Michael Kans' Technology Policy Update
27 June 2019
By Michael Kans, Esq.

FTC Investigating YouTube For COPPA Violations

According to multiple media reports, the Federal Trade Commission (FTC) may be close to levying large fines on Google's YouTube for violations of the "Children's Online Privacy Protection Act of 1998" (COPPA) (P.L. 105–277). Theoretically, the total could be billions of dollars as each violation of COPPA enables the FTC to wage a $41,484 fine. However, any such action against Google would likely also entail a settlement requiring Google to desist from certain activities and engage in others to ensure compliance with COPPA, which may mean a smaller fine in exchange for agreeing to comply in the future.

Word of this investigation comes amidst specific calls to revisit COPPA to tighten the language under which online platforms like YouTube operate and general calls for cracking down on privacy abuses by platforms collecting and sharing the personal information of Americans.

While the FTC has received complaints about YouTube since 2015, in April 2018, 23 consumer advocacy organizations filed a complaint with the FTC asking the agency "to take enforcement action against Google for violating children's privacy laws in operating the YouTube online video and advertising network services." These groups suggested that the FTC impose a fine of billions of dollars given Google's "particularly egregious" violations. The groups added

> Google has made substantial profits from the collection and use of personal data from children on YouTube. Its illegal collection has been going on for many years and involves tens of millions of U.S. children. The parties request that the FTC enjoin Google from committing further violations of the COPPA, impose effective means for monitoring compliance, and assess civil penalties that demonstrate that the FTC will not permit violations of COPPA.

In February, the FTC reached a $5.7 million settlement with Tik Tok over allegations that under its former name, Musical.ly, the company violated COPPA and the FTC's regulations promulgated to implement COPPA. This is the largest COPPA settlement ever. As explained on the FTC's website, Musical.ly "by collecting personal information from kids without parental consent." The FTC explained

> To register for the Musical.ly app, users provided their email address, phone number, full name, username, a profile picture, and a short bio. For the first three years, Musical.ly didn't ask for the user's age. Since July 2017, the company has asked about age and prevents people who say they're under 13 from creating accounts. But Musical.ly didn't go back and request age information for people who already had accounts.

Tik Tok will also need to meet compliance and recordkeeping reporting requirements for the next ten years.

There are some in Congress that would like to see the FTC receive additional authority under COPPA. One of COPPA's original cosponsors, Senator Ed Markey (D-MA), asserted "[a]n FTC

investigation into YouTube's treatment of children online is long overdue…[b]ut we must do much more to ensure that our children are protected from online dangers known and unknown." In March, Markey and Senator Josh Hawley (R-MO) introduced a bill to tighten the current COPPA standards, most notably by changing the knowledge necessary for an internet platform or game to violate the statute from actual knowledge to constructive knowledge. Additionally, the bill would require those currently covered under COPPA (i.e. those 13 years old and younger) to opt-in to the collection of their personal information and

In their press release, Hawley and Markey stated "[t]he legislation strengthens privacy protections specifically for children and minors by:

- Prohibiting internet companies from collecting personal and location information from anyone under 13 without parental consent and from anyone 13 to 15 years old without the user's consent;
- Banning targeted advertising directed at children;
- Digital Marketing Bill of Rights for Teens" that limits the collection of personal information of teens;
- Revising COPPA's "Actual knowledge" standard to a "constructive knowledge" standard for the definition of covered operators;
- Creating an "Eraser Button" for parents and children by requiring companies to permit users to eliminate publicly available personal information content when technologically feasible;
- Establishing a Youth Marketing and Privacy Division at the Federal Trade Commission (FTC);
- Prohibiting the sale of internet connected devices to children and minors unless they meet robust cyber security standards;
- Requiring manufacturers of connected devices to children and minors to prominently display on their packaging a privacy dashboard detailing how sensitive information is collected, transmitted, retained, used, and protected."

ICO Report on Ad Tech

The United Kingdom's (UK) data protection authority released its assessment of the real-time bidding (RTB) market for online advertising. The Information Commissioner's Office (ICO) stated "[w]hilst we accept that RTB is an innovative means of advertisement delivery, our view is that, in its current form, it presents a number of challenges to good data protection practices." The ICO explained that it has "been reviewing how personal data is used in real time bidding (RTB) in programmatic advertising, engaging with key stakeholders directly and via our fact-finding forum event to understand the views and concerns of those involved."

ICO stated that "[t]his update report therefore clarifies the ICO's views on adtech, specifically the use of personal data in RTB, and our intended next steps…[and] [t]he findings have come from our:

- research undertaken as part of our Technology Strategy;
- stakeholder engagement with industry;
- consideration of concerns we have received; and
- recent Fact Finding Forum (where participants from across the adtech industry met to discuss lawful basis, transparency and security challenges).

The ICO stated that "[w]hile many RTB market participants place some controls on their processing and sharing of personal data, it's become apparent during our work that there are substantially different levels of engagement and understanding of how data protection law applies, and the issues that arise." The ICO said that "[o]ur initial investigations raised a number of concerns with the

data protection practices within RTB." The ICO stated that "[f]or the purposes of this report we have prioritised the following areas:

- **Transparency and consent:** The protocols used in RTB include data fields that constitute special category data, which requires the explicit consent of the data subject. Furthermore, current practices remain problematic for the processing of personal data in general, even if the special category data were removed. For example:
    - identifying a lawful basis for the processing of personal data in RTB remains challenging, as the scenarios where legitimate interests could apply are limited, and methods of obtaining consent are often insufficient in respect of data protection law requirements;
    - the privacy notices provided to individuals lack clarity and do not give them full visibility of what happens to their data;
    - the scale of the creation and sharing of personal data profiles in RTB appears disproportionate, intrusive and unfair, particularly when in many cases data subjects are unaware that this processing is taking place; and
    - it is unclear whether RTB participants have fully established what data needs to be processed in order to achieve the intended outcome of targeted advertising to individuals. The complex nature of the ecosystem means that in our view participants are engaging with it without fully understanding the privacy and ethical issues involved.
- **Data supply chain**: In many cases there is a reliance on contractual agreements to protect how bid request data is shared, secured and deleted. This does not seem appropriate given the type of personal data sharing and the number of intermediaries involved.

The ICO explained that "[w]e intend to enhance our understanding by:

> **5.1 Targeted information-gathering activities.** Based on the need to further explore the data protection implications of RTB, we will undertake targeted information-gathering activities related to the data supply chain and profiling aspects, the controls in place, and the DPIAs undertaken. We will start this work in July 2019.
>
> **5.2 Engagement activities with key stakeholders.** We will also continue targeted engagement with key stakeholders. This autumn, we envisage holding an event, similar to the Fact-Finding Forum to continue dialogue and update stakeholders on developments. We will also continue bilateral engagement with IAB Europe and Google.
>
> **5.3 Cooperation with other Data Protection Authorities.** To date, complaints have been raised in at least seven European jurisdictions. We will continue to liaise and share information with our European colleagues.
>
> **5.4 Industry sweep.** Following continued engagement to obtain more information, we may undertake a further industry review in six months' time. The scope and nature of such an exercise will depend on our findings over the forthcoming months.

The ICO stated that "[i]n the meantime, we expect data controllers in the adtech industry to re-evaluate their approach to privacy notices, use of personal data, and the lawful bases they apply within the RTB ecosystem."

House Administration Election Security Markup

House Democrats are making another run at pressuring Senate Republicans to take up legislation to secure U.S. elections against interference. The Senate has declined to take up the "For The People Act of 2019" (H.R. 1), which included a process by which cybersecurity standards would be

established for election infrastructure vendors and would also authorize grants for states and localities to upgrade and secure their election systems. For example, "qualified election infrastructure vendors" must agree "to ensure that the election infrastructure will be developed and maintained in a manner that is consistent with the cybersecurity best practices issued by the Technical Guidelines Development Committee" and to promptly report cybersecurity incidents to the Department of Homeland Security (DHS) and the Election Assistance Commission (EAC).

The House Administration Committee marked up and reported out the "Securing America's Federal Elections (SAFE) Act of 2019" (H.R. 2722) at the end of last week. The committee adopted an amendment in the nature of a substitute and considered a handful of amendments. This bill could soon come to the House floor as House Democrats seem intent on making the security and safety of elections a part of their legislative program despite dim prospects in the Senate where Senate Majority Leader Mitch McConnell (R-KY) has said he will not being any such legislation to the floor.

The House Administration summarized H.R. 2722 in its press release:

- Require voting systems to use individual, durable, voter-verified paper ballots – a widely agreed upon reform to protect our elections from manipulation;
- Expand risk-limiting audits, equipping our states with the systems needed to ensure the accuracy of the vote tallies in an efficient manner;
- Authorize a $600 million Election Assistance Commission grant program to assist in securing election infrastructure, while providing states with $175 million in biannual sustainment funding to help maintain election infrastructure – this initial $600 million is being appropriated by the Financial Services and General Government Appropriations bill;
- Foster accountability for election technology vendors, creating a "qualified election infrastructure vendor" designation and much needed cyber security deadlines; and
- Implement cyber security safeguards to protect our systems from attack, including prohibition on wireless communications devises and a prohibition on election system internet connectivity.

Klobuchar and Murkowski Health Privacy Bill

This past week, Senators Amy Klobuchar (D-MN) and Lisa Murkowski (R-AK) introduced a bill, the "Protecting Personal Health Data Act" (S. 1842), that would address the privacy and security of health-related technology and testing that is outside the current regulatory regime with which most of the health care field comply. Should Congress take up broader privacy legislation, this targeted bill could possibly be included given that it addresses privacy in the health care space which has largely not been the focus of legislators when they discuss privacy issues.

Broadly speaking, this bill would require the Department of Health and Human Services (HHS) to "promulgate regulations to help strengthen privacy and security protections for consumers' personal health data that is collected, processed, analyzed, or used by consumer devices, services, applications, and software." Klobuchar and Murkowski observed in their press release that "[c]urrent laws such as the Health Insurance Portability and Accountability Act of 1996 were enacted by Congress when many of the wearable devices, apps, social media sites, and DNA testing companies collecting and sharing health data today did not exist."

Senate Homeland Markup of Two Bills

Last week, the Senate Homeland Security and Governmental Affairs Committee marked up and reported out a pair of cybersecurity-related bills: the "Internet of Things Cybersecurity Improvement Act of 2019" (S. 734) and the "State and Local Government Cybersecurity Act of 2019" (S. 1846).

As introduced, the "State and Local Government Cybersecurity Act of 2019" would:

- Provide the Department of Homeland Security (DHS) the authority "[t]o make grants to and enter into cooperative agreements or contracts with States, local governments, and other non-Federal entities as the Secretary determines necessary to carry out the responsibilities of the Secretary related to cybersecurity and infrastructure security under this Act and any other provision of law, including grants, cooperative agreements, and contracts that provide assistance and education related to cyber threat indicators, defensive measures and cybersecurity technologies, cybersecurity risks, incidents, analysis, and warnings."
- Direct the National Cybersecurity and Communications Integration Center (NCCIC) to work with "with Federal and non-Federal entities, such as the Multi-State Information Sharing and Analysis Center" on addressing a variety of cybersecurity-related responsibilities, including but not limited to
    - Conducting exercises;
    - Providing "operational and technical cybersecurity training;"
    - Sharing "cyber threat indicators, defensive measures, cybersecurity risks, and incidents from and to the Federal Government" with Federal and non-Federal entities;
    - Working "with senior Federal and non-Federal officials, including State and local Chief Information Officers, senior election officials, and through national associations" to quarterback national efforts "related to information security to secure and ensure the resiliency of Federal and non-Federal information systems and including election systems;" and
    - Making available "operational and technical assistance to Federal and non-Federal entities to implement tools, products, resources, policies, guidelines, controls, and procedures on information security, including by, as appropriate, deploying and sustaining cybersecurity technologies, such as an intrusion detection capability, to assist those Federal and non-Federal entities in detecting cybersecurity risks and incidents;
- Establish "a pilot program to deploy network sensors capable of utilizing classified indicators for the purpose of identifying and filtering malicious network traffic" within 180 days."

However, this bill was amended and the final bill text is not yet available.

The Committee's action on the bill to tighten the federal government's standards with respect to buying and using IoT comes a week after the House committee of jurisdiction marked up the companion bill. The Committee amended S. 734 twice before reporting the bill out, but the amendment language has not been made available and, one of the amendments was in the nature of a substitute sponsored by Chair Ron Johnson (R-WI). Nonetheless, one of the bill's sponsors, Senator Mark Warner (D-VA), issued a press release asserting "the Internet of Things (IoT) Cybersecurity Improvement Act of 2019 as passed out of Committee today would:

- Require the National Institute of Standards and Technology (NIST) to issue recommendations addressing, at a minimum, secure development, identity management, patching, and configuration management for IoT devices.

- Direct the Office of Management and Budget (OMB) to issue guidelines for each agency that are consistent with the NIST recommendations, and charge OMB with reviewing these policies at least every five years.
- Require any Internet-connected devices purchased by the federal government to comply with those recommendations.
- Direct NIST to work with cybersecurity researchers, industry experts, and the Department of Homeland Security (DHS) to publish guidance on coordinated vulnerability disclosure to ensure that vulnerabilities related to agency devices are addressed.
- Require contractors and vendors providing information systems to the U.S. government to adopt coordinated vulnerability disclosure policies, so that if a vulnerability is uncovered, that can be effectively shared with a vendor for remediation."

Last week, the House Oversight and Reform Committee marked up and reported out the "Internet of Things (IoT) Cybersecurity Improvement Act of 2019" (H.R. 1668) after adopting an amendment in the nature of a substitute that narrowed the scope of the bill and is more directive than the bill initially introduced in March.

Further Reading

"Iranian Hackers Launch a New US-Targeted Campaign as Tensions Mount" – *WIRED*
"Facebook usage falling after privacy scandals, data suggests" – *The Guardian*
"'Horns' are growing on young people's skulls. Phone use is to blame, research suggests." – *The Washington Post*
"FBI And DHS Blunders Reveal Names Of Child Abuse Victims Via Facebook IDs" – *Forbes*
"DHS to Move Biometric Data on Hundreds of Millions of People to Amazon Cloud" – *Nextgov*
"Goodbye, Chrome: Google's web browser has become spy software" – *The Washington Post*