Cyber Update
26 February 2019
By Michael Kans

Final UK Report on Facebook

Last week, the U.K.'s House of Commons' Digital, Culture, Media and Sport Committee released its final report on "Disinformation and 'fake news.'" The Committee further heard testimony and collected evidence relating to the "the spread of false, misleading, and persuasive content, and the ways in which malign players, whether automated or human, or both together, distort what is true in order to create influence, to intimidate, to make money, or to influence political elections." Specifically, the revelations about Facebook, Cambridge Analytica, and others' involvement in efforts to sway the outcome of the U.K.'s Brexit referendum and the 2016 U.S. presidential election spurred this Committee investigation. The Committee's revelations about Facebook may involve legislative responses in the U.K. and U.S. and possibly the Federal Trade Commission's (FTC) investigation of whether Facebook violated a 2012 settlement. The Committee released its interim report in July 2018.

The Committee explained that the final report:

> builds on the main issues highlighted in the seven areas covered in the Interim Report: the definition, role and legal liabilities of social media platforms; data misuse and targeting, based around the Facebook, Cambridge Analytica and Aggregate IQ (AIQ) allegations, including evidence from the documents we obtained from Six4Three about Facebook's knowledge of and participation in data-sharing; political campaigning; Russian influence in political campaigns; SCL influence in foreign elections; and digital literacy. We also incorporate analysis by the consultancy firm, 89up, of the repository data we received from Chris Vickery, in relation to the AIQ database.

The Committee stated that

> In this Final Report, we build on the principle-based recommendations made in the Interim Report. We look forward to hearing the Government's response to these recommendations within two months. We hope that this will be much more comprehensive, practical, and constructive than their response to the Interim Report, published in October 2018.

Among other recommendations and conclusions, the Committee called for:

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

- Social media companies cannot hide behind the claim of being merely a 'platform' and maintain that they have no responsibility themselves in regulating the content of their sites. We repeat the recommendation from our Interim Report that a new category of tech company is formulated, which tightens tech companies' liabilities, and which is not necessarily either a 'platform' or a 'publisher'. is approach would see the tech companies assume legal liability for content identified as harmful after it has been posted by users. We ask the Government to consider this new category of tech company in its forthcoming White Paper. (Paragraph 14)
- Our Interim Report recommended that clear legal liabilities should be established for tech companies to act against harmful or illegal content on their sites. ere is now an urgent need to establish independent regulation. We believe that a compulsory Code of Ethics should be established, overseen by an independent regulator, setting out what constitutes harmful content. e independent regulator would have statutory powers to monitor relevant tech companies; this would create a regulatory system for online content that is as effective as that for offline content industries. (Paragraph 37)
- We support the recommendation from the ICO that inferred data should be as protected under the law as personal information. Protections of privacy law should be extended beyond personal information to include models used to make inferences about an individual. We recommend that the Government studies the way in which the protections of privacy law can be expanded to include models that are used to make inferences about individuals, in particular during political campaigning. is will ensure that inferences about individuals are treated as importantly as individuals' personal information. (Paragraph 48)
- In our Interim Report, we recommended a levy should be placed on tech companies operating in the UK to support the enhanced work of the ICO. We reiterate this recommendation. e Chancellor's decision, in his 2018 Budget, to impose a new 2% digital services tax on UK revenues of big technology companies from April 2020, shows that the Government is open to the idea of a levy on tech companies. e Government's response to our Interim Report implied that it would not be financially supporting the ICO any further, contrary to our recommendation. We urge the Government to reassess this position.
- The Information Commissioner told the Committee that Facebook needs to significantly change its business model and its practices to maintain trust. From the documents we received from Six4Three, it is evident that Facebook intentionally and knowingly violated both data privacy and anti-competition laws. e ICO should carry out a detailed investigation into the practices of the Facebook Platform, its use of users' and users' friends' data, and the use of 'reciprocity' of the sharing of data.

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

Google Admits Home Security System Had Undisclosed Microphone

Last week, Google came under fire for not informing consumers that its product Nest Secure has a built-in microphone on Nest Guard, the system's alarm, keypad, and motion-sensor component. After *Business Insider* reported on the development, the company conceded it made an "error." However, some Members of Congress responded strongly and were critical of Google in particular and contextualized the news in a larger pattern of privacy abuses by the technology sector. These revelations, by themselves, are unlikely to spur Congressional action on legislation relating to privacy or the Internet of Things (IOT), but cumulatively this and other recent articles may keep focus and pressure on these issues.

In early February, Google announced in a blog posting that

> You can also arm your Nest Secure system using Assistant, but notably, it can't be *disarmed* using your voice. You'll still need the keycode or tag to do that. An update is rolling out today to enable Google Assistant on the Nest Guard component of your Nest Secure system.
>
> Starting today, we're adding a feature to Nest Secure to do just that: the Google Assistant will be available on your Nest Guard, so you can ask it questions like, "Hey Google, do I need an umbrella today?" before you set your alarm and leave the house. Nest Guard is the brains of your Nest Secure; it contains a keypad and all the smarts that power the system. It's usually placed in a spot with lots of traffic (like the front doorway) making it useful as you come and go.

The Members quoted by *Business Insider* linked Google's explanation and apology to other technology company's responses after similar incidents and even called for greater government oversight.

Senator Kamala Harris (D-CA) stated that "Americans shouldn't have to fear that the products in their home could be spying on them." She added that "[i]t's easier to ask for forgiveness than seek permission' or 'it's in the fine print' are not workable privacy policies…[b]ut they're ones that tech companies routinely fall back on."

Senator Mark Warner (D-VA), the Ranking Member of the Senate Intelligence Committee, said "[t]he standard talking point that consumers 'don't care about privacy' has been increasingly disproven, as we learn that consumers and policymakers have been kept in the dark for years about data collection and commercialization practices." He added that "[b]oth responsible federal agencies and the U.S. Congress must have hearings to shine a light on the dark underbelly of

the digital economy, including how incumbents are shaping the smart home ecosystem in potentially unfair and anti-competitive ways."

Senator Josh Hawley (R-MO) characterized the news "another classic screw up by another creepy tech company." He asserted that "[t]his time, Google is shamelessly surveilling customers with a secret microphone, used for who knows what - and here we are again with their asks for forgiveness after the fact." He said that "it's time for these tech giants to be held accountable."

Head of U.K. Cybersecurity Agency Proposes Different Path Than U.S. On Huawei

During his CyberSec speech in Brussels, the U.K.'s National Cyber Security Centre CEO Ciaran Martin spoke on the rollout of 5G and continued cooperation with European partners aside and part from Brexit. Martin's remarks touched on Huawei and the pending buildout of 5G, and some Trump Administration officials were hoping that the President would have signed a long rumored executive order banning Huawei from U.S. telecommunications networks. However, this did not come to pass.

Martin said

> Like many countries, including our five eyes partners, and partners here in Europe, the UK is looking at the right policy approach to 5G security. That policy process is being led by the Digital Department and its Secretary of State. It concludes its analysis in the spring. The government will then take decisions. As its public terms of reference make clear, it is a holistic review, taking account of economic, security, quality of service and other factors. It is considering a full range of policy options.

Martin said that "[e]verything is on the table…[and] [c]ontrary to some reporting no decisions have been taken and no decisions are being announced today."

Regarding Huawei, Martin stated that "Huawei's presence is subject to detailed, formal oversight, led by the NCSC." He said that "[b]ecause of our 15 years of dealings with the company and ten years of a formally agreed mitigation strategy which involves detailed provision of information, we have a wealth of understanding of the company." Martin explained that "[w]e also have strict controls for how Huawei is deployed…[i]t is not in any sensitive networks – including those of the government…[and] [i]ts kit is part of a balanced supply chain with other suppliers."

Separately, the NCSC's Technical Director Ian Levy said of Huawei that "[l]ast year we said we found some worrying engineering issues..[and] [a]s of today, we

have not seen a credible plan" to address the shortcomings turned up by the Huawei Cyber Security Evaluation Centre (HCSEC) Oversight Board last year.

CCPA Hearing

Last week, the California State Assembly's Privacy and Consumer Protection held a hearing titled "Understanding the Rights, Protections, and Obligations Established by the California Consumer Privacy Act of 2018: Where should California go from here?" This hearing is likely the beginning of another pass at perfecting a statute that has been criticized for some as being poorly drafted. The committee made available a video, an agenda, and a background memorandum.

Chairman Ed Chau (D-49) said the CCPA came about through the work and input of many stakeholders, which has been described as the most "comprehensive privacy rights law in the nation." He said the statute is based on the simple idea that people should be able to control their own data and not be discriminated against for exercising that right. Chau noted that the Assembly has turned to enforcement of the CCPA, and the Attorney General's (AG) office was provided an additional $700,000 to enforce the new statute. He said that passage of SB 1121 allowed for technical corrections and clarifications related to the financial services industry and newspapers and addressed concerns raised by the AG. However, he added that after conversations with businesses and privacy groups, "it is clear that our work is not done yet, and this hearing is being held in recognition of that fact." Chau said that law would be enforced while it is refined true to the intentions of the drafters.

The California Attorney General's Office (AG) has been holding listening sessions as a prelude to drafting the regulations necessary for implementation of the CCPA. Of course, the regulations were set to take effect on January 1, 2020 until the California legislature amended the statute and the deadline was pushed back until July 1, 2020 at latest or six months after the AG promulgates the required regulations. The AG has asked for written input by March 8 to PrivacyRegulations@doj.ca.gov "for consideration during this pre–rulemaking stage." The AG has also laid out a timeline for drafting regulations in the deck used at each public meeting. Additionally, the AG's Office identified the items in the CCPA about which regulations will be drafted:

(1) Categories of Personal Information
(2) Definition of Unique Identifiers
(3) Exceptions to CCPA
(4) Submitting and Complying with Requests
(5) Uniform Opt–Out Logo/Button
(6) Notices and Information to Consumer, including Financial Incentive Offerings
(7) Verification of Consumer's Request

In August 2018 when the California legislature was considering amendments to the CCPA, technology companies and affiliated stakeholders sent a letter to lawmakers regarding their preferred legislative fixes. In December 2018, consumers, privacy, and civil liberties groups listed their asks in a letter to Assembly and Senate members. More recently, in late January "the nation's leading advertising and marketing trade associations" sent the AG a letter detailing their concerns with implementation and enforcement of the CCPA.

Moreover, legislators have begun introducing bills to amend the CCPA and more are expected. In this vein, earlier this month, four Republican Members of the Assembly sent a letter to the House Energy and Commerce and the Senate Commerce, Science, and Transportation Committees that discusses, in part, their bill package, "Your Data, Your Way," that would "give consumers the absolute right to have their social media information deleted upon the closure of a social media account; prohibit smart-speaker manufacturers from storing and/or data mining voice recordings; mandate that social media companies receive verifiable consent from parents of potential users under 16; and mandate that potential data breach victims are notified within 72 hours of the company identifying the breach." The lawmakers suggested that the U.S. Congress should focus on antitrust legislation and enforcement instead of preempting California's privacy laws, the implication being that a federal standard would likely be weaker than the CCPA.

Finally, new Governor Gavin Newsom may have his own proposal on privacy and personal data he may seek to have enacted. In his February 12 State of the State Address, Newsom affirmed the need for the CCPA

> California is proud to be home to technology companies determined to change the world. But companies that make billions of dollars collecting, curating and monetizing our personal data have a duty to protect it. Consumers have a right to know and control how their data is being used. I applaud this legislature for passing the first-in-the-nation digital privacy law last year.

Newsom also then provided the barest of detail about his proposal, the "Data Dividend for Californians:"

> But California's consumers should also be able to share in the wealth that is created from their data. And so I've asked my team to develop a proposal for a new Data Dividend for Californians, because we recognize that your data has value and it belongs to you.

The Electronic Frontier Foundation responded to Newsom's proposal:

> Some observers have speculated that by "Data Dividend," Governor Newsom means payments by corporations directly to consumers in exchange for their personal information. We hope not. EFF strongly opposes "pay-for-privacy" schemes. Corporations should not be allowed to require a consumer to pay a premium, or waive a discount, in order to stop the corporation from vacuuming up—and profiting from—the consumer's personal information. It is not a good deal for consumers to get a handful of dollars from companies in exchange for surveillance capitalism remaining unchecked.

Groups Call on FTC To Investigate Facebook

On February 21, "privacy, technology, parent, and consumer advocacy organizations" asked the Federal Trade Commission (FTC) to "investigate whether Facebook has engaged in unfair or deceptive practices in violation of Section 5 of the Federal Trade Commission Act and the Children's Online Privacy Protection Act (COPPA)." The groups referred to a *Center for Investigative Reporting* report based on unsealed documents from a 2012 class action suit brought by parents against Facebook, alleging that the company intentionally induced and tricked children into making purchases through Facebook and then threw up numerous obstacles to getting refunds. Facebook settled with the plaintiffs in 2016.

In their letter, these groups claimed that

> The unsealed documents show that for years–at least as far back as 2010 and as recently as 2014–Facebook maintained a system that encouraged children to make unknowing and unauthorized credit card purchases for virtual items in games on Facebook's platform. After parents and minors repeatedly complained about the credit card charges, internal Facebook documents demonstrate the company refused to refund charges and set up a labyrinthine complaint system to deter refund requests. Internal documents also reveal that the company was aware that games on its platform were popular with children as young as five.

The groups pointed to previous FTC actions against other technology companies such as Apple, Google, and Amazon regarding these in-app purchases "when it was not clear when a purchase was being made and when parents were not given a choice whether to allow the minor child's purchases." These companies were required to change their billing practices and provide refunds. The groups also stated that "Facebook's practices also indicate a potential violation of COPPA, which the Federal Trade Commission should investigate…[and] [d]ocuments demonstrate that Facebook knew that certain games were highly popular with young children, some as young as five years old."

The signatories of the letter were:

- Common Sense Media
- Campaign for a Commercial-Free Childhood
- Center for Digital Democracy
- Badass Teachers Association, Inc.
- Children and Screens
- Consumer Action
- Consumer Federation of America
- Defending the Early Years
- Electronic Privacy Information Center
- Media Education Foundation
- New Dream
- Parent Coalition for Student Privacy
- Parents Television Council
- Peace Educators Allied for Children Everywhere (P.E.A.C.E.) Public Citizen
- Story of Stuff
- TRUCE (Teachers Resisting Unhealthy Childhood Entertainment)

Further Reading

"Cyber Incident Response and Resiliency in Cities" – New America
"As Concerns Over Facial Recognition Grow, Members Of Congress Are Considering Their Next Move" – BuzzFeed
"You Give Apps Sensitive Personal Information. Then They Tell Facebook." – Wall Street Journal
"Telecom industry to throw fundraiser for Senate chair the night before data privacy hearing" – The Hill
"Google will end a practice that prevents their workers from taking the company to court over workplace disputes" – recode
"California to close data breach notification loopholes under new law" –TechCrunch