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

U.S. Government Investigating Google and Amazon

A number of media outlets reported over the weekend that the U.S. Department of Justice (DOJ) and the Federal Trade Commission (FTC) will commence with investigations into the alleged antitrust activities of Google and Amazon. Most of the articles rely on the statements of three people with "knowledge" of the discussions but who are unauthorized to discuss the deliberations publicly, suggesting senior officials at DOJ and/or the FTC. The announcement comes at a time when the agencies are feeling more pressure from Capitol Hill on what are being called anti-competitive and anti-consumer policies of a number of large technology firms, including Facebook and others, from both the right and the left.

The DOJ and FTC have overlapping, interlocking authority to police antitrust and anti-competitive practices granted primarily under three statutes: the Sherman Act (15 U.S.C. §§ 1-7), the Clayton Act (15 U.S.C. §§ 12-27), and the FTC Act (15 U.S.C. §§ 41 et seq.). The agencies have traditionally divided markets based on expertise with the FTC specializing in these matters relating to "health care, pharmaceuticals, professional services, food, energy, and certain high-tech industries like computer technology and Internet services." The agencies often decide which one will tackle a possible antitrust or anti-competitive issue, and according to *Reuters*, DOJ's Antitrust Division and the FTC met a few weeks ago and decided that the former agency would look into Google and Apple while the latter agency would investigate Amazon and Facebook.

The DOJ is said to be interested in Google's practices in its digital advertising business and its Android operating system. However, the DOJ reportedly needed to consult with the FTC regarding the launch of an investigation given the latter agency's recent investigation of Google. During the Obama Administration, the FTC investigated Google and secured a commitment from the company to stop some practices but ultimately did not find evidence supporting an antitrust action.

The FTC announced in January 2013 that "Google Inc. has agreed to change some of its business practices to resolve FTC concerns that those practices could stifle competition in the markets for popular devices such as smart phones, tablets and gaming consoles, as well as the market for online search advertising." The FTC's outside counsel noted "regarding the specific allegations that the company biased its search results to hurt competition, the evidence collected to date did not justify legal action by the Commission…[and] [t]he evidence did not demonstrate that Google's actions in this area stifled competition in violation of U.S. law." The FTC explained:

> Under a settlement reached with the FTC, Google will meet its prior commitments to allow competitors access – on fair, reasonable, and non-discriminatory terms – to patents on critical standardized technologies needed to make popular devices such as smart phones, laptop and tablet computers, and gaming consoles. In a separate letter of commitment to the Commission, Google has agreed to give online advertisers more flexibility to simultaneously manage ad campaigns on Google's AdWords platform and on rival ad platforms; and to refrain from misappropriating online content from so-called "vertical" websites that focus on specific categories such as shopping or travel for use in its own vertical offerings.

Regarding Apple's possibly anti-competitive behavior, the European Commission (EC) is currently investigating a complaint filed by Spotify that the so-called "Apple-tax" is anti-competitive and violates the European Union's antitrust and anti-competition statutes and regulations. In a March 13 blog post, Spotify's CEO Daniel Ek explained that

> after careful consideration, Spotify has filed a complaint against Apple with the European Commission (EC), the regulatory body responsible for keeping competition fair and nondiscriminatory. In recent years, Apple has introduced rules to the App Store that purposely limit choice and stifle innovation at the expense of the user experience—essentially acting as both a player and referee to deliberately disadvantage other app developers. After trying unsuccessfully to resolve the issues directly with Apple, we're now requesting that the EC take action to ensure fair competition.

Ek added that

> Apple requires that Spotify and other digital services pay a 30% tax on purchases made through Apple's payment system, including upgrading from our Free to our Premium service. If we pay this tax, it would force us to artificially inflate the price of our Premium membership well above the price of Apple Music. And to keep our price competitive for our customers, that isn't something we can do.

In May, the EU's Competition Commissioner Margrethe Vestager said "[w]e are looking into that and we have been asking questions around in that market but of course also Apple themselves, for them to answer the allegations…[a]nd when they come back, we will know more."

Amazon's practices and policies have been subject to recent scrutiny. After a law review article was published on Amazon's third-party seller practices, in December 2018, Senator Richard Blumenthal (D-CT) wrote the FTC to express his "deep[] concern that the price parity provisions Amazon's contracts with third-party sellers could stifle market competition and artificially inflate prices on consumer goods that millions of Americans are planning to buy this holiday season." He urged the FTC to open an investigation into these provisions, and Amazon subsequently ended the practices in question. Nonetheless, the FTC will look more broadly into Amazon's business practices.

This will not be Facebook's first investigation by a federal regulator, however. The FTC has investigated and settled with Facebook regarding privacy practices that were deemed to be in violation of Section 5 of the FTC Act and is currently in talks to settle alleged violations of a consent decree. In February 2019, the *Washington Post* reported that the FTC and Facebook could be close to a settlement of the FTC's investigation of Facebook's interactions with Cambridge Analytica. The FTC is likely alleging that Facebook violated the 2012 settlement by allowing Cambridge Analytica access to its users' personal information beyond what these users agreed to share. In November 2011, the FTC and Facebook agreed on a draft consent order regarding the agency's allegations that Facebook violated Section 5 of the FTC Act through its privacy practices, and the FTC issued a final order in August 2012. The 20-year final order required Facebook "establish and implement, and thereafter maintain, a comprehensive privacy program that is reasonably designed to (1) address privacy risks related to the development and management of new and existing products and services for consumers, and (2) protect the privacy and confidentiality of covered information."

In February 2019, the FTC announced the "creation of a task force dedicated to monitoring competition in U.S. technology markets, investigating any potential anticompetitive conduct in those markets, and taking enforcement actions when warranted" modeled "the FTC's successful Merger Litigation Task Force, launched in 2002 by then-Bureau of Competition Director [and now FTC Chair] Joe Simons." The FTC added that "the Technology Task Force will, among other things, coordinate and consult with staff throughout the FTC on technology-related matters, including prospective merger reviews in the technology sector and reviews of consummated technology mergers."

The DOJ and FTC investigations will likely activate critics of the companies on Capitol Hill where Republicans have been critical of practices they claim are censoring conservatives on social media platforms while Democrats have been more focused on practices they decry as anti-competitive. Last week's Senate Judiciary Committee hearing into the digital advertising market and possible antitrust practices by the market's two dominant players, Google and Facebook, and these differing perspectives were in evidence.

The conduct of so-called "big tech" has bled into the presidential campaign, too. In March, Senator Elizabeth Warren (D-MA) proposed using anti-trust laws to break up large technology companies as part of her campaign to win the Democratic nomination for President. In her blog posting "Here's how we can break up Big Tech," Warren outlined her approach to addressing companies like Google, Amazon, Facebook, and others. Even if Warren does not secure the nomination, her proposals may quickly become the consensus position among most of the Democratic challengers, meaning that the Democratic Party might more fully align itself with those seeking to use anti-trust laws and enforcement to combat what they see as the excesses of the large technology firms.

Still No Senate Privacy Legislation

After months of assurances that a select bipartisan group of Senators on the Senate Commerce, Science, and Transportation Committee were progressing on the committee's privacy legislation, recent public comments suggest talks have stalled. Reportedly, Republicans and Democrats are split over whether a federal law would preempt laws like the "California Consumer Privacy Act" (A.B. 375) and if consumers would have a private right of action against companies. Generally, the Republicans favor preemption and oppose a right to sue, and the Democrats oppose preemption and support the right of consumers to file litigation. The working group includes the chair of the committee, Senator Roger Wicker (R-MS), the Senate Majority Whip John Thune (R-SD), the Manufacturing, Trade, and Consumer Protection Chair Jerry Moran (R-KS) and Ranking Member Richard Blumenthal (D-CT), and Senators Brian Schatz (D-HI) and Ed Markey (D-MA).

In mid-May, Moran claimed the working group would release a bill by the Memorial Day recess, but that date came and went without legislation. At the time, Moran conceded "there's a lot of words that remain to be determined." In late May, Thune remarked "[t]here's some not inconsequential issues that we have to work through, but I don't think that any of them is a deal breaker."

The House Energy and Commerce Committee is negotiating its own privacy bill, and it would not be surprising if both preemption and private rights of action also form fault lines in those talks. However, at some point, committee Democrats could decide that talking to the Republicans is not yielding fruit and could opt to work within the Democratic Caucus on a bill, thus cutting out Republicans. Another consideration is that Speaker of House Nancy Pelosi (D-CA) has said she will not support a bill that preempts the CCPA, which could bring other California Democrats in line with

this position and may complicate drafting and passage of privacy legislation, especially should a bill reach the Senate.

CCPA Advance Through Assembly; CCPA Bill Dies In Senate

The California Senate Appropriations Committee has essentially blocked further consideration of S.B. 561 for this legislative session. By being in the committee's Suspense File, the legislation cannot advance to the Senate floor and will therefore not be considered during this legislative session, disappointing those who wanted to see additional mechanisms and teeth in the "California Consumer Privacy Act" (A.B. 375) (CCPA) for consumers to sue entities that violate the CCPA. As you likely recall, SB 561 would eliminate the requirement that the California Department of Justice must furnish an opinion to a business or other entity with "guidance on how to comply with the provisions" of the CCPA. The legislation would also expand the private right of action available to California residents. The bill would allow consumers to sue if their rights under the CCPA are violated as opposed to the current statutory language limiting actions to "consumers whose nonencrypted or nonredacted personal information…is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business's violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information." Finally, the bill would remove the current 30-day window in which businesses alerted to CCPA violations can "cure" the noncompliance. Moreover, SB 561 would allow the Attorney General to sue for an injunction and civil penalties of $2,500 per violation or $7,500 per "intentional violation."

However, this month, the Assembly passed the following CCPA bills and sent them over to the California State Senate:

- **A.B. 25:** This bill would clarify the definition of consumer under the CCPA to exempt a person's personal information (PI) only to the extent that their PI is collected and used solely within their employee role, or in similar roles within the employment context, as specified. This bill would also reflect the Legislature's intent to ensure that a business complies with a consumer's request for specific pieces of information in a privacy protective manner, as specified.
- **A.B. 846:** This bill would replace the "financial incentive programs" provisions in the nondiscrimination statute of the CCPA with an authorization for offerings that include, among other things, gift cards or certificates, discounts, payments to consumers, or other benefits associated with a loyalty or rewards program, as specified.
- **A.B. 873:** This bill would narrow the definition of personal information (PI) in the CCPA to: (1) exclude information that "is capable of being associated with" a particular consumer; (2) exclude information that could be linked to particular "households"; and, (3) potentially exclude items that are otherwise listed as types of PI even if those items actually identify a particular consumer. This bill would also revise a provision of the CCPA prohibiting the act from being construed to require a business to reidentify or otherwise link information that is not maintained in a manner that would be considered PI. Lastly, this bill would replace the CCPA's current definition of "deidentified."
- **A.B. 874:** This bill would expand the "publicly available" information that is exempted from the definition of "personal information" (PI) in the CCPA to ensure that "publicly available" information includes any information that is lawfully made available from government records. This bill would also correct a drafting error in the definition of "PI" to clarify that PI does not include deidentified or aggregate consumer information.

- **A.B. 981:** This bill would exempt insurance institutions, agents, and support organizations (insurers) to which the Insurance Information and Privacy Protection Act (IIPPA) applies from the CCPA, except as specified. The bill would also, among other things, incorporate specific concepts from the CCPA into the IIPPA.
- **A.B. 1146:** This bill would establish an additional exemption from the CCPA for vehicle and ownership information shared pursuant to or in anticipation of a vehicle repair relating to warranty work or a recall conducted pursuant to federal law, except with respect to a consumer's right to access their personal information (PI), to know what PI has been collected or sold about them, and to bring a private right of action in the case of a data breach.
- **A.B. 1355:** This bill would address various drafting errors and make other clarifying changes in the California Consumer Privacy Act of 2018 (CCPA). Specifically, this bill would: 1) Correct a drafting error in the CCPA's definitions to specify that "personal information" (as opposed to "publicly available") does not include consumer information that has been deidentified or aggregate consumer information. 2) Address duplicative language in the CCPA relating to a consumer's right to know what personal information (PI) has been collected about them. 3) Clarify that consumers who are at least 13 years of age and less than 16 years of age (as opposed to "between 13 and 16 years of age") have the right to opt-in to the sale of their PI. 4) Align various requirements throughout the CCPA, such as with respect to the information that must be disclosed about the categories of third parties to which a business has sold PI, as specified. 5) Correct various cross-references and include missing cross-references to appropriate CCPA provisions. 6) Correct various drafting errors and make other clarifying or technical, non-substantive changes.
- **A.B. 1564:** This bill would revise a requirement in the CCPA for businesses to make available to consumers "two or more designated methods" for submitting requests for information to be disclosed pursuant to specified provisions of the CCPA, including, at a minimum, a toll-free telephone number and, if the business maintains an internet website, a website address. Instead, this bill would require that businesses: (1) make available to consumers either a toll-free telephone number or an email address; and, (2) if the business maintains an internet website, make an internet website available to consumers to submit requests for information required to be disclosed pursuant to specified provisions of the CCPA. This bill would make other technical, non-substantive changes.
- **A.B. 1202:** This bill "would require data brokers to register with the Attorney General (AG), and would additionally require the AG to create a publicly available registry of data brokers on its website, and would grant enforcement authority for violations of these requirements to the AG."
- **A.B. 1416:** This bill would do the following:

  1) Specifies that the obligations imposed on businesses by the CCPA shall not restrict a business's ability to comply with any rules or regulations adopted pursuant to and in furtherance of state or federal laws.

  2) Provides that the obligations imposed on businesses by the CCPA shall not restrict a business's ability to provide a consumer's personal information (PI) to a government agency solely for the purposes of carrying out a government program, including providing government services in furtherance of a government program, provided that certain requirements are met.

  3) Provides that the obligations imposed on businesses by the CCPA shall not restrict a business's ability to sell the PI of a consumer who has opted-out of the sale of the consumer's PI to another person for the sole purpose of detecting security incidents, protecting against malicious, deceptive, fraudulent, or illegal activity, and

> prosecuting those responsible for that activity, provided that the business and the person shall not further sell that information for any other purpose.

Case Made Against GCHQ Encryption Proposal

Late last month, "an international coalition of civil1society organizations dedicated to protecting civil liberties, human rights, and innovation online; security researchers with expertise in encryption and computer science; and technology companies and trade associations" sent an open letter to the United Kingdom's Government Communications Headquarters (GCHQ) regarding the agency's proposal that one way to solve the problem posed by criminal and terrorists using end-to-end encrypted apps is to add law enforcement as a silent participant to these chats. In the letter, these groups argued that "this particular proposal poses serious threats to cybersecurity and fundamental human rights including privacy and free expression."

In a *Lawfare* piece, the GCHQ asserted

> In a world of encrypted services, a potential solution could be to go back a few decades. It's relatively easy for a service provider to silently add a law enforcement participant to a group chat or call. The service provider usually controls the identity system and so really decides who's who and which devices are involved - they're usually involved in introducing the parties to a chat or call. You end up with everything still being end-to-end encrypted, but there's an extra 'end' on this particular communication. This sort of solution seems to be no more intrusive than the virtual crocodile clips that our democratically elected representatives and judiciary authorise today in traditional voice intercept solutions and certainly doesn't give any government power they shouldn't have.

The GCHQ stressed that "[w]e're **not** talking about weakening encryption or defeating the end-to-end nature of the service." The agency stated that "[i]n a solution like this, we're normally talking about suppressing a notification on a target's device, and **only** on the device of the target and possibly those they communicate with…[and] [t]hat's a very different proposition to discuss and you don't even have to touch the encryption."

The groups stated

> The "ghost key" proposal put forward by GCHQ would enable a third party to see the plain text of an encrypted conversation without notifying the participants. But to achieve this result, their proposal requires two changes to systems that would seriously undermine user security and trust. First, it would require service providers to surreptitiously inject a new public key into a conversation in response to a government demand. This would turn a two-way conversation into a group chat where the government is the additional participant, or add a secret government participant to an existing group chat. Second, in order to ensure the government is added to the conversation in secret, GCHQ's proposal would require messaging apps, service providers, and operating systems to change their software so that it would 1) change the encryption schemes used, and/or 2) mislead users by suppressing the notifications that routinely appear when a new communicant joins a chat.

Nonetheless, the groups stated "[t]he six principles set forth by GCHQ officials are an important step in the right direction, and highlight the importance of protecting privacy rights, cybersecurity, public confidence, and transparency." They stated that "[w]e especially appreciate the principles'

recognition that governments should not expect 'unfettered access' to user data, that the 'trust relationship' between service providers and users must be protected, and that 'transparency is essential.'"

Further Reading

"In Baltimore and Beyond, a Stolen N.S.A. Tool Wreaks Havoc" – *The New York Times*
"Britain may not have made final decision on Huawei and 5G: Bolton says" – *Reuters*
"New York could soon pass its own GDPR-inspired data security law" – *cyberscoop*
"Trump Wants to Wall Off Huawei, but the Digital World Bridles at Barriers" – *The New York Times*
"It's the middle of the night. Do you know who your iPhone is talking to?" – *The Washington Post*
"Spies with that? Police can snoop on McDonald's and Westfield wifi customers" – *Guardian*
"Some federal prosecutors disagreed with decision to charge Assange under Espionage Act" – *The Washington Post*
"The Pentagon has its own island off New York where nobody can go that it's using to run war games for a giant cyber attack on power grid" – *Business Insider*