# Michael Kans' Technology Policy Update
# 29 May 2019
# By Michael Kans, Esq.

**Oversight and Reform Hearing on Facial Recognition**

The House Oversight and Reform Committee held a hearing titled "Facial Recognition Technology (Part 1): Its Impact on our Civil Rights and Liberties" "examining the use of facial recognition technology by government and commercial entities and the need for oversight on how this technology is used on civilians" according to the committee's background memorandum. There was bipartisan agreement that Congress and the federal government needs to more tightly regulate the use of facial recognition technology by federal and state law enforcement agencies and the private sector. The chair of the committee laid out his plans for the committee to consider the issues presented by this technology over a series of hearings and then formulate its response. However, the area of consensus regarding the harms of using facial recognition technology centers on the use against people on the left and right exercising their First Amendment rights of free speech and assembly whereas committee Democrats also articulated their concerns about the use of this technology in ways that violate a person's rights under the Fourth Amendment against unreasonable searches and seizures.

The committee heard from the following witnesses:

- National Organization of Black Law Enforcement Executives former President Dr. Cedric Alexander
- Algorithmic Justice League Founder Joy Buolamwini
- The University of the District of Columbia's David A. Clarke School of Law Professor Andrew G. Ferguson
- Georgetown University Law Center's Center on Privacy & Technology Senior Associate Clare Garvie
- American Civil Liberties Union Senior Legislative Counsel Neema Singh Guliani

Chair Elijah Cummings (D-MD) remarked that this is the first hearing in this Congress on facial recognition technology. He said that the committee is uniquely situated to examine the issue as it has cross-cutting jurisdiction over the federal government and state and local governments. Cummings stressed that this is a bipartisan issue both to conservatives and liberals alike as to when they being monitored, why they are being monitored, who is monitoring them, and what happens to this information. Cummings thanked Ranking Member Jim Jordan (R-OH) for his input and cooperation. He acknowledged that facial recognition holds potential, but he added that in 2016 the Government Accountability Office (GAO) recommended that the Federal Bureau of Investigation (FBI) make numerous changes to its facial recognition database to improve data security and accuracy, privacy, and transparency. Cummings noted last month's GAO letter highlighting six priority recommendations the FBI has yet to implement. He said that at the local level cities like Detroit and Chicago are rapidly expanding the use of facial recognition technology that tracks citizens in real time. He said at the same time, cities like San Francisco are banning the use of facial recognition technology altogether. Cummings asserted that private companies are using this technology for advertising, security, and a variety of customer experiences. He emphasized that there are virtually no controls on where this information goes. He stated in 2017 the committee held a hearing to review law enforcement's use of facial recognition technology and

discovered that 18 states have memoranda of understanding with the FBI to share their databases. Cummings stated that, as a result, more than half of America adults are in a facial recognition database and likely do not know it. He said that facial recognition technology misidentifies women and minorities at a much higher rate than males, increasing the risk of racial and gender bias. Cummings said that Baltimore City Police had used facial recognition technology to fine and arrest the protestors of Freddy Graves death even though these citizens were using their rights under the Constitution. He declared that Congress must do more to safeguard the rights to free speech and assembly under the First Amendment, the right to privacy under the Fourth Amendment, and the right to equal protection under the law under the Fourteenth Amendment. Cummings said the committee would be conducting further hearings with an eye towards generating concrete recommendations for legislation or other action to address the issues turned up.

Ranking Member Jim Jordan (R-OH) characterized the hearing as critical and said that Congressional oversight is of paramount importance. He stated that the committee has a history of bipartisan work on civil liberties and privacy rights. Jordan recalled a hearing a few years earlier on stingray technology and said the threats to civil liberties posed by that technology is "scary." Jordan added that the Internal Revenue Service (IRS) was involved in the use of stingrays, the same agency "that targeted people for their political beliefs." He said technology that allows for facial recognition in real time is troublesome and the stuff of George Orwell's 1984. Jordan remarked that the unregulated nature of facial recognition technology needs to change.

Buolamwini said she wanted to make five key points:

- First, facial recognition technology is expanding rapidly, with little to no formal oversight.
- Second, this is occurring even though the threat of face surveillance puts civil liberties at risk, in particular endangering traditionally marginalized and vulnerable populations.
- Third, failures of a broad set of facial analysis technologies including facial recognition technology have real and dire consequences for people's lives, including in critical are as such as law enforcement, housing, employment, and access to government services.
- Fourth, the development and evaluation of these technologies raise an additional set of privacy and fairness concerns.
- Fifth and finally, given what we already know about the critical flaws of facial analysis technology, along with its rapid advancement and adoption across the country, Congress should enact a moratorium that halts law enforcement adoption of this technology unless and until appropriate regulatory mechanisms are put in place.

Ferguson asserted that "Congress should act to regulate new facial recognition surveillance technologies, because the case-by-case, slow process of Fourth Amendment litigation is inadequate to address the rapidly changing world of mass surveillance." He stated that "I will be making five main point:

- First, the Fourth Amendment will not save us from the privacy threat posed by facial recognition technology. The Supreme Court is making solid strides in trying to update Fourth Amendment principles in the face of new technology, but they are chasing an accelerating train and will not catch up. Legislation is needed to respond to the real-time threats of real-time technology.
- Second, the Fourth Amendment was never meant to be the sole source of government regulation. Instead, our entire constitutional system is premised upon Congress taking a leading role, guided by—and only in the rare instance overruled by—our founding Constitution.

- Third, the few steps the Supreme Court has made on the subject of locational tracking technologies offer guidance on how to avoid drafting a law that could get struck down on Fourth Amendment grounds.
- Fourth, as Congress builds a scaffolding off that constitutional floor, we need to think about the technology not just though the lens of today, but with an eye toward the expansion of surveillance technologies that will combine, aggregate, link, and share data in ways that will reshape the existing power dynamics of government and the people.
- Finally, these Fourth Amendment questions must be coupled with a focus on First Amendment freedoms, civil rights, and fundamental fairness when it comes to public safety protections. The burden of surveillance technology has never been equally shared across socio-economic or racial groups. Surveillance is both a civil rights issue and a civil liberties issue and Congress needs to regulate with racial justice in mind.

Garvie contended that "[b]y giving police the capability to identify individuals in real-time or reconstruct their every movement from photos or videos, face recognition can create a near constant surveillance state that threatens our core constitutional values." She stated that "[a]lready, many existing uses of the technology violate the Fourth Amendment…[and] [t]hese harms fall disproportionately on communities of color and immigrant communities, who are already overpoliced and more likely to be stopped, arrested, or have force wrongly used against them." Garvie stated that "the ACLU urges the Committee to:

> 1) Take steps to halt the use of face recognition for law enforcement and immigration enforcement purposes until Congress passes a law dictating what, if any, uses are permissible and ensures that individuals' rights can be protected;
> 2) Fully utilize its oversight powers to make public information regarding how federal agencies, including the FBI and ICE, are using face recognition; whether they are complying with their constitutional notice obligations; what policies are in place to prevent rights abuses; and whether their systems are accurate; and
> 3) Investigate companies, like Amazon and Microsoft, that sell face recognition for law enforcement use and without taking adequate responsibility or enforcing sufficient safeguards to prevent abuse.

**Senate Digital Advertising**

The Senate Judiciary Committee held its fourth technology and policy hearing over the last few months as the committee continues its survey of the issues posed by the internet, social media, and other facets of 21st Century communication. In last week's hearing, the committee examined the digital advertising market, which a report earlier this year showed had surpassed "traditional" advertising markets in terms of cumulative revenues.

Last June, the House Energy and Commerce Committee's Digital Commerce and Consumer Protection Subcommittee also looked into the issue at a hearing. The Republican staff memorandum explained

> According to the consultancy PwC, "[o]ver the past 21 years the Internet has grown from a nascent industry to the largest ad supported media in the United States." During this period, the digital advertising ecosystem has continually redefined and disrupted online content and media businesses, as advertising delivered over the Internet continues to grow in influence and impact.

During that hearing, Members and witnesses discussed privacy concerns, possible fraudulent activity, bots, fake accounts, "fake news," antitrust considerations, and discrimination in employment, housing, and commerce.

The witnesses before the committee were:

- University of Toronto Professor Avi Goldfarb
- Yale Professor Dr. Fiona M. Scott Morton, Ph.D.
- AppNexus Inc. Founder and Former CEO Brian O'Kelley
- Brave Chief Policy & Industry Relations Officer Dr. Johnny Ryan, Ph.D.
- Freshfields Bruckhaus Deringer LLP Counsel Jan M. Rybnicek

Chair Lindsey Graham (R-SC) said the committee would hear testimony about digital advertising, privacy, competition and how privacy legislation could affect those issues. He noted the committee has "some jurisdiction" over these issues and expressed his hope that the committees of jurisdiction would work together on "bills related to privacy so the consumer knows what they're getting in for, how to take down content, what to take down, what to leave up, [and] make sure we harden this infrastructure against foreign involvement."

Senator Patrick Leahy (D-VT) said everyone knows every business has to monetize its prodcuts and services but there has been a perception among Americans that the internet provided free content. He asserted consumers now realize the currency of the internet is the personal information and data of consumers, and it turns out these data can be very valuable. Leahy claimed intenet companies know everything we purchase, collect information about our health and medical conditions, know the routes we travel to work and school, can replicate fingerprints and faceprints, are entrusted with Americans' most private communications with friends and families, and hold private photographs in the cloud. He explained that this information is not merely held by these companies but rather sold and resold to third party data brokers without the consumer's knowledge. Leahy said these data can be sued to build a comprehensive digital profile on everyone. He stated that digital advertising plays a key role in these issues and practices and if a company can monopolize these data, there will be profound impacts on competition, too. Leahy declared his approach to protecting the privacy of American is simple: when consumers trust their most sensitive personal information to corporations, these companies must be required to obtain their consent in a clear, easily understood manner about how data is collected and used and to keep their information safe and to allow consumers ownership of their own data. He added that companies would be required "to do the right thing" by promptly notifying and remedying breaches immediately instead months after the fact as some companies have done. Leahy claimed the federal government is "way behind the curve when it comes to this issue" and it takes time to effect changes. He noted his introduction of versions of the "Consumer Privacy Protection Act" over the last fifteen years that would set baseline data security standards. He said that in the absence of federal action, states have passed laws such as the "California Consumer Privacy Act" (A.B. 375) and a law in Vermont to transform how data brokers can operate. Leahy said he understands and appreciates technology companies' interest in a single, national privacy standard, but he said he would oppose any statute that would impose a low privacy ceiling on states serving more to blunt the impact of state privacy laws instead of guarding the privacy rights of all Americans. Leahy emphasized that all Americans should enjoy strong privacy protection and legislators should be mindful of the competition facet to these issues as the playing field should be level for new startups and technology. He added that the issue of privacy is foremost Constitutional in nature, making it all the more important that privacy rights are secured.

Goldfarb said his testimony would "focus on the interaction between privacy, competition, and innovation…[and] will emphasize four points:

- There are often trade-offs between privacy regulation and innovation. Data is a key input into innovation, especially for dynamic sectors in the economy. However, privacy regulation restricts the use of data and may reduce the dynamism of these sectors.
- There are often trade-offs between privacy regulation and competition. Large established companies have the resources to comply with regulation. In addition, they already have access to the data needed to improve their products. This means that regulation can disadvantage startups and smaller companies.
- Consumers value privacy. A growing body of research indicates that consumers value privacy in a variety of contexts. Therefore, costs related to reduced innovation and competition should be weighed against real benefits.
- It is possible to mitigate many of the negative consequences of privacy regulations on both competition and innovation. For example, data portability can help startups and smaller firms innovate and compete, and regulatory consistency can reduce the resources needed to ensure compliance.

Morton noted that "[w]hile some markets may self-correct, the findings of this report suggest that rapid self-correction in markets dominated by large digital platforms is unlikely." She said that "[w]hile US antitrust law has long been flexible in combatting anticompetitive conduct, there is increasing concern that it has been underenforced in recent years." Morton stated that "[a]ntitrust enforcement better suited to the challenges of the Digital Age may therefore require new legislation…[and] [t]echnology platforms present particular challenges for antitrust enforcement." She explained that "[m]arkets tip and the resulting market power is durable, so even effective antitrust enforcement is unlikely to generate fragmented markets." She contended that "[n]onetheless, enforcement that protects competition on the merits in the first stage and prevents exclusionary conduct in the second stage will help ensure that market-participants make unfettered choices among competing platforms and that entry and innovation are not inhibited by private rent-seeking." Morton stated that "the report suggests that Congress should consider creating a specialist regulator, the Digital Authority…[that] could be tasked with creating general conditions conducive to competition."

O'Kelley stated that "[a]s an entrepreneur, I am hesitant to ask the government to split up Facebook or Google." He conceded that "[t]hese are incredible companies that have done much good for consumers, employees, and communities." O'Kelley stated that "[a]t the same time, we must ask ourselves whether having the internet concentrated in the hands of a few companies is good for America." He proposed "three actions to ensure that consumers have choice, and thus agency, in the internet economy:

1. Create a consumer bill of data rights that lays out first principles to ensure transparency, control, and portability of data.
2. Create a regulatory entity to enforce these principles as the internet continues to evolve.
3. Close the anti-trust advertising exception and either break up the internet giants or force them to treat their component parts at arms-length.

**Election Security Hearing**

Another House committee that shares jurisdiction over federal, state, and local election security held a hearing on the issues posed by Russian interference and influence in the 2016 election at a time when election security legislation is stalled. At the "Securing U.S. Election Infrastructure and

Protecting Political Discourse" hearing, the House Oversight and Reform Committee's National Security Subcommittee heard from witnesses from the federal government charged with securing elections and election infrastructure and private sector stakeholders:

- Panel 1
  - Cybersecurity and Infrastructure Security Agency Director Christopher Krebs
  - Deputy U.S. Assistant Attorney General Adam Hickey
  - U.S. Election Assistance Commission Chair Christy McCormick
  - U.S. Federal Election Commission Commissioner Ellen L. Weintraub
- Panel 2
  - Secretary of the Commonwealth of Massachusetts Bill Galvin
  - Google Director of Law Enforcement and Information Security Richard Salgado
  - Facebook Head of Cybersecurity Policy Nathaniel Gleicher
  - Twitter Public Policy Manager Kevin Kane

Chair Stephen Lynch (D-MA) said the hearing would examine the security of the nation's election infrastructure systems as well as how well the federal government is working with private sector partners to respond to "malicious attempts to unduly influence public opinion, sow discord, and undermine confidence in our political institutions. He stressed that the hearing's purpose is not to relitigate the outcome of the 2016 presidential election. Lynch said that the goal is safeguard the fundamental political principles underscored by President Abraham Lincoln when he said "elections belong to the people." He emphasized that the integrity of U.S. democracy is now at stake. Lynch noted the January 2017 Intelligence Community (IC) assessment that the democracy of the United States had been subject to attack by foreign adversaries that also found with "high confidence" that Russian President Vladimir Putin ordered an influence campaign in 2016 aimed at the U.S. presidential elections. He said Russian efforts included clandestine efforts along with "blatant meddling" by Russian government agencies, state-sponsored media, paid intermediaries, and trolls. He said Special Counsel Robert Mueller's report confirmed and augmented the IC's high confidence judgement. Lynch said some of the methods included fake social media accounts, the purchase of online political advertisements, and the deployment of automated bots to amplify content and fuel the organization of political rallies in the U.S. He explained that a Russian military agency, the GRU, perpetrated a hacking operation targeting U.S. individuals, political committees, state election boards, state secretaries of state, county governments, and private manufacturers of election related software and voting machines. Lynch noted the indictment of Russian hackers and companies and Facebook's post-election assessment that Russian's Internet Research Agency may have reached more than 126 million people prior to its account being deactivated. He asserted that Russian interference in elections has continued with China, Iran, and other hostile states following suit and that the IC has warned that malign foreign influence will continue and will evolve in the 2020 presidential election cycle. Lynch said the nonpartisan Brookings Institute predicted that artificial intelligence (AI) will be employed in the next election cycle. He called for a "frank and bipartisan assessment of the vulnerabilities that remain in our electoral process."

Ranking Member Jody Hice (R-GA) said voting is a bedrock for the republic grounded in federalism and is a fundamental Americans take pride in. He said that it is imperative that election systems are secure that Americans can have full confidence their votes are heard on election day. Hice said the hearing is about protecting election systems but also how to protect political discourse on social media platforms like Facebook, Twitter, and YouTube. He said the federal agencies represented at the hearing help state and local officials ultimately responsible for administering elections. He noted in January 2017 in order to reduce cyber and physical risks to state and local election systems, the Department of Homeland Security (DHS) designated election systems as a critical piece

of U.S. infrastructure, allowing state and local officials to receive a wide range of services to address cyber and physical risks to their facilities. He added that the FY 2018 omnibus appropriations act provided $380 million to the Election Assistance Commission (EAC) to disburse to states. Hice said that the hearing's second panel had representatives from Facebook, Twitter, and Google, the social media platforms that make up much of the territory in which Americans engage in political discourse. He called for full transparency by these companies and should "advance the freedom of speech and not censor it." Hice said that some accounts are nonetheless banned, and he expressed his interest in determining why bans are instituted. He added that platforms should also better secure their systems against foreign adversaries that will likely challenge the validity of the U.S. election system. Hice emphasized there is a clear distinction between content from foreign adversaries and content with which people disagree.

Krebs said that "[s]ince 2016, DHS's Cybersecurity and Infrastructure Security Agency (CISA) has led a voluntary partnership of Federal Government and election officials who regularly share cybersecurity risk information." He stated that "CISA has engaged directly with election officials—coordinating requests for assistance, risk mitigation, information sharing, and incident response…[and] [t]o ensure a coordinated approach, CISA convened stakeholders from across the Federal Government through the Election Task Force." Krebs stated that "[d]uring the 2018 midterms, CISA provided a coordinated response from DHS and its federal partners to plan for, prepare for, and mitigate risk to election infrastructure." He said that "[w]orking with election infrastructure stakeholders was essential to ensuring a more secure election." Krebs stated that "CISA and our stakeholders increased awareness of potential vulnerabilities and provided capabilities to enhance the security of U.S. election infrastructure as well as that of our democratic allies." He said that "DHS goals for the 2020 election cycle include improving the efficiency and effectiveness of election audits, continue to incentivize the patching of election systems, and working with the National Institute of Standards and Technology (NIST) and the states to develop cybersecurity profiles utilizing the NIST Cybersecurity Framework for Improving Critical Infrastructure." Krebs stated that "[w]e will also continue to engage any political entity that wants our help. DHS offers these entities the same tools and resources that we offer to state and local election officials, including trainings, cyber hygiene support, information sharing, and other resources."

Hickey noted the Department of Justice's (DOJ) "recently drafted an analysis of the types of foreign influences that can target democratic and electoral processes as well as the Department's responses to counter them…included in the first chapter of the Report of the Attorney General's Cyber-Digital Task Force, released last summer:

> 1. Cyber operations targeting election infrastructure. Such operations could seek to undermine the integrity or availability of election-related data. For example, adversaries could employ cyber-enabled or other means to target election infrastructure, such as voter registration databases and voting machines. Operations aimed at removing otherwise eligible voters from the rolls or attempting to manipulate the results of an election (or even just disinformation suggesting that such manipulation has occurred) could undermine the integrity and legitimacy of elections, as well as public confidence in election results. To our knowledge, no foreign government has succeeded in perpetrating ballot fraud,8 but raising even the doubt that it has occurred could be damaging.
> 2. Cyber operations targeting political organizations, campaigns, and public officials. These operations could seek to compromise the confidentiality of private information of the targeted groups or individuals, as well as its integrity. For example, adversaries could conduct cyber or other operations against U.S. political organizations and campaigns to

steal confidential information and use that information, or alterations thereof, to discredit or embarrass candidates, undermine political organizations, or impugn the integrity of public officials.

3. Covert influence operations to assist or harm political organizations, campaigns, and public officials. For example, adversaries could conduct covert influence operations to provide assistance that is prohibited from foreign sources to political organizations, campaigns, and government officials. These intelligence operations might involve covert offers of financial, logistical, or other campaign support to, or covert attempts to influence the policies or positions of, unwitting politicians, party leaders, campaign officials, or even the public.

4. Covert influence operations, including disinformation operations, to influence public opinion and sow division. Using false U.S. personas, adversaries could covertly create and operate social media pages and other forums designed to attract U.S. audiences and spread disinformation or divisive messages. These messages need not relate directly to campaigns. They may seek to depress voter turnout among particular groups, encourage third-party voting, or convince the public of widespread voter fraud in order to undermine confidence in election results.

5. Overt influence efforts, such as the use of foreign media outlets or other organizations to influence policymakers and the public. For example, adversaries could use state-owned or state-influenced media outlets to reach U.S. policymakers or the public. Governments can disguise these outlets as independent, while using them to promote divisive narratives and political objectives.

Weintraub said that

> Even fully disclosed money spent by U.S. corporations with foreign parents raises concerns about foreign influence. When a U.S.-based company is owned by foreigners, the U.S. managers are obliged to spend company resources in a way that best serves the interests of the foreign owners, not the American people. I have proposed rulemakings that would address these concerns, but these efforts have so far been blocked at the FEC. Even my proposal to address spending in our elections by companies that are wholly owned by foreign governments was rejected. Until we address, by statute or regulation, the various ways that foreigners may route money through corporate entities, our political system remains at risk of being influenced by foreign corporate or governmental interests. The idea behind regulating foreign-owned entities is not novel.

Weintraub added

> Congress and the FEC must respond to foreign disinformation campaigns that have proliferated online. For my agency to do so, the FEC needs better tools from Congress so that we can get a handle on the advertising dollars that are pouring into the social-media networks. Online political manipulation can take many forms: disinformation, political botnets, fake social media accounts, troll farms, and paid digital advertising. I have written about these dangers before, and while today's cybersecurity threats are complex problems requiring a multifaceted response, one easy place to start is with more robust disclosure requirements for online political advertising. At a minimum, digital advertising should be subject to the same disclosure and disclaimer requirements as broadcast advertising. The Honest Ads Act would be a very good first step.

> In addition to more robust advertising disclosure requirements, we must consider cybersecurity countermeasures for political campaigns. Campaign cybersecurity is essential, but efforts to put these in place are in their early stages and face significant hurdles. In the wake of campaign-related cyber-attacks that have targeted Democratic and Republican campaigns alike, security companies, technology companies, and nonprofits have considered offering free or discounted cybersecurity products and services to political campaigns. These offers pose complications for political campaigns, however, because campaign finance regulations prohibit corporations from donating directly to campaigns. This prohibition applies to in-kind contributions such as free or discounted cybersecurity services. The Commission is currently considering whether to allow a nonprofit to provide free or discounted cybersecurity services. It is a proposal that I am seriously considering approving through a tailored advisory opinion, but this is a problem that would benefit from a legislative solution. I am also proposing an interpretive rule that would allow national party committees to use their building funds to pay for cybersecurity expenses for themselves, state parties, and candidates.

**FEC Allows Use of Campaign Funds For Cybersecurity Measures**

Last week, the Federal Election Commission (FEC) took two actions to help federal political campaigns install and maintain better cybersecurity in light of the interference in the 2016 election and the continued threat posed by cyber-attacks.

The FEC issued a "notice of interpretive rule" "issuing guidance on the payment by national party committees for secure information communications technology and cybersecurity products or services for national and state party committees and federal candidate committees by using funds from party segregated accounts for headquarters buildings" "[t]o serve the compelling governmental interest in preventing foreign interference in United States elections." The FEC stated that "[a]s with other disbursements from the headquarters building accounts, such payments will not count against coordinated party expenditure limits…[and] [e]xpenditures by federal candidate committees for cybersecurity protection for candidates' personal devices and accounts is allowed according to the terms of Advisory Opinion 2018-15 (Wyden)."

The FEC remarked that "foreign cyberattacks, in which the attackers may not have any spending or physical presence in the United States, may present unique challenges to both criminal prosecution and civil enforcement." The FEC recognized "that fulfilling its "obligation to preserve the basic conception of a political community" under section 30121 cannot hinge solely on prosecution of foreign violators abroad." The agency contended that "[e]ffective enforcement of that provision to protect American elections from urgent cyber threats also requires that countermeasures be taken within the United States."

The FEC stated that

> "Secure information communications technology" means a commercial-off-the-shelf computing device which has been configured to restrict unauthorized access and uses publicly available baseline configurations. The term "cybersecurity product or service" means a product or service that helps an organization cost-effectively identify and detect cyber risks and prevent, protect against, respond to, and recover from cyber attacks by achieving the set of standards, guidelines, best practices, methodologies, procedures, and

processes as developed by the National Institute of Standards and Technology pursuant to 15 U.S.C. 272 (c)(15) and (e).

The FEC also issued an advisory opinion granting the request of the Defending Digital Campaigns, Inc. (DDC) to "offer free or reduced-cost cybersecurity services, including facilitating the provision of free or reduced-cost cybersecurity software and hardware from technology corporations, to federal candidates and parties according to a pre-determined set of criteria." The DDC was created by the leaders of the Defending Digital Democracy Project (D3P) at the Belfer Center for Science and International Affairs at Harvard Kennedy School. The D3P has made a number of materials available to help campaigns:

- Cybersecurity Campaign Playbook
- The State and Local Election Cybersecurity Playbook
- Election Cyber Incident Communications Coordination Guide
- Election Cyber Incident Communications Plan Template

The FEC remarked that the DDC intended to achieve two goals: "1) to create secure, nonpartisan forums for sharing information among and between campaigns, political parties, technology providers, law enforcement, and other government agencies to detect cyber threats and facilitate effective responses to those threats; and 2) to provide campaigns and political parties with knowledge, training, and resources to defend themselves from cyber threats."

The FEC stated that "[u]nder the unusual and exigent circumstances presented by your request and in light of the demonstrated, currently enhanced threat of foreign cyberattacks against party and candidate committees, the Commission approves DDC's proposed activity." The FEC stated that the "DDC's proposal is a unique response to such threats." The agency stated that "DDC proposes to offer free or reduced-cost cybersecurity services, including facilitating the provision of free or reduced-cost cybersecurity software and hardware from technology corporations, to federal candidates and parties according to a pre-determined set of criteria." The FEC stated that the "DDC proposes to make its services available on a nonpartisan basis and 'not to benefit any one campaign or political party over another or to otherwise influence any federal election.'" The FEC added that the "DDC plans to offer its services not only to political committees, but also to "think tanks" and other public policy-focused NGOs."

**OMB Revises How Federal Agencies Manage Identity and Credentials**

Last week, the Office of Management and Budget (OMB) completed its revamp of how civilian federal agencies will manage identity, credential, and access management (ICAM) through the issuance of a new framework and the rescission of the previous ICAM system. The new framework will use a risk management approach to ICAM efforts as opposed to the Levels of Assurance (LOA) model formulated and implemented during the George W. Bush Administration. The Department of Commerce, National Institute of Standards and Technology (NIST), the General Services Administration (GSA), and the Department of Homeland Security (DHS) have been tasked with a number of follow-on steps to fully bring the new risk-based ICAM procedures into full practice. Additionally, each civilian agency (as "national security systems" are exempted so is almost all the Department of Defense (DOD) and the Intelligence Community (IC)) will need to implement new ICAM procedures and policies. OMB explained that "[t]o ignite adoption of this new mindset around ICAM capability deployment across the Federal Government, each agency must harmonize its enterprise-wide approach to governance, architecture, and acquisition."

OMB memorandum M-19-17 "sets forth the Federal Government's ICAM policy and includes the following sections:

I. Contextualizing Identity in the Federal Government
II. Managing Identities, Credentials, and Access in Modern Government
III. Adapting the Government's Approach to Homeland Security Presidential Directive 12 (HSPD-12)
IV. Shifting the Operating Model beyond the Perimeter
V. Improving Digital Interactions with the American Public VI. Enumerating Government-wide Responsibilities

OMB stated that "identity management has become even more critical to the Federal Government's successful delivery of mission and business promises to the American public…[and] [a]s such, through this Federal ICAM policy, the Government is enacting a common vision for identity as an enabler of mission delivery, trust, and safety of the Nation." OMB said that "[t]o ensure secure and efficient operations, agencies of the Federal Government must be able to identify, credential, monitor, and manage subjects that access Federal resources, including information, information systems, facilities, and secured areas across their respective enterprises." OMB added that "[i]n particular, how agencies conduct identity proofing, establish enterprise digital identities, and adopt sound processes for authentication and access control significantly affects the security and delivery of their services, as well as individuals' privacy."

OMB stated that "in line with the Federal Government's updated approach to modernization, it is essential that agencies' ICAM strategies and solutions shift from the obsolete LOA model towards a new model informed by risk management perspectives, the Federal resource accessed, and outcomes aligned to agency missions." OMB said that "[t]o set the foundation for identity management and its usage to access physical and digital resources, agencies must implement NIST Special Publication (SP) 800-63-3 and any successive versions (hereafter referred to as NIST SP 800-63)." OMB advised that "[w]hile NIST SP 800-63 is the foundation for digital identity, agencies must use it in combination with the remaining suite of publications that relate to identity management issued by NIST, the Office of Personnel Management (OPM), and DHS to form a comprehensive approach to identity proofing that safeguards privacy and security."

OMB explained that "[t]he interwoven technical architecture of the Federal Government creates complexity in managing access to resources, safeguarding networks, and protecting information." OMB asserted that "[w]hile hardening the perimeter is important, agencies must shift from simply managing access inside and outside of the perimeter to using identity as the underpinning for managing the risk posed by attempts to access Federal resources made by users and information systems."

**Trump Administration Grants Huawei Concessions**

In light of the recent Trump Administration executive order EO titled "Securing the Information and Communications Technology and Services Supply Chain" aimed at Huawei, the Department of Commerce's Bureau of Industry and Security (BIS) "announced that it would issue a Temporary General License (TGL) amending the Export Administration Regulations (EAR) to authorize specific, limited engagement in transactions involving the export, reexport, and transfer of items – subject to the EAR – to Huawei Technologies Co. Ltd. and its sixty-eight non-U.S. affiliates, which were added to the Bureau's Entity List on May 16, 2019" in its press release. BIS explained that "[t]his license will be effective on May 20, 2019 and lasts 90 days." This respite came a day after the

agency "amend[ed] the Export Administration Regulations (EAR) by adding Huawei Technologies Co., Ltd. (Huawei) to the Entity List." The BIS explained that "[t]he U.S. Government has determined that there is reasonable cause to believe that Huawei has been involved in activities contrary to the national security or foreign policy interests of the United States."

In granting a Temporary General License (TGL), BIS explained that

> The TGL authorizes certain activities necessary to the continued operations of existing networks and to support existing mobile services, including cybersecurity research critical to maintaining the integrity and reliability of existing and fully operational networks and equipment. Exporters will be required to maintain certifications, to be made available when requested by BIS, regarding their use of the TGL. With the exception of the transactions explicitly authorized by the TGL, any exports, reexports, or in country transfers of items subject to the EAR will continue to require a special license granted after a review by BIS under a presumption of denial. The Department will evaluate whether to extend the TGL beyond 90 days.

**Court Rules For FTC Against Qualcomm**

A U.S. district court ruled against Qualcomm in a suit filed by the Federal Trade Commission (FTC) and granted permanent injunctive relief against Qualcomm. The FTC claimed "that Qualcomm has harmed competition in two markets for baseband processors, also called modem chips, through a set of interrelated Qualcomm practices." In 2017 the FTC "filed a complaint in federal district court charging Qualcomm Inc. with using anticompetitive tactics to maintain its monopoly in the supply of a key semiconductor device used in cell phones and other consumer products" according to its press release. The FTC alleged "that Qualcomm has used its dominant position as a supplier of certain baseband processors to impose onerous and anticompetitive supply and licensing terms on cell phone manufacturers and to weaken competitors.

The court found

> In combination, Qualcomm's licensing practices have strangled competition in the Code Division Multiple Access (CDMA) and premium Long-Term Evolution (LTE) modem chip markets for years, and harmed rivals, original equipment manufacturers (OEMs), and end consumers in the process. Qualcomm's conduct "unfairly tends to destroy competition itself." *Spectrum Sports*, 506 U.S. at 458. Thus, the Court concludes that Qualcomm's licensing practices are an unreasonable restraint of trade under § 1 of the Sherman Act and exclusionary conduct under § 2 of the Sherman Act. *Microsoft*, 253 F.3d at 58–59 (holding that where conduct causes anticompetitive harm not justified by procompetitive business reasons, the monopolist violates both § 1 and § 2). Therefore, Qualcomm's practices violate § 1 and § 2 of the Sherman Act, and that Qualcomm is liable under the FTC Act, as "unfair methods of competition" under the FTC Act include "violations of the Sherman Act." *Cement Inst.*, 333 U.S. at 693–94.

"[B]ecause Qualcomm's unlawful practices continue and there is a significant risk that Qualcomm will be dominant in 5G, the Court concludes that the unlawful conduct is likely to recur and that a permanent injunction is warranted…[and] granted the Following injunctive relief:

> (1) Qualcomm must not condition the supply of modem chips on a customer's patent license status and Qualcomm must negotiate or renegotiate license terms with customers in good

faith under conditions free from the threat of lack of access to or discriminatory provision of modem chip supply or associated technical support or access to software.
(2) Qualcomm must make exhaustive standard essential patents (SEP) licenses available to modem-chip suppliers on fair, reasonable, and non-discriminatory (FRAND) terms and to submit, as necessary, to arbitral or judicial dispute resolution to determine such terms.
(3) Qualcomm may not enter express or de facto exclusive dealing agreements for the supply of modem chips.
(4) Qualcomm may not interfere with the ability of any customer to communicate with a government agency about a potential law enforcement or regulatory matter.
(5) In order to ensure Qualcomm's compliance with the above remedies, the Court orders Qualcomm to submit to compliance and monitoring procedures for a period of seven (7) years. Specifically, Qualcomm shall report to the FTC on an annual basis Qualcomm's compliance with the above remedies ordered by the Court.

**Further Reading**

"Exclusive: Behind Grindr's doomed hookup in China, a data misstep and scramble to make up" – *Reuters*
"Inside Google's Civil War" – *Fortune*
"How the US-China Trade War Could Hike iPhone Prices" – *WIRED*
"Prince Harry won a legal battle with the paparazzi using Europe's GDPR privacy law — and it gives the royals a powerful new weapon against the media" – *Business Insider*
"China Paper Says U.S. 'Fabricated' Forced Tech Transfer Claims" – *Bloomberg*
"Bluetooth's Complexity Has Become a Security Risk" – *WIRED*
"Appealing for collaboration, DHS nudges ICS companies toward a more 'proactive' defense" – *cyberscoop*
"Soon You May Not Even Have to Click on a Website Contract to Be Bound by Its Terms" – *ProPublica*
"Hobbling Huawei: Inside the U.S. war on China's tech giant" – *Reuters*