Michael Kans' Technology Policy Update
7 August 2019
By Michael Kans, Esq.

Privacy Legislation Continues To Stall

While there has been continued talks on legislation and aspirations to release bill text, Congressional stakeholders in neither chamber have crafted federal privacy legislation. With the pending effective date of the "California Consumer Privacy Act" (CCPA) (A.B. 375) and possible legislation in states like New York, Members are feeling pressure from businesses and their advocacy organizations to implement a national standard. However, Republicans and Democrats remain some distance apart on the principles underlying a bill with some issues continuing to spark disagreement: a private right of action for consumers; whether laws like CCPA will be preempted; the FTC's authority, resources, and structure; whether and to what extent small businesses will be exempted; and if data security will be part of a bill.

In the last week of July, the chair and ranking member of the primary committee of jurisdiction in the Senate met this week to continue talks over a federal privacy bill. Senate Commerce, Science, and Transportation Committee Chair Roger Wicker (R-MS) and Ranking Member Maria Cantwell (D-WA) sat down on July 31 to try and resolve their differences on what a federal privacy statute should look like, including the possibility that data security legislation could be joined to such a bill, an outcome Cantwell has advocated for. At a May 1 hearing, Cantwell made clear she wishes to see privacy and data security addressed in the same bill. In remarks to reporters before the meeting, Wicker conceded that he is open to such a bill, stating such a bill is "not outside the realm of possibility." However, Wicker characterized language allowing consumers to sue companies over privacy violations a "total non-starter," reflecting the position most Republican stakeholders hold on a private right to action. However, the framework for legislation Cantwell and her staff has developed would include a right for consumers to sue, so this impasse would need to be resolved, possibly among others, before Wicker and Cantwell could reach agreement on a bill. In terms of timeline on a bill, Wicker expressed his hopes that he and Cantwell could reach agreement before Congress returns in September.

Moreover, despite Wicker and Cantwell effectively excluding the other committee Members who were part of a bipartisan working group aiming at developing privacy legislation, two Members are still developing a bill. Senators Jerry Moran (R-KS) and Richard Blumenthal (D-CT) also met this week to continue crafting their bill. Moran told a reporter that they would seek to introduce a bill before the end of the year. This bill would reportedly preempt state laws like the "CCPA and would bolster the Federal Trade Commission's ability to police privacy. Additionally, Moran did not rule out including a private right of action for consumers, remarking that "I've never taken anything off the table in looking for the overall view of what the bill looks like." He added that his understanding of Cantwell's framework is "very similar to where we were in our working group."

In the House, the House Energy and Commerce Committee's Consumer Protection & Commerce Subcommittee Chair Jan Schakowsky (D-IL) is now looking to introduce a bill in late September or early October but this timeline could slip. Schakowsky had originally said she wanted to introduce a bill before the August recess.

With respect to the substance of privacy legislation, unnamed committee aides have been quoted as saying that preemption of state laws is necessary for a bill to be enacted. However, Speaker Nancy Pelosi (D-CA), Senate Judiciary Committee Ranking Member Dianne Feinstein (D-CA), and other California Democrats have stated they would block any federal bill weaker than the CCPA. It is unclear whether they will, in fact, honor this commitment or even be in a position to do so if a bipartisan consensus bill can be crafted. Additionally, two allies of Pelosi are said to be working on a bill (Representatives Anna Eshoo (D-CA) and Zoe Lofgren (D-CA)) but a timeline for unveiling is not apparent.

Additionally, there seem to be differences between Schakowsky and her Republican counterpart on what federal legislation would look like. Earlier in the summer, Schakowsky remarked that "[a]t this point I think we will not be calling for a separate independent agency [to police data privacy], but we will be calling for a division within the Federal Trade Commission." Yet, Ranking Member Cathy McMorris Rodgers (R-WA), stated "I agree that the FTC should be the cop on the beat when it comes to enforcement of privacy standards, but I'm focused on helping consumers through limited and specific jurisdiction of the FTC, not through creating even more bureaucracy." Yet, Schakowsky made clear that Democratic efforts to work with the minority will only go so far: "[o]bviously it would be a great thing if we could do it with the Republicans...[but] [w]e want to, plan to, with or without them."

Election Security Legislation Blocked

Before the Senate adjourned for the August recess, Senate Democrats again pressured Senate Majority Leader Mitch McConnell (R-KY) to allow election security legislation to come to the floor. Senators Richard Blumenthal (D-CT), Amy Klobuchar (D-MN), and Mark Warner (D-VA) called on Senate Republicans and the White House to support a number of election security bills. However, McConnell and Senate Republicans did not respond publicly regarding their willingness to allow the Senate to move to such legislation.

In mid-July, after the Senate Intelligence Committee released the first of the five volume report on the 2016 presidential election, Blumenthal, Warner, Klobuchar, and other Democrats sought unanimous consent to proceed to a number of election security related bills but were blocked by Senate Republicans. The bills Senate Democrats tried to bring up for immediate consideration included:

- The "Duty To Report Act" (S. 1247)
- The "FIRE Act" (S. 2242)
- The "Senate Cybersecurity Protection Act" (S. 890)
- The "Securing America's Federal Elections Act" (SAFE Act) (H.R. 2722)

However, Senate Republicans objected to each unanimous consent request.

In late June, Klobuchar's unanimous consent request that the Senate immediately begin debate on the "Secure Elections Act of 2019" (S. 1540) was blocked by Senator James Lankford (R-OK) who had sponsored similar legislation in the last Congress. Klobuchar claimed that S. 1540

> would also require States to use paper ballots, and it would provide funding for States to implement post-election audits. It would strengthen the Federal response to attacks on our election systems by requiring the President to issue a national security strategy to protect U.S. democratic institutions from cyber attacks and influence operations, and it would

> establish a bipartisan commission to develop recommendations—drawing upon lessons learned from our European allies, who have also been repeatedly subject to at-tacks from Russia—to counter election interference.

In response, Lankford asserted

> The administration is taking steps on [election security.] In fact, we had multiple hearings with DHS to talk about what they are doing to get security clearances. Now every single State has individuals within their State who have security clearances. Every State has greater cooperation now with the Federal Government. Multiple layers of cyber security have been offered to every single State so that each State can use their own cyber protection or add an additional layer from the Federal Government. It is up to that State to choose. It is not a mandated piece that has come down on them.

Lankford added that

> I have been clear, though, through this process that this cannot be a way of federalizing elections and trying to run the elections or saying that every piece of election equipment has to be run through some bureaucracy here in DC, whatever it may be. This is a State responsibility that the State has to take on. Right now, there is not a way for the States that do not have an election system—pieces of hardware for their elections—to change that hard-ware before 2020.

Klobuchar claimed

> So let's be very precise about why we are having this discussion today, and that is that we could have done this bill with the backup paper ballots at-tached to the funding 1 year ago, but it was blocked by the Republicans. So now we are where we are. There is this idea that we just wait and every year say: It won't help the next election, and it won't help that next election. I believe in the importance and urgency of getting this done.

Yet, the Senate has taken up and passed two election-related bills addressing facets of the cybersecurity challenges. On July 17, the Senate passed the "Defending the Integrity of Voting Systems Act" (S. 1321) by unanimous consent that would "make it a federal crime to hack any voting systems used in a federal election" according to the Senate Judiciary Committee's website. In June the Senate also passed the "Defending Elections against Trolls from Enemy Regimes (DETER) Act" (S. 1328) that "will make "improper interference in U.S. elections" a violation of U.S. immigration law, and violators would be barred from obtaining a visa to enter the United States. The House has yet to act on these bills.

However, despite action on S. 1321 and 1328, Senate Democrats seem intent on continuing to try and force consideration of election security legislation as part of their messaging strategy. It is unclear whether McConnell will relent.

Senate Intelligence Committee Releases First Volume Of Investigation Into Russian Interference

In mid-July, the Senate Intelligence Committee released the first of five anticipated volumes of its report detailing the results of its investigation into Russian interference in the 2016 presidential election. Given the bipartisan nature of the report, the first release neither denies Russian hacking

of election cyber infrastructure during the last presidential election nor does it claim that these and related-activities affected the outcome of the election. The recommendations also do not call for increased federal control or oversight over states' election activities. Given the current deadlock in the Senate regarding election security measures, it seems unlikely Congress would enact any of the changes that might be addressed by legislation. Moreover, with President Donald Trump's antipathy to officials conceding explicitly or implicitly that Russia significantly interfered in the 2016 election, federal agencies would likely proceed very cautiously on implementing any of the recommendations.

The Committee explained

> From 2017 to 2019, the Committee held hearings, conducted interviews, and reviewed intelligence related to Russian attempts in 2016 to access election infrastructure. The Committee sought to determine the extent of Russian activities, identify the response of the U.S. Government at the state, local, and federal level to the threat, and make recommendations on how to better prepare for such threats in the future. The Committee received testimony from state election officials, Obama administration officials, and those in the Intelligence Community and elsewhere in the U.S. Government responsible for evaluating threats to elections.

In terms of top-line findings, the Committee asserted "[t]he Russian government directed extensive activity, beginning in at least 2014 and carrying into at least 2017, against U.S. election infrastructure' at the state and local level." However, the Committee noted it "has seen no evidence that any votes were changed or that any voting machines were manipulated."

The Committee offered the following recommendations:

> 1. Reinforce States' Primacy in Running Elections. States should remain firmly in the lead on running elections, and the federal government should ensure they receive the necessary resources and information.
> 2. Build a Stronger Defense, Part I: Create Effective Deterrence. The United States should communicate to adversaries that it will view an attack on its election infrastructure as a hostile act, and we will respond accordingly. The U.S. Government should not limit its response to cyber activity; rather, it should create a menu of potential responses that will send a clear message and create significant costs for the perpetrator. Ideally, this principle of deterrence should be included in an overarching cyber doctrine for the U.S. Government.
> 3. Build a Stronger Defense, Part II: Improve Information Gathering and Sharing on Threats. The U.S. government needs to build the cyber expertise and capacity of its domestic agencies, such as DHS and FBI, and reevaluate the current authorities that govern efforts to defend against foreign cyber threats. NSA and CIA collection is, by law, directed outside the United States. The U.S. government should invest in capabilities for rapid attribution of cyber attacks, without sacrificing accuracy.
> 4. Build a Stronger Defense, Part III: Secure Election-Related Cyber Systems. Despite the expense, cybersecurity needs to become a higher priority for election-related infrastructure. The Committee found a wide range of cybersecurity practices across the states. Some states were highly focused on building a culture of cybersecurity; others were severely under-resourced and relying on part-time help. The Committee recommends State officials work with DHS to evaluate the security of their election systems end-to-end and prioritize implementing the following steps to secure voter registration systems, state records, and other pre-election activities.

> 5. Build a Stronger Defense, Part IV: Take Steps to Secure the Vote Itself. Given Russian intentions to undermine the credibility of the election process, states should take urgent steps to replace outdated and vulnerable voting systems. When safeguarding the integrity of U.S. elections, all relevant elements of the government—including at the federal, state, and local level—need to be forward looking and work to address vulnerabilities before they are exploited.

The day the Committee released the report, Senate Majority Leader Mitch McConnell (R-KY) blocked Democratic efforts to immediately bring House-passed election security to the floor. Senate Intelligence Committee Ranking Member Mark Warner (D-VA) and Senators Richard Blumenthal (D-CT) and Ron Wyden (D-OR) each made unanimous consent requests to consider House-passed election security McConnell blocked.

FTC Settles With Facebook

In July, the Federal Trade Commission (FTC) formally announced its long awaited $5 billion settlement with Facebook arising from its partnership with Cambridge Analytica in violation of a 2012 settlement. However, the FTC was not unanimous. In approving the settlement, the FTC split along partisan lines 3-2 with the two Democratic Commissioners voting against the settlement.

To put Facebook's $5 billion settlement in perspective, the company announced earnings on July 24 of $16.9 billion for the second quarter of 2019 and an overall profit of $22 billion in 2018. Additionally, the company budgeted for the $5 billion settlement by writing down $3 billion in the first quarter of 2019, meaning that the second quarter charge would be only $2 billion.

Moreover, there was disapproval from a number of stakeholders. Last weekend when word of the settlement was leaked, numerous Democratic Members and privacy advocates decried the settlement which they claimed the total fine was not significant in light of Facebook's conduct and annual revenues and profits. Some went so far as to use the alleged settlement as reasons why any privacy legislation should provide the FTC with vastly more resources and direct the agency to be more vigilant. Additionally, the FTC opted not to hold CEO Mark Zuckerberg and other Facebook executives personally responsible for Facebook's conduct, a step many privacy advocates claim will be necessary for companies to heed federal statutes and regulations.

In his statements about the settlement, FTC Chair Joseph Simons explained that

> Today's complaint alleges that Facebook violated the Commission's order in three ways. First, we allege that Facebook told consumers that they could limit the sharing of their information to groups—their "friends," for example—but, in fact, Facebook shared the information more broadly with app developers. Second, we allege that Facebook did not adequately assess and address privacy risks posed by third-party app developers. Third, we allege that Facebook misrepresented to certain users that they would have to "turn on" facial recognition technology, but for millions of users, that technology was "on" by default. In addition to these alleged order violations, we also allege that Facebook violated the FTC Act when it told users it would collect their phone numbers to enable a security feature, but did not disclose that it also used those numbers for advertising purposes.

Simons outlined the structure of the settlement:

> The settlement with Facebook is based on the recommendation of the FTC's career enforcement staff, and includes three major components. First, Facebook must pay a $5 billion civil penalty, one of the largest in corporate history. Second, the order subjects the company to new, expanded privacy requirements. Third, the order imposes significant structural reforms on how Facebook does business, including greater corporate accountability, more rigorous compliance monitoring, and increased transparency.

In his dissenting statement, Commissioner Rohit Chopra listed his reasons for breaking with the FTC on the Google settlement:

- Facebook's violations were a direct result of the company's behavioral advertising business model. The proposed settlement does little to change the business model or practices that led to the recidivism.
- The $5 billion penalty is less than Facebook's exposure from its illegal conduct, given its financial gains.
- The proposed settlement lets Facebook off the hook for unspecified violations.
- The grant of immunity for Facebook's officers and directors is a giveaway.
- The case against Facebook is about more than just privacy – it is also about the power to control and manipulate.

Commissioner Rebecca Kelly Slaughter explained in her dissent that "[m]y principal objections are:

> (1) The negotiated civil penalty is insufficient under the applicable statutory factors we are charged with weighing for order violators: injury to the public, ability to pay, eliminating the benefits derived from the violation, and vindicating the authority of the FTC.
> (2) While the order includes some encouraging injunctive relief, I am skeptical that its terms will have a meaningful disciplining effect on how Facebook treats data and privacy. Specifically, I cannot view the order as adequately deterrent without both meaningful limitations on how Facebook collects, uses, and shares data and public transparency regarding Facebook's data use and order compliance.
> (3) Finally, my deepest concern with this order is that its release of Facebook and its officers from legal liability is far too broad.

She added that "[r]ather than accepting this settlement, I believe we should have initiated litigation against Facebook and its CEO Mark Zuckerberg…[and] [t]he Commission would better serve the public interest and be more likely to effectively change Facebook by fighting for the right outcome in a public court of law."

As mentioned, the response from some on Capitol Hill was negative. As word of the settlement was leaked a week before it was announced, Senators Edward Markey (D-MA), Richard Blumenthal (D-CT), and Josh Hawley (R-MO) wrote a letter to the FTC and characterized the $5 billion settlement then being floated as "fail[ing] to hold Facebook accountable for its actions and to effectively change the company's behavior." Markey, Blumenthal, and Hawley asserted that "the reported settlement is woefully inadequate" and that "a $5 billion fine alone is a far cry from the type of monetary figure that would alter the incentives and behavior of Facebook and its peers." They called for substantially stronger prohibitions and requirements on Facebook's future conduct that were ultimately not part of the settlement.

Hawley was quoted after the announcement of the settlement:

> If the reports are accurate that the agreement will include no restrictions on user data collection and then sharing with third parties, then what was the consent decree good for in the first place? Why do we even have it?

House Energy and Commerce Committee Chair Frank Pallone Jr (D-NJ) stated

> While $5 billion is a record fine for the FTC, monetary damages are not enough. Facebook has repeatedly demonstrated that it prioritizes profit over people. Tough oversight is needed to prevent the abuse of consumer information by Facebook and other companies. Comprehensive privacy legislation is necessary to strengthen the FTC's authorities and give it more enforcement tools and resources so that violating consumers' privacy and breaking public trust isn't just the cost of doing business.

Pallone's Republican counterpart, Representative Greg Walden (R-OR) and Consumer Protection and Commerce Subcommittee Ranking Member Cathy McMorris Rodgers (R-WA) asserted that

> Today's settlement announcement by the FTC against Facebook is one of the largest civil penalties ever imposed by the U.S. government, and it is by far the largest privacy or data security settlement the world has seen yet. There are many questions about how the new requirements on Facebook will be enforced and what impact that will have on users' privacy moving forward. Those details will really matter, but what we do know is that this order covers a wide range of privacy and data security issues at Facebook, WhatsApp, and Instagram. When Mr. Zuckerberg came to testify before the Energy and Commerce Committee, it was clear that things needed to change. We will continue our oversight of the agency to get answers on these new enforcement requirements, because we must ensure these settlement order terms are enforced to protect the American public. We will also continue our work on a federal privacy framework that sets clear rules of the road to protect consumers

Senate Commerce, Science, and Transportation Committee Chair Roger Wicker (R-MS) argued

> The settlement between the FTC and Facebook further stresses the need for a strong federal data privacy law. The details of Facebook's conduct that were illuminated by the FTC's investigation are troubling. This investigation and settlement, including a fine significantly larger than has ever been assessed by a privacy enforcer anywhere in the world, are examples of the great work the FTC can do. However, without a robust, comprehensive federal privacy law covering data collectors and consumers, bad actors will be able to continue to abuse data in the online marketplace.

Ranking Member Maria Cantwell stated

> This decision underscores the need for strong privacy legislation. When companies betray the public trust, there must be immediate and significant consequences. We need a strong data privacy bill to ensure that the Commission has the tools it needs to protect privacy—including the authority to levy fines on the first offense.

FTC and CFPB Reach Settlement With Equifax

Last month, the Federal Trade Commission (FTC), Consumer Financial Protection Bureau (CFPB), and numerous states and territories unveiled their settlement with Equifax regarding what may be the biggest breach in U.S. history. In 2017, the credit reporting agency was hacked and it the sensitive personal information of nearly 145 million Americans was accessed and possibly exfiltrated. The settlement may total as much as $700 million depending on how much financial assistance consumers will need in monitoring and repairing their credit on account of fraud related to the breach.

The FTC explained

> As part of the proposed settlement, Equifax will pay $300 million to a fund that will provide affected consumers with credit monitoring services. The fund will also compensate consumers who bought credit or identity monitoring services from Equifax and paid other out-of-pocket expenses as a result of the 2017 data breach. Equifax will add up to $125 million to the fund if the initial payment is not enough to compensate consumers for their losses. In addition, beginning in January 2020, Equifax will provide all U.S. consumers with six free credit reports each year for seven years—in addition to the one free annual credit report that Equifax and the two other nationwide credit reporting agencies currently provide. The company also has agreed to pay $175 million to 48 states, the District of Columbia and Puerto Rico, as well as $100 million to the CFPB in civil penalties.

CUI Guidance Released

The National Institute of Standards and Technology (NIST) has released draft guidelines for federal agencies and contractors on how they can protect so-called controlled unclassified information (CUI), an effort that dates back well into the Obama Administration:

- Draft NIST Special Publication (SP) 800-171 Revision 2: Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations
- NIST SP 800-171B: Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations: Enhanced Security Requirements for Critical Programs and High Value Assets
- A Department of Defense (DOD) Cost Estimate for implementation of SP 800-171B

A number of the requirements in the two draft Special Publications may be binding on defense contractors per a DOD regulation and clauses in contracts. Comments were due last week.

It must be noted that SP 800-171 only applies "for a nonfederal system or organization when mandated by a federal agency in a contract, grant, or other agreement...[and] apply only to the components of nonfederal systems that process, store, or transmit CUI, or that provide security protection for such components." NIST explained that SP 800-171 "focuses on protecting the confidentiality of CUI in nonfederal systems and organizations and recommends specific security requirements to achieve that objective...[and] does not change the requirements set forth in FISMA, nor does it alter the responsibility of federal agencies to comply with the full provisions of the statute, the policies established by OMB, and the supporting security standards and guidelines developed by NIST."

NIST stated SP 800-171B "provides a set of enhanced security requirements to protect the confidentiality of CUI in nonfederal systems and organizations from the advanced persistent threat (APT)." NIST explained that "[t]he enhanced security requirements provide the foundation for a new multidimensional, defense-in-depth protection strategy that includes three, mutually supportive and

reinforcing components: (1) penetration resistant architecture; (2) damage limiting operations; and (3) designing for cyber resiliency and survivability."

NIST added

> The enhanced security requirements are not required for any particular category or article of CUI, rather are focused on designated high value assets or critical programs that contain CUI. These critical programs and high value assets are potential targets for the APT, and thus, require enhanced protection. The enhanced security requirements are to be implemented in addition to the basic and derived requirements in NIST Special Publication 800-171, since the basic and derived requirements are not designed to address the APT. The enhanced requirements apply only to the components of nonfederal systems that process, store, or transmit CUI or that provide protection for such components when the designated CUI is contained in a critical program or high value asset.

In the DOD Cost Estimate, the Pentagon stated that "the Defense Federal Acquisition Regulation (DFARS) clause 252.204-7012 requires contractors to implement basic cybersecurity requirements if processing DOD CUI on their unclassified information systems." The DOD stated that "Draft NIST SP 800-171B is intended to apply on a contract-by-contract basis for a critical programs with the costs to implement and maintain these additional protections typically being an allowable contract cost to the government."

Trump Administration Releases AI Policy Documents

The National Institute of Standards and Technology (NIST) has released for comment "U.S. Leadership in AI: Plan for Federal Engagement in Developing Technical Standards and Related Tools" (AI Federal Engagement Plan) and the Office of Science and Technology Policy (OSTP) has released National AI Research & Development Strategic Plan: 2019 Update (AI R&D Plan) to fulfill directives laid out in the February 2019 Executive Order 13859, the American Artificial Intelligence Initiative. It bears note that both of these efforts are being driven by Deputy Assistant to the President for Technology Policy/Chief Technology Officer (CTO) Michael Kratsios, who has proven influential on technology issues in the Administration.

EO 13859 directs the Department of Commerce through NIST to "issue a plan for Federal engagement in the development of technical standards and related tools in support of reliable, robust, and trustworthy systems that use AI technologies," and the AI Federal Engagement Plan is NIST's response. NIST is asking for comments by July 19, as the agency is required to submit the final document to the White House by August 10, 2019. NIST explained that the AI Federal Engagement Plan "provides guidance for bolstering Federal agencies' engagement in AI technical standards to promote continued U.S. leadership in AI...[and] focuses on the Federal government's role in advancing AI standards and priorities for research that support development of technically sound and fit for purpose standards." NIST stated that "America's success and prospects as the global AI leader demands that the Federal government play an active role in developing AI standards...[incuding] AI standards-related efforts needed by agencies to fulfill their missions by:

- supporting and conducting AI research and development,
- engaging at the appropriate involvement level in AI standards development, procuring and deploying standard-based products and services, and
- developing and implementing policies, including regulatory policies where needed.

NIST contended that "[t]he government's meaningful engagement in fulfilling that role is necessary – but not sufficient – for the nation to maintain its leadership in this competitive realm." NIST stated that "[a]ctive involvement and leadership by the private sector, as well as academia, is required." NIST argued that "[i]n addition to the guidance provided regarding priorities and levels of engagement called for in the previous section of this plan, the Federal government should commit to deeper, consistent, long-term engagement in AI standards development activities to help the United States to speed the pace of trustworthy AI technologies...[and] [s]pecifically, the Federal government should:

1. Bolster AI standards-related knowledge, leadership, and coordination among Federal agencies to maximize effectiveness and efficiency.
2. Promote focused research to advance and accelerate broader exploration and understanding of how aspects of trustworthiness can be practically incorporated within standards and standards-related tools.
3. Support and expand public-private partnerships to develop and use AI standards and related tools to advance trustworthy AI.
4. Strategically engage with international parties to advance AI standards for U.S. economic and national security needs.

Kratsios stated in NIST's press release, that "[t]oday's draft plan is another critical step in implementing the American AI Initiative, our national strategy to maintain and strengthen America's leadership in AI."

OSTP explained that the AI R&D Plan "highlights the key priorities for Federal investment in AI R&D." In the cover letter, Kratsios conceded that "[w]hile this Plan does not define specific research agendas for Federal agency investments, it does provide an expectation for the overall portfolio for Federal AI R&D investments." He said that the plan identifies "eight strategic priorities," seven of which "continue from the 2016 [National Artificial Intelligence Research and Development Strategic Plan], reflecting the reaffirmation of the importance of these strategies by multiple respondents from the public and government, with no calls to remove any of the strategies." Kratsios asserted that "[t]he eighth strategy is new and focuses on the increasing importance of effective partnerships between the Federal Government and academia, industry, other non-Federal entities, and international allies to generate technological breakthroughs in AI and to rapidly transition those breakthroughs into capabilities."

OTSP outlined the eight strategic priorities:

- Strategy 1: Make long-term investments in AI research. Prioritize investments in the next generation of AI that will drive discovery and insight and enable the United States to remain a world leader in AI.
- Strategy 2: Develop effective methods for human-AI collaboration. Increase understanding of how to create AI systems that effectively complement and augment human capabilities.
- Strategy 3: Understand and address the ethical, legal, and societal implications of AI. Research AI systems that incorporate ethical, legal, and societal concerns through technical mechanisms.
- Strategy 4: Ensure the safety and security of AI systems. Advance knowledge of how to design AI systems that are reliable, dependable, safe, and trustworthy.
- Strategy 5: Develop shared public datasets and environments for AI training and testing. Develop and enable access to high-quality datasets and environments, as well as to testing and training resources.

- Strategy 6: Measure and evaluate AI technologies through standards and benchmarks. Develop a broad spectrum of evaluative techniques for AI, including technical standards and benchmarks.
- Strategy 7: Better understand the national AI R&D workforce needs. Improve opportunities for R&D workforce development to strategically foster an AI-ready workforce.
- Strategy 8: Expand public-private partnerships to accelerate advances in AI. Promote opportunities for sustained investment in AI R&D and for transitioning advances into practical capabilities, in collaboration with academia, industry, international partners, and other non-Federal entities.

There are other-EO related deliverables. Notably, by mid-August the Office of Management and Budget (OMB) is required to issue a memorandum to all federal agencies that "inform the development of regulatory and non-regulatory approaches by such agencies regarding technologies and industrial sectors that are either empowered or enabled by AI, and that advance American innovation while upholding civil liberties, privacy, and American values; and consider ways to reduce barriers to the use of AI technologies in order to promote their innovative application while protecting civil liberties, privacy, American values, and United States economic and national security." But, OMB is required to issue a draft for public comment, and to date this has not been made available.

Three Bills To Amend The CCPA Advance

A few weeks ago, the California Senate Judiciary Committee took up five of the bills the California Assembly passed to amend the California Consumer Privacy Act (CCPA) (A.B. 375). However, the three bills the Committee passed were narrowed considerably commensurate with the views of consumer and privacy advocates: A.B. 25, a bill to address the compliance obligations of employers regarding employee personal information; A.B. 846, a bill on how the CCPA would treat customer loyalty and reward programs; and A.B. 1564, legislation that would have narrowed the means by which consumers could make requests regarding their personal information. The two other bills failed to advance; one was voted down and the other was not brought up for a vote: A.B. 873 would have narrowed the definition of personal information and A.B. 1416 which would have created new exemptions for using personal information to meet government and security obligations.

The next step for the three passed bills is the Senate Appropriations Committee where a consumer-friendly CCPA bill sponsored by the Senate Judiciary Committee Chair died last month. It is unclear whether these bills will be sent to the floor of the California Senate for a vote. The Senate Judiciary Committee's actions may spell the end of efforts in this legislative session by businesses and related advocacy organizations to try and change the CCPA, meaning the bill as written and fleshed out by forthcoming regulations may take effect next year.

The amended version of A.B. 25 the Committee agreed to would exempt employers from the CCPA for only one year for activities related to collecting information from job applicants and employees. The bill as passed out of the Assembly would have made this exemption permanent. Now, it would expire on January 1, 2021. Additionally, employers would still need to inform applicants and employees about the categories of information the employer is collecting and the purposes for which the information will be used. When the CCPA takes effect, most companies doing business in California would need to meet this requirement. However, as reported out of the Assembly, A.B. 25 would have exempted businesses from meeting this responsibility. Moreover, employers may still be sued by job applicants and employees for a failure to "implement reasonable security

procedures and practices if that failure results in a consumer's personal information being subject to unauthorized access and exfiltration, theft, or disclosure." Other language in A.B. 25, as passed by the Assembly, was left unchanged that would allow businesses to require consumers to use an existing consumer account for the purposes of authenticating a consumer's request for certain personal information collected and used by the company. Under the CCPA generally, "businesses must disclose and deliver the required information within 45 days of receiving a "verifiable consumer request," which means a request that is made by a consumer, and that the business can reasonably verify, pursuant to regulations to be adopted by the Attorney General, to be the consumer about whom the business has collected personal information."

A.B. 846, a bill on how customer loyalty programs would be treated under the CCPA, was also amended. At present, the CCPA "prohibits a business from discriminating against the consumer for exercising any of the consumer's rights under the act, except that a business may offer a different price, rate, level, or quality of goods or services to a consumer if the differential treatment is reasonably related to value provided to the consumer by the consumer's data." Likewise, businesses are authorized "to enter a consumer into a financial incentive program only if the consumer affirmatively consents, subject to revocation at any time by the consumer, to the material terms of the incentive program, and the act requires a business that offers a financial incentive to a consumer to notify the consumer of the financial incentive, as specified." The CCPA also "prohibits a business from using a financial incentive practice that is unjust, unreasonable, coercive, or usurious in nature." Proponents of A.B. 846 claim these provisions would impair or functionally prohibit consumer loyalty or rewards programs.

A.B. 846, as passed by the Assembly in May, 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. However, the Senate Judiciary Committee narrowed this authorization, for opponents pointed out that the authorization served as a loophole under which personal information collected under these programs would functionally be exempted from the broader requirements of the CCPA. Consequently, companies operating loyalty and rewards programs would not need to meet the consent and notice provisions in the CCPA. The amendment version of A.B. 846 specifies that the CCPA allows for loyalty or rewards programs and allows consumers using these programs to opt out of certain data collection and sale without facing adverse repercussions.

The Committee took up another bill and narrowed it, A.B. 1564. This bill, as passed by the Assembly, 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.

The amended version of A.B. 1564 would require bricks and mortar businesses to provide at least a toll-free number while allowing online-only businesses some flexibility in how to provide the means for consumers to submit requests for information. If a bricks and mortar business operates an online website, then it must have a website address at which these requests can be made. Online only

businesses that have direct relationships with consumers from whom they collect personal information "shall only be required to provide an email address for submitting requests for information required to be disclosed."

The Committee voted against advancing A.B. 873, a bill consumer and privacy advocates strongly opposed because they claimed it would create a loophole so broad in the CCPA as to render the rest of the bill superfluous. As you may recall, A.B. 873 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."

Finally, the Committee opted against considering A.B. 1416, which would do the following:

1) Provides 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 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 specified requirements are met.
3) Provides that the obligations imposed on businesses by the CCPA shall not restrict a business's ability to sell the personal information of a consumer who has opted-out of the sale of the consumer's personal information 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.
4) Sunsets these new exemptions on January 1, 2024

Consumer and privacy advocates strongly opposed A.B. 1416 for much the same reason they opposed A.B. 873: they claimed loopholes would be established that would essentially negate the broader CCPA requirements.

In May, the California Senate Appropriations Committee blocked further consideration of a bill (S.B. 561) backed by Senate Judiciary Committee Chair Hannah-Beth Jackson and California Attorney General Xavier Becerra that was widely viewed as being consumer-friendly and would have expanded the scope of the CCPA. Notably, the bill 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. S.B. 561 would also expand the private right of action available to California residents by allowing consumers to sue if any of the rights granted by the CCPA are violated. Under the CCPA as enshrined in statute, consumers may only sue if their "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."

NY SHIELD Act Passed; Privacy Bill Introduced

New York State has updated its data security and breach notification statute such that any business holding the personal information of New York citizens is now subject to its requirements. Previously, covered entities needed to be conducting business in New York. Additionally, if an unauthorized person merely accesses personal information that should be safeguarded, then New York will consider that a breach in most circumstances. Under the previous statute, this type of information had to be acquired for a breach to have occurred. New York's new "Stop Hacks and Improve Electronic Data Security Act" (SHIELD Act) fully takes effect in eight months.

The new statute imposes a duty of any entity that holds the private information of New York residents. Consequently, "[a]ny person or business which owns or licenses computerized data which includes private information shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the system to any resident of New York state whose private information was, or is reasonably believed to have been, accessed or acquired by a person without valid authorization." The statute previously imposed this duty only if the covered entity "conducts business in New York state," but now it is any entity that holds the private information of New York residents, causing the state's data security and breach notification law to include any entities that do not conduct business in New York but hold the private information of those residents. In this vein, these entities must "develop, implement and maintain reasonable safeguards to protect the security, confidentiality and integrity of the private information including, but not limited to, disposal of data." Yet, what constitutes "reasonable safeguards" is not spelled out in the statute. Small businesses are subject to a sliding scale as "reasonable" data security will be determined by "the size and complexity of the small business, the nature and scope of the small business's activities, and the sensitivity of the personal information the small business collects from or about consumers."

As noted earlier, the definition of what constitutes a breach has been widened to include instances where private information has been merely accessed without valid authorization and not acquired. There is an exception for "good faith" access or acquisition by an employee or agent of the business "for the purposes of the business." Covered entities will need to determine whether information has been accessed or is reasonably believed to have been accessed in contravention of the statute, and in doing so "may consider, among other factors, indications that the information was viewed, communicated with, used, or altered by a person without valid authorization or by an unauthorized person."

However, there is a significant exception to the responsibility to inform consumers in the instance of a breach. Notice is not necessary "if the exposure of private information was an inadvertent disclosure by persons authorized to access private information, and the person or business reasonably determines such exposure will not likely result in misuse of such information." In this case, the covered entity must document this finding and keep it for five years unless over 500 New York residents were affected provide this finding to the New York Attorney General. Also, covered entities are exempted from providing notification to New York residents if they have already done so pursuant to Gramm-Leach-Bliley, HIPAA, or the New York State Department of Financial Services' Cybersecurity Regulation (23 NYCRR 500).

The SHIELD Act significantly expands the type of information that must be protected and that could give rise to a breach and notification responsibilities in the event of being accessed or acquired. Notably, the new statute would include these types of information as needing protection:

- account number, credit or debit card number, if circumstances exist wherein such number could be used to access an individual's financial account without additional identifying information, security code, access code, or password; or
- biometric information, meaning data generated by electronic measurements of an individual's unique physical characteristics, such as a fingerprint, voice print, retina or iris image, or other unique physical representation or digital representation of biometric data which are used to authenticate or ascertain the individual's identity; or
- a user name or e-mail address in combination with a password or security question and answer that would permit access to an online account.

Under the revised statute, the accessing or acquisition of these types of information along with "personal information" would constitute a breach in most cases. However, like many data security and breach notification regimes, if the information is encrypted and the encryption key is not accessed or acquired, then even if an unauthorized user obtains or views the information, then this is not considered a breach.

In the event a covered entity is breached but fails to properly notify affected consumers, then the Attorney General may sue for a range of remedies including injunctive relief, actual losses and financial harm and also for penalties in the event of a company knowingly or recklessly violating the SHIELD Act up to $250,000.

Incidentally, there is a privacy bill in committee in the New York Senate, the "New York Privacy Act" (S. 5642), that would institute a duty on entities that "will require the companies to attain consent from consumers before they share and/or sell their information by acting as fiduciary entities." This bill could potentially sweep wider than the "California Consumer Privacy Act" (CCPA) (A.B. 375). Specifically, the bill provides

> Personal data of consumers shall not be used, processed or transferred to a third party, unless the consumer provides express and documented consent. Every legal entity, or any affiliate of such entity, and every controller and data broker, which collects, sells or licenses personal information of consumers, shall exercise the duty of care, loyalty and confidentiality expected of a fiduciary with respect to securing the personal data of a consumer against a privacy risk; and shall act in the best interests of the consumer, without regard to the interests of the entity, controller or data broker, in a manner expected by a reasonable consumer under the circumstances.

This bill shares similarities with a bill introduced in the last Congress. Last December, Senator Brian Schatz (D-HI) and 14 other Senate Democrats introduced the "Data Care Act" (S. 3744), which would extend the concept of fiduciary responsibility currently binding on health care professionals and attorneys with respect to the patients and clients' information to "online service providers" such as Facebook, Google, Apple, etc. In short, these online service providers would be severely be limited on how they collect, share, and sell the personally identifiable information (PII), for these companies would need to treat their customers' PII as privileged and deserving of a greater level of protection, much like the HIPAA regulations impose this standard on health care providers or bar associations' rules on attorneys. Thus far, Schatz and his cosponsors have not reintroduced this bill likely because of the Senate Commerce Committee's efforts to craft a bipartisan bill.

IOT Legislation Sent To Full Senate

On July 10, the Senate Commerce, Science, and Transportation Committee held a markup and reported out the "Developing Innovation and Growing the Internet of Things (DIGIT) Act" (S. 1611) sponsored by Senators Deb Fischer (R-NE), Cory Gardner (R-CO), Brian Schatz (D-HI), and Cory Booker (D-NJ). In her press release, Fischer explained the bill would "would convene a working group of federal entities and experts from the private and academic sectors tasked with providing recommendations to Congress on how to facilitate the growth of connected Internet of Things (IoT) technologies." She added that "[t]he group's recommendations would focus on how to plan for, and encourage, the development and deployment of the IoT in the U.S…[and] directs the Federal Communications Commission (FCC) to complete a report assessing spectrum needs required to support the Internet of Things." S. 1611 is substantially similar to legislation (S. 88) the Senate passed unanimously in the last Congress the House never took up. It is not clear whether the same resistance exists in the House, but unlike the last Congress a companion DIGIT Act has not yet been introduced in the House.

CDM Legislation Reintroduced

Last week, Senators John Cornyn (R-TX) and Maggie Hassan (D-NH) introduced the "Advancing Cybersecurity Continuing Diagnostics and Mitigation Act" (S. 2318), a bill that would codify the Department of Homeland Security's (DHS) Continuous Diagnostics and Mitigation (CDM) Program, the system that DHS and many federal agencies use to increase their visibility into their networks and top better fend off attacks and probes. This bill is similar to a bill the House passed last year and legislation Cornyn and Hassan introduced last year.

In their press release they explained "[t]his bill would:

- Codify the work of the CDM program to date;
- Require the Secretary to make CDM capabilities available, at the federal, state and local level;
- Establish policies for reporting cyber risks and incidents based upon data collected under CDM;
- Direct the Secretary to deploy new CDM technologies to continuously evolve the program;
- Mandate that DHS to develop a strategy to ensure the program continues to adjust to the cyber threat landscape."

Last year, the House passed legislation to codify the CDM program that died in the Senate. The "Advancing Cybersecurity Diagnostics and Mitigation Act" (H.R. 6443) that "codifies and defines the activities of the CDM program at the DHS." Cornyn and Hassan also introduced a similar bill last fall, S. 3464, that was referred to the Senate Homeland and Governmental Affairs Committee which did not act on it.

Further Reading

"NSA Isn't Always Following Its Own Cybersecurity Policies, Watchdog Says" – Nextgov
"How CISA Says to Protect Smart Devices from Bad Apps" – Nextgov
"Huawei staff share deep links with Chinese military, new study claims" – CNBC
"A City Paid a Hefty Ransom to Hackers. But Its Pains Are Far From Over." – New York Times
"FTC to Ask About Disabling YouTube Ads for Kids' Privacy" – Bloomberg

"China Snares Tourists' Phones in Surveillance Dragnet by Adding Secret App" – *The New York Times*
"Exclusive: Inside the effort to turn Trump against Amazon's bid for a $10 billion contract" – *CNN*
"Why we should be very scared by the intrusive menace of facial recognition" – *The Guardian*
"FaceApp Is the Future" – *The New York Times*
"Put Another Zero on Facebook's Fine. Then We Can Talk." – *The New York Times*
"'This isn't IAD 2.0': NSA's new Cybersecurity Directorate plots its mission" – *cyberscoop*