. wireless networks before

MWC Barcelona to be held at month's end. In the same vein, at a think tank event last week, in a conversation on the coming transition to secure 5G networks, Deputy Assistant Secretary of State for Cyber and International Communications and Information Policy Robert Strayer named China and Huawei as posing problems to the development of 5G.

Strayer said that "I think we need to prevent three things: one is unauthorized access to that data, second is the disruption of the functionalities that we expect to occur from the processing, the Internet of Things – all the new transformational uses that we talked about earlier in this discussion – and third, we need to make sure that networks are not a venue for the introduction of other types of malicious cyberthreats that could cause the manipulation of data or the malfunctioning of those types of systems."

Strayer added that "with so much at stake, we talk to our partners about how important it is to continue to seek to have trusted and secure networks." He pointed to fair and transparent bidding processes that would ameliorate corruption issues. Regarding the technology side of 5G, Strayer identified China as a country that raises significant concerns for the U.S. given the close ties between Chinese technology companies and their intelligence agencies. He also pointed to the recent indictments of Huawei as reason for the U.S. and its allies to be wary of the company."

Last week, Huawei responded to a British Parliament committee and explained that it would spend $2 billion over five years in large part to remediate the shortcomings turned up by a British government oversight board. Huawei stated that this funding will "help ensure that our products are better prepared for a more complex security environment both now and in the future." In January, the Chair of the House of Commons Science and Technology Committee wrote Huawei with his concerns about the United Kingdom's communications infrastructure in light of three Five Eyes nations' actions to reduce the roles of Chinese firms in their systems and China's recently enacted National Intelligence Law. In its annual report in July 2018, the Huawei Cyber Security Evaluation Centre (HCSEC) Oversight Board found that "[d]ue to areas of concern exposed through the proper functioning of the mitigation strategy and associated oversight mechanisms, the Oversight Board can provide only limited assurance that all risks to UK national security from Huawei's involvement in the UK's critical networks have been sufficiently mitigated."

Germany Finds Facebook Has Abused its Market Position

Michael Kans, Esq. | mdk@michaelkanslaw.com | @michael_kans

The German agency with jurisdiction over competition issued a decision that potentially could block Facebook from combining the personal data of Germans from other Facebook-owned entities such as Instagram and WhatsApp or from unrelated third-party sources. According to the Bundeskartellamt's press release, the agency "has imposed on Facebook far-reaching restrictions in the processing of user data."

This action follows a month after France's data protection authority levied a €50 million fine on Google "under the General Data Protection Regulation (GDPR), for lack of transparency, inadequate information and lack of valid consent regarding the ads personalization."

The Bundeskartellamt asserted

> According to Facebook's terms and conditions users have so far only been able to use the social network under the precondition that Facebook can collect user data also outside of the Facebook website in the internet or on smartphone apps and assign these data to the user's Facebook account. All data collected on the Facebook website, by Facebook-owned services such as e.g. WhatsApp and Instagram and on third party websites can be combined and assigned to the Facebook user account.

The Bundeskartellamt claimed that "Facebook's terms of service and the manner and extent to which it collects and uses data are in violation of the European data protection rules to the detriment of users." The Bundeskartellamt explained that it "closely cooperated with leading data protection authorities in clarifying the data protection issues involved."

The Bundeskartellamt stated that

> In the authority's assessment, Facebook's conduct represents above all a so-called exploitative abuse. Dominant companies may not use exploitative practices to the detriment of the opposite side of the market, i.e. in this case the consumers who use Facebook. This applies above all if the exploitative practice also impedes competitors that are not able to amass such a treasure trove of data. This approach based on competition law is not a new one, but corresponds to the case-law of the Federal Court of Justice under which not only excessive prices, but also inappropriate contractual terms and conditions constitute exploitative abuse (so-called exploitative business terms).

The Bundeskartellamt 's "decision covers different data sources:

(i) Facebook-owned services like WhatsApp and Instagram can continue to collect data. However, assigning the data to Facebook user accounts will only be possible subject to the users' voluntary consent. Where consent is not given, the data must remain with the respective service and cannot be processed in combination with Facebook data.
(ii) Collecting data from third party websites and assigning them to a Facebook user account will also only be possible if users give their voluntary consent."

The Bundeskartellamt stated that "[i]f consent is not given for data from Facebook-owned services and third party websites, Facebook will have to substantially restrict its collection and combining of data…[and] Facebook is to develop proposals for solutions to this effect."

Wyden and Rubio Press DHS on VPNs

Senators Ron Wyden (D-OR) and Marco Rubio (R-FL) urged the Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency Director Christopher Krebs in a letter to "conduct a threat assessment of the national security risks stemming from foreign virtual private network (VPN) apps" according to their press release. Wyden and Rubio stated that "[i]f DHS determines federal workers face security risks from foreign VPN apps…[then the agency should] issue a Binding Operational Directive banning their use on federal phones and computers." They stated that "[w]e are particularly concerned about the potential threat posed by foreign-made apps that are affiliated with countries of national security concern and urge you to examine the national security risk they pose." Wyden and Rubio stated that "[b]ecause these foreign apps transmit users' web-browsing data to servers located in or controlled by countries that have an interest in targeting U.S. government employees, their use raises the risk that user data will be surveilled by those foreign governments…[and] [t]he compromise of that data could harm U.S. national security."

Other Hearings and Events

Winning the Race to 5G and the Next Era of Technology Innovation in the United States–Senate Commerce, Science, and Transportation
Preserving an Open Internet for Consumers, Small Businesses, and Free Speech–House Energy and Commerce/Communications & Technology

Further Reading

Michael Kans, Esq. | mdk@michaelkanslaw.com | @michael_kans

Amazon's barely-transparent transparency report somehow gets more opaque –Tech Crunch
This Is How Much Fact-Checking Is Worth to Facebook – The Atlantic
UAE senior diplomat denies hacking Americans – Reuters
Huawei Sting Offers Rare Glimpse of the U.S. Targeting a Chinese Giant – Bloomberg Businessweek
DoD tightens enforcement of cyber regulations on contractors to protect data – Federal News Network
There's No Good Reason to Trust Blockchain Technology – Wired

Michael Kans, Esq. | mdk@michaelkanslaw.com | @michael_kans