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

CCPA Bills Advance To Senate Floor

The California Senate Appropriations Committee has allowed six bills to advance that would amend the "California Consumer Privacy Act" (CCPA) (A.B. 375) under the use of a Senate rule that found the bills would not have a significant financial impact on the state government. This means by which these bills advanced matters to those looking to expand the bills in any attempt to rewrite or soften the CCPA because now all proposed amendments will need to be proposed and debated on the Senate floor. Had the Senate Appropriations Committee Chair found these bills had a financial impact, then all changes could have been made behind proverbial closed doors and reported out in the form of amended bills. This latter route is often used by advocacy organizations to change legislation to their liking. Now, the bills, AB 25, AB 846, AB 1564, AB 1146, AB 874, and AB 1355, are scheduled to come to the Senate floor this week, and as some of them have been changed since the Assembly passed them, they will have to go back to that body before being sent to Governor Gavin Newsom to sign or veto. Specifically, the more substantive of the bills, AB 25, AB 846, AB 1564, and AB 1146, would be sent back to the Assembly for further consideration. Moreover, given the California legislature's calendar, work on these bills will need to be finished by next month when the Assembly and Senate adjourn on September 13 until January 6, 2020. The CCPA, of course, takes effect on January 1, 2020.

Last month, the California Senate Judiciary Committee approved an amended version of A.B. 25 that 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."

A.B. 1146 would "narrowly limit[] the CCPA's opt-out and deletion rights in order to facilitate prompt and effective recalls and warranty work" of automobiles. Consequently, the CCPA's opt-out right for consumers "does not apply to "vehicle information or ownership information retained or shared between a new motor vehicle dealer . . . and the vehicle's manufacturer" if such information is shared "for the purpose of effectuating, or in anticipation of effectuating, a vehicle repair covered by a vehicle warranty or a recall." During the process under which the bill was amended, language was added to prevent "the new motor vehicle dealer and vehicle manufacturer from selling, sharing, or otherwise using this information for any other purpose." It bears note that at least one committee analysis of the bill claims existing language under the CCPA would allow car dealers and manufacturers to retain consumer information for the purpose of communicating warranty and recall information.

The two remaining bills have not been changed by the California Senate and are non-controversial. If these are passed, then they would go straight to the Governor.

A.B. 1355 would address various drafting errors and make other clarifying changes in the California Consumer Privacy Act of 2018 (CCPA). Specifically, this bill would: 1) Correct a drafting error in the CCPA's definitions to specify that "personal information" (as opposed to "publicly available") does not include consumer information that has been deidentified or aggregate consumer information. 2) Address duplicative language in the CCPA relating to a consumer's right to know what personal information (PI) has been collected about them. 3) Clarify that consumers who are at least 13 years of age and less than 16 years of age (as opposed to "between 13 and 16 years of age") have the right to opt-in to the sale of their PI. 4) Align various requirements throughout the CCPA, such as with respect to the information that must be disclosed about the categories of third parties to which a business has sold PI, as specified. 5) Correct various cross-references and include missing cross-references to appropriate CCPA provisions. 6) Correct various drafting errors and make other clarifying or technical, non-substantive changes.

A.B. 874 would expand the "publicly available" information that is exempted from the definition of "personal information" (PI) in the CCPA to ensure that "publicly available" information includes any information that is lawfully made available from government records. This bill would also correct a drafting error in the definition of "PI" to clarify that PI does not include deidentified or aggregate consumer information.

DOD Updates Its IT Modernization Strategy

The Department of Defense's (DOD) Chief Information Officer (CIO) Dana Deasey has released the "DOD Digital Modernization Strategy: DOD Information Resource Management Strategic Plan FY19-23" (the Strategy) that "presents the DOD Chief Information Officer's (DOD CIO) vision for achieving the Department's goals and creating "a more secure, coordinated, seamless, transparent, and cost-effective IT architecture that transforms data into actionable information and ensures dependable mission execution in the face of a persistent cyber threat." The Strategy represents the first major policy document issued by the CIO since the FY 2018 National Defense Authorization Act expansion of his authority to "oversee Department IT budget requests and modernization efforts with a comprehensive management system including both annual and multi-year processes" among other powers. The DOD explained that the Strategy "also serves as the Department's Information Resource Management (IRM) Strategic Plan, presents Information Technology (IT)-related modernization goals and objectives that provide essential support for the three lines of effort in the National Defense Strategy (NDS), and the supporting National Defense Business Operations Plan (NDBOP)." Finally, this Strategy replaces the 2014 "Department of Defense Information Resources Management Strategic Plan."

The DOD stated the Strategy "highlights DOD CIO-led efforts that are key enablers for accomplishing the Department's missions more effectively and efficiently." The DOD noted the "CIO is responsible for all matters relating to the DOD Information Enterprise (IE)." The DOD asserted that "[m]ost efforts in this strategy therefore fall within the JIE Framework, which improves networking capabilities for fixed and mobile users, institutes new DOD-wide enterprise IT services, modernizes technology through coordinated refresh efforts, implements a new joint cybersecurity capability, and improves access to data." The DOD explained that "[t]he JIE Framework also provides a networking design that improves defenses against malicious cyberspace activity and is

managed through a tiered structure of network operations and security centers."

The Strategy "is guided by four priorities and framed within four organizing goals:

- DOD CIO Priorities:
  - Cybersecurity
  - Artificial Intelligence (AI)
  - Cloud
  - Command, Control and Communications (C3)
- Digital Modernization Goals:
  - Innovate for Competitive Advantage
  - Optimize for Efficiencies and Improved Capability
  - Evolve Cybersecurity for an Agile and Resilient Defense Posture
  - Cultivate Talent for a Ready Digital Workforce

The DOD claimed that the Strategy "also fulfills the Office of Management and Budget (OMB) requirement to provide a description of how information resources management activities help accomplish agency missions, and ensure that information resource management decisions are integrated with organizational planning, budget, procurement, financial management, human resources management, and program decisions." The DOD added that the Strategy "includes narratives that summarize the Department's approach to IT modernization, focused on the Joint Information Environment (JIE) Framework (in Section 3), and describe how Cybersecurity is being strengthened (Section 4)." The DOD contended that "[t]hese efforts support achievement of the DOD CIO's modernization vision, and the goals and objectives identified in this strategy...[and the] appendices provide a brief description of promising technologies; tables showing alignment to the NDBOP, the President's Management Agenda, and DOD IT Reform Initiatives, respectively; and a summary of DOD CIO authorities."

The DOD explained

> However, more effective oversight of IT investments is necessary due to the decentralized nature of DOD operations and spending. Recognizing this need, Congress amended DOD CIO authorities and responsibilities, at Section 142 of Title 10, United States Code (U.S.C.), to include annual certification of Military Department and Defense Agency budgets, effective January 1, 2019. The DOD CIO will now oversee Department IT budget requests and modernization efforts with a comprehensive management system including both annual and multi-year processes as shown in Figure 3. The annual CIO Capability Planning Guidance (CPG) will provide programming and budgeting guidance in support of this system. That guidance will support this strategy and provide the primary basis for CIO Budget Certifications. This certification enhances established strategic planning, guidance, and scorecard processes.

Additionally, the CIO identified three future strategy documents that are being worked on: Cyber Risk Strategy, IT Reform Strategy, and C3 Modernization Strategy.

NIST Issues Guidance For Manufacturers To Better Secure IoT

The National Institute of Standards and Technology (NIST) has released a draft of a guide to help Internet of Things (IoT) manufacturers build better cybersecurity into IoT, most of which features notoriously weak or non-existent cybersecurity. NIST wants comments by September 30, 2019 on

its draft "Core Cybersecurity Feature Baseline for Securable IoT Devices" (Draft NISTIR 8259). NIST asserted that "by including cybersecurity features in the IoT devices they design and develop, IoT device manufacturers can help enable IoT device customers to effectively manage their cybersecurity risk, as well as strengthening the security of their devices." Manufacturers do not have to follow or heed this document as it is entirely voluntary. NIST's goal is to provide a framework and lexicon to help drive both better IoT cybersecurity and policy action on achieving that goal.

NIST explained that "intended to help IoT device manufacturers understand the cybersecurity risks their customers face so IoT devices can provide cybersecurity features that make them at least minimally securable by the individuals and organizations who acquire and use them." NIST stated that "[t]his document presents a core baseline of cybersecurity features for all IoT devices that makes devices at least minimally securable by the customers who acquire and use them." The agency explained that "[t]his publication does not specify how customers should secure the IoT devices they deploy and use; it only addresses the importance of manufacturers making all IoT devices minimally securable for their customers." NIST stated that "[t]he core baseline is intended to help customers achieve a basic cybersecurity posture that mitigates general cybersecurity risks…[but] [t]hese features are not exhaustive, and IoT device manufacturers are encouraged to use the core baseline as a starting point."

NIST encouraged interested parties to comment on the entire publication but emphasized its interest in feedback on these issues:

> 1. Section 3 is intended to help IoT device manufacturers better identify the cybersecurity risks their expected customers (individuals and organizations) are likely to face, instead of assuming a generic set of risks faced by a generic set of customers. This would help manufacturers identify the cybersecurity features their customers need their IoT devices to have. Is the proposed process for identifying features appropriate and reasonable? If not, how can it be improved?
> 2. Are the cybersecurity features and the key elements of those features defined in Section 4 the right set for a generic starting point for IoT devices? If not, which cybersecurity features and key elements should be added, removed, or changed, and why?
> 3. We have received considerable feedback that the lack of transparency into the characteristics of many IoT devices can make it harder to understand and address the cybersecurity risks for those devices. Feedback on how useful the communication considerations outlined in Section 6 may be for consumers and manufacturers, as well as how the considerations can be improved, is particularly important.

Of course, IoT has been at the root of a number of infamous bot networks and related distributed denial of service (DDoS) attacks such as Mirai, and this and other guidance documents have been part of the federal government's response. This NIST guidance document flows from the 2017 Executive Order 13800, Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure that "tasked the Department of Commerce and Department of Homeland Security with leading a process to "...identify and promote action by appropriate stakeholders to improve the resilience of the internet and communications ecosystem and to encourage collaboration with the goal of dramatically reducing threats perpetrated by automated and distributed attacks (e.g., botnets)." Thereafter, in May 2018, the agencies submitted "A Report to the President on Enhancing the Resilience of the Internet and Communications Ecosystem Against Botnets and Other Automated, Distributed Threats" that identified a number of steps and prompted a follow on "A Road Map Toward Resilience Against Botnets" released in November 2018. In drafting the instant document, NIST is helping to "address three of the botnet roadmap tasks: "Define Core Security Capability

Baseline," "Enable Risk Management Approach to IoT Security," and "Publish Best Practices for IoT Device Manufacturers." Of course, the roadmap identifies 85 tasks organized in five lines of effort; it is not clear when NIST or other agencies will address these other tasks.

NIST has, of course, also initiated other guidance on IoT. In the recently released "Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks" (NISTIR 8228), the agency sought "to help organizations better understand and manage the cybersecurity and privacy risks associated with individual IoT devices throughout the devices' lifecycles." Although the recommendations in that report are not binding on federal agencies, federal contractors, or other private entities, it is quite likely that NIST's cachet could result in this and other IoT documents setting a de facto standard for IoT security and possibly be folded into federal legislation. For example, the "Internet of Things Cybersecurity Improvement Act of 2019" (H.R. 1668/S. 734) calls on NIST to complete its work on its IoT guidance documents and then use them as the basis for recommendations to the Office of Management and Budget (OMB) to form the federal approach to requiring federal IoT meet certain security standards. Both committees of jurisdiction in the House and Senate have reported out their versions of this bill, opening the possibility that NISTIR 8259 and NISTIR 8228 could ultimately drive IoT cybersecurity in the federal government and in the private sector.

OIG Finds Pentagon Does Not Know If Contractor CUI Is Secure And What CUI Contractors Hold

The Department of Defense's (DOD) Inspector General (IG) released a report titled "Protection of DOD Controlled Unclassified Information on Contractor-Owned Networks and Systems" that identified major shortcomings in how DOD contractors managed the Controlled Unclassified Information (CUI) they hold and use under DOD contracts and how the DOD oversees these contractors. The IG concluded

> the DOD does not know the amount of DOD information managed by contractors and cannot determine whether contractors are protecting unclassified DOD information from unauthorized disclosure. Without knowing which contractors maintain CUI on their networks and systems and taking actions to validate that contractors protect and secure DOD information, the DOD is at greater risk of its CUI being compromised by cyberattacks from malicious actors who will target DOD contractors.

The initiative to better secure CUI started in the Obama Administration and culminated in this 2016 final rule "to establish policy for agencies on designating, safeguarding, disseminating, marking, decontrolling, and disposing of CUI, self-inspection and oversight requirements, and other facets of the Program." The Obama Administration explained that "[t]he rule affects Federal executive branch agencies that handle CUI and all organizations (sources) that handle, possess, use, share, or receive CUI—or which operate, use, or have access to Federal information and information systems on behalf of an agency."

The IG pointed out that "Defense Federal Acquisition Regulation Supplement (DFARS) clause 252.204-7012 requires contractors that maintain CUI to implement security controls specified in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171, which lists security requirements for safeguarding sensitive information on non-Federal information systems." The IG explained that "[t]he requirements include controls related to user authentication, user access, media protection, incident response, vulnerability management, and confidentiality of information." NIST is in the process of revising SP 800-171, Rev. 2 and its sister publications SP 800-171A and

SP 800-171B, all of which are intended to help DOD contractors control and secure CUI on nonfederal systems.

NIST explained the family of CUI publications:

- SP 800-171 "focuses on protecting the confidentiality of CUI in nonfederal systems and organizations and recommends specific security requirements to achieve that objective."
- SP 800-171A "provide[s] a framework and a starting point for developing specific procedures to assess the CUI security requirements in NIST Special Publication 800-171."
- SP 800-171B "contains recommendations for enhanced security requirements to provide additional protection for CUI in nonfederal systems and organizations when such information is part of a critical program or a high value asset. The enhanced security requirements are designed to respond to the advanced persistent threat (APT) and supplement the basic and derived security requirements in NIST Special Publication 800-171 that provide the foundational protection for CUI."

The IG found that "DOD contractors did not consistently implement security controls in accordance with Federal and DOD requirements for safeguarding Defense CUI...[and] [s]pecifically, of the 10 contractors that we assessed:

- seven contractors did not enforce the use of multifactor authentication to access their networks and systems;
- seven contractors did not configure their systems to enforce the use of strong passwords;
- two contractors did not identify network and system vulnerabilities;
- six contractors did not mitigate network and system vulnerabilities in a timely manner;
- six contractors did not protect CUI stored on removable media by using technical and nontechnical safeguards to restrict the use of removable media;
- one contractor did not oversee network and boundary protection services provided by a third-party company;
- one contractor did not document and track cybersecurity incidents;
- eight contractors configured user sessions to lock after extended periods and did not limit unsuccessful logon attempts to reduce the risk of malicious activities;
- two contractors did not implement physical security controls, such as installing internal surveillance cameras, maintaining visitor logs, and securing servers, at their facilities that maintain CUI;
- three contractors did not configure their networks and systems to generate system activity reports nor did they review the networks and systems for malicious or unusual activity; and
- three contractors did not grant system access based on the user's assigned duties and apply the principle of least privilege when granting access.

The IG noted that "[a]lthough the DOD requires contractors to protect CUI by complying with NIST SP 800-171 requirements, DOD Component contracting offices and requiring activities did not establish processes to:

- verify that contract offerors' networks and systems that process, store, and transmit CUI met the NIST security requirements before contract award;
- notify contractors of the specific CUI category related to the contract requirements;
- determine whether contractors accessed, maintained, or developed CUI to meet contractual requirements;
- properly mark documents that contained CUI; and
- verify that contractors implemented minimum security controls required by NIST SP 800-171.

The IG added that "DOD Component contracting offices and requiring activities did not always know which contracts required contractors to maintain CUI because the DOD did not implement processes and procedures to track which contractors maintain CUI...[and] the contracting offices inconsistently tracked which contractors maintain CUI on their networks and systems."

The IG made the following recommendations:

- We recommend that the Director for Contract Policy and Oversight for the Defense Threat Reduction Agency revise the agency's process for monitoring security incidents, [REDACTED], to verify that contractors took appropriate steps to identify, respond to, and report security incidents that involve DOD data. We also recommend that the Director review the performance of the contracting officer responsible for monitoring the security incident identified in this report and consider administrative action, as appropriate, for not ensuring that a contractor took actions to remove the classified information from its corporate network and the contractor's commercial cloud environment. Furthermore, we recommend that the Director for the Defense Counterintelligence and Security Agency (formerly known as the Defense Security Service) assess and document the risk of leaving classified information unprotected in unclassified environments and, based on the assessment, develop and implement controls to protect the information.
- We recommend that the DOD Chief Information Officer direct DOD Component contracting offices and requiring activities to require contractors to use strong passwords that are, at a minimum, 15 characters, and configure their networks and systems to align with DOD requirements for locking accounts after 15 minutes of inactivity and three unsuccessful logon attempts.
- We also recommend that the DOD Component contracting offices, in coordination with requiring activities, implement a plan to verify that the internal control weaknesses for the contractors discussed in this report are addressed.
- In addition, we recommend that the Principal Director for Defense Pricing and Contracting:
    - Revise its current policy related to assessing a contractor's ability to protect DOD information to require DOD Component contracting offices, as part of the Request for Proposal and source selection processes, and requiring activities during contract performance, to validate, at least annually, that contractors comply with security requirements for protecting CUI before contract award and throughout the contract's period of performance.
    - Develop and implement policy requiring DOD Component contracting offices and requiring activities to maintain an accurate accounting of contractors that access, maintain, or develop controlled unclassified information as part of their contractual obligations.
    - Revise its current policy to include language that would require DOD Component contracting offices to validate contractor compliance with minimum security requirements.

If not implemented by the DOD, the IG's findings and recommendations could well make their way into language inserted into an National Defense Authorization Act (NDAA) or the accompanying committee report.

GAO Finds NNSA Has Never Excluded Risky Supply Chain IT From Nuclear Weapon and Command and Control Architecture

The Government Accountability Office (GAO) has released its third assessment of how the Department of Energy's (DOE) National Nuclear Security Administration (NNSA) has used its authority to exclude contractors with information technology (IT) supply chain risks, which is virtually the same as the authority granted to the Intelligence Community (IC) in the FY 2012 Intelligence Authorization Act and the Department of Defense (DOD) in the FY 2011 and FY 2019 National Defense Authorization Acts (NDAA). Most notably, the GAO found "neither DOE nor NNSA has used the authority since it was enacted in December 2013" and recommended that the agencies finish and submit draft recommendations to Congress "to address NNSA's concerns about the authority and improve its usability." However, the GAO's understanding of NNSA's recommendations on how Congress can improve its enhanced procurement authority relating to IT supply chain would be to allow the authority to be used below the Secretary's level and to allow for the exclusion of risky non-national security information technology (IT). It is likely that this report on how NNSA has used its supply chain authority will receive attention in IC agencies, the DOD and Congress regarding the use of their authority given the many reports and allegations regarding supply chain risks in IT. The GAO sent the report to the House and Senate Armed Committees, the House and Senate Appropriations Committee's Energy and Water Development Subcommittees, the Senate Energy and Natural Resources Committee, and the House Energy and Commerce Committee.

The GAO has released two previous reports on the NNSA's use of its supply chain authority, one in 2016 and the other in 2018, both of which called on the DOE and NNSA to implement and use its enhanced procurement authority. In this report, the GAO detailed DOE and NNSA's reluctance to use this authority and their development of recommendations on how Congress could later the supply chain risk authority to make it more usable and effective. The GAO contended that "[b]y communicating the agency's concerns about, and suggested changes to, the enhanced procurement authority in a timely manner, NNSA would provide Congress with relevant information to support congressional decision-making about how best to amend the authority and make it more useful to DOE and NNSA for managing supply chain risks." Consequently, the GAO recommended that "[t]he Secretary of Energy, in coordination with the Administrator of NNSA, should formally communicate to the relevant congressional committees concerns about, and suggested changes to, the enhanced procurement authority in a timely manner."

The GAO reported that the DOE and NNSA found using the authority to exclude bidders on NNSA contracts cumbersome and time consuming. Moreover, the GAO noted the agency's claim that the authority was of limited use because it applied only to the procurement at hand, and if a contractor was excluded on account of supply chain risk, it was only for that procurement and not future procurements. The NNSA argued that existing Federal Acquisition Regulation (FAR) provisions allowed it alternative, more flexible and timely means to exclude risky companies. Incidentally, the NNSA almost used its enhanced procurement authority against Kaspersky in 2018 when the issuance of a Department of Homeland Security (DHS) Binding Operational Directive (BOD) forbidding the use of the Russian company's products and services made moot the agency's considerations.

The GAO explained that NNSA's draft report reportedly "includes suggestions for amending the authority to address NNSA's concerns by

> (1) delegating approval authority to a lower level than the Secretary of Energy to reduce the amount of time it may take to get approval to use the enhanced procurement authority and
>
> (2) allowing NNSA to apply the enhanced procurement authority across multiple contract actions that include the same supplier of concern.

The GAO related that "DOE officials told us that they agree with NNSA's suggestion that the enhanced procurement authority be delegated to a lower level and also suggested that among other things the authority be broadened to include more than covered systems." In a footnote, the GAO explained further NNSA's suggestion: "DOE officials suggested that the authority's definition of a covered system be broadened to include information technology systems that are not directly part of a national security system, in part to make the authority useful to other entities within the department, such as the Power Marketing Administrations, which have responsibility for the electrical grid." The GAO cited statements from DOE and NNSA officials who remarked "that if [its current authority] is amended to address these concerns, the enhanced procurement authority could provide DOE and NNSA with a powerful tool to manage supply chain risks in ways that other tools and authorities cannot." However, given the agencies' target submission date of September 30, 2019, it is almost certainly too late for inclusion in this year's NDAA, and if the recommendations are enshrined in statute, it would be in the FY 2021 NDAA. However, this could be an opportunity for Congress to expand the supply chain exclusion authority of IC agencies and the DOD in similar fashion if they were to report similar problems in using their authority which is almost the same as DOE and NNSA's.

ICO Announces Intention To Levy Fines of £183 Million On British Airways and and £99 Million Marriott For GDPR Vlolations

The United Kingdom's (UK) data protection authority (DPA) has announced its intention to fine two multinationals hundreds of millions of pounds for failing to meet the requirements of the European Union's (EU) General Data Protection Directive (GDPR). British Airways and Marriott stand accused of failing to meet the GDPR's requirements to keep customer data safe, and the UK's Information Commissioner's Office (ICO) is the lead EU DPA investigating the claims against both entities. It must be stressed that these are not final fines and rather represent the ICO's intention to levy such fines subject to the companies making their cases to the regulator. Moreover, these fines are less than

In all, the ICO is proposing to fine British Airways £183,390 million, and in its statement, the ICO explained that

> The proposed fine relates to a cyber incident notified to the ICO by British Airways in September 2018. This incident in part involved user traffic to the British Airways website being diverted to a fraudulent site. Through this false site, customer details were harvested by the attackers. Personal data of approximately 500,000 customers were compromised in this incident, which is believed to have begun in June 2018.

The ICO stated that its "investigation has found that a variety of information was compromised by poor security arrangements at the company, including log in, payment card, and travel booking details as well name and address information." The ICO said that "British Airways has cooperated with the ICO investigation and has made improvements to its security arrangements since these events came to light…[and] [t]he company will now have opportunity to make representations to the ICO as to the proposed findings and sanction."

In its filing with the London Stock Exchange, British Airways Chairman and CEO Alex Cruz stated that "[w]e are surprised and disappointed in this initial finding from the ICO." He claimed that "British Airways responded quickly to a criminal act to steal customers' data…[and] [w]e have found no evidence of fraud/fraudulent activity on accounts linked to the theft." Biritsh Airways indicated

that the proposed fine of £183,390,000 is "1.5 per cent of British Airways' worldwide turnover for the financial year ended 31 December 2017."

The ICO issued a similar statement regarding its intention to fine Marriott for lapses in meeting its GDPR responsibilities. The ICO stated that "[f]ollowing an extensive investigation the ICO has issued a notice of its intention to fine Marriott International £99,200,396 for infringements of the GDPR" relating "to a cyber incident which was notified to the ICO by Marriott in November 2018." The ICO stated that "[a] variety of personal data contained in approximately 339 million guest records globally were exposed by the incident, of which around 30 million related to residents of 31 countries in the European Economic Area (EEA)…[and] [s]even million related to UK residents." The ICO stated that "[i]t is believed the vulnerability began when the systems of the Starwood hotels group were compromised in 2014." The ICO added that "Marriott subsequently acquired Starwood in 2016, but the exposure of customer information was not discovered until 2018…[and] [t]he ICO's investigation found that Marriott failed to undertake sufficient due diligence when it bought Starwood and should also have done more to secure its systems."

In a filing with the U.S. Securities and Exchange Commission (SEC), Marriott stated that it "intends to respond and vigorously defend its position" to the ICO. Marriott International's President and CEO, Arne Sorenson remarked that "[w]e are disappointed with this notice of intent from the ICO, which we will contest…[because] Marriott has been cooperating with the ICO throughout its investigation into the incident, which involved a criminal attack against the Starwood guest reservation database."

The ICO has issued a number of recent fines for data security and privacy violations, most of which were under the UK's Data Protection Act 1998, which allowed for lower maximum fines. In October 2018, the ICO fined Facebook "£500,000 for serious breaches of data protection law…the maximum allowable under the laws which applied at the time the incidents occurred." These fines were levied because of Facebook's involvement with Cambridge Analytica. The ICO explained that

> The ICO's investigation found that between 2007 and 2014, Facebook processed the personal information of users unfairly by allowing application developers access to their information without sufficiently clear and informed consent, and allowing access even if users had not downloaded the app, but were simply 'friends' with people who had.
> Facebook also failed to keep the personal information secure because it failed to make suitable checks on apps and developers using its platform. These failings meant one developer, Dr Aleksandr Kogan and his company GSR, harvested the Facebook data of up to 87 million people worldwide, without their knowledge. A subset of this data was later shared with other organisations, including SCL Group, the parent company of Cambridge Analytica who were involved in political campaigning in the US.

Likewise, Equifax was also fined £500,000 for its massive breach under the Data Protection Act 1998 "for failing to protect the personal information of up to 15 million UK citizens during a cyber attack in 2017." The ICO stated that "[t]he incident, which happened between 13 May and 30 July 2017 in the US, affected 146 million customers globally." The ICO asserted that "[t]he UK arm of the company failed to take appropriate steps to ensure its American parent Equifax Inc, which was processing the data on its behalf, was protecting the information."

The largest GDPR fine before the ICO announced its intention to fine British Airways and Marriott was France's National Data Protection Commission's (CNIL) €50,000,000 fine on Google "for not

having a valid legal basis to process the personal data of the users of its services, particularly for ads personalization purposes."

Australia's Competition Watchdog Finishes Inquiry Into Facebook and Google

The Australian Competition & Consumer Commission (ACCC) released the final report from its "Digital Platforms Inquiry" that "proposes specific recommendations aimed at addressing some of the actual and potential negative impacts of digital platforms in the media and advertising markets, and also more broadly on consumers." Not surprisingly, the report focuses entirely on Facebook and Google but not Amazon, which the ACCC remarked was still relatively small in Australia. The ACCC expressed its interest in working with Parliament and other competition and privacy regulators to better balance competition in digital markets. This report follows a number of others released this year in the European Union regarding the effect that big technology companies are exerting on markets. The ACCC explained that its 2018 "Preliminary Report contributed to the wider debate about the role digital platforms play and the appropriate level of government oversight."

The ACCC explained that its "Inquiry has focused on the three categories of digital platforms identified in the Terms of Reference: online search engines, social media platforms and other digital content aggregation platforms." The ACCC added that "[a] large part of this Inquiry has focused on Google and Facebook…[which] reflects their influence, size and significance. Google and Facebook are the two largest digital platforms in Australia and the amount of time Australian consumers spend on Google and Facebook dwarfs other rival applications and websites."

The ACCC stated

> This Inquiry has highlighted the intersection of privacy, competition, and consumer protection considerations. Privacy and data protection laws can build trust in online markets. They can increase consumer protections by addressing sources of market inefficiencies such as information asymmetries and bargaining power imbalances. Strengthened privacy and data protection laws can also empower consumers to make more informed choices about how their data is processed. This, in turn, is likely to increase competition between digital platforms regarding the privacy dimension of their services. It may also encourage the emergence of alternative business models that generate value for, and from, consumers in other ways.

The ACCC stated that it "has had particular regard to the impact of digital platforms on news and journalism, including their effects on the sustainability of the commercial news sector and their influence on the consumption, choice and quality of news in Australia." The ACCC asserted that "[o]ther important concerns, including the role of digital platforms in promoting terrorist, extremist or other harmful content and how social media is used for political advertising, are outside the scope of this Inquiry."

The ACCC made a number of detailed recommendations for Parliament and other regulatory bodies:

- Recommendation 1: Changes to merger law
- Recommendation 2: Advance notice of acquisitions
- Recommendation 3: Changes to search engine and internet browser defaults

- Recommendation 4: Proactive investigation, monitoring and enforcement of issues in markets in which digital platforms operate
- Recommendation 5: Inquiry into the supply of ad tech services and advertising agencies
- Recommendation 6: Process to implement harmonised media regulatory framework
- Recommendation 7: Designated digital platforms to provide codes of conduct governing relationships between digital platforms and media businesses to the Australian Communications and Media Authority (ACMA)
- Recommendation 8: Mandatory ACMA take-down code to assist copyright enforcement on digital platforms.
- Recommendation 9: Stable and adequate funding for the public broadcasters
- Recommendation 10: Grants for local journalism
- Recommendation 11: Tax settings to encourage philanthropic support for journalism
- Recommendation 12: Improving digital media literacy in the community
- Recommendation 13: Digital media literacy in schools
- Recommendation 14: Monitoring efforts of digital platforms to implement credibility signalling Recommendation 15: Digital Platforms Code to counter disinformation
- Recommendation 16: Strengthen protections in the Privacy Act
- Recommendation 17: Broader reform of Australian privacy law
- Recommendation 18: Office of the Australian Information Commissioner (OAIC) privacy code for digital platforms
- Recommendation 19: Statutory tort for serious invasions of privacy
- Recommendation 20: Prohibition against unfair contract terms
- Recommendation 21: Prohibition against certain unfair trading practices
- Recommendation 22: Digital platforms to comply with internal dispute resolution requirements
- Recommendation 23: Establishment of an ombudsman scheme to resolve complaints and disputes with digital platform providers

The ACCC stated that "[w]hile different recommendations are made in these reports, the findings reached, and the concerns expressed, are broadly consistent with the ACCC's conclusions…[and] [s]ome examples of international reports include:

- In February 2019, the (UK) Department for Digital, Culture, Media and Sport published the report of the Cairncross Review. This review, led by Dame Frances Cairncross, considered the sustainability of production and distribution of high quality journalism and in particular, the future of the press. It looked at the overall state of news media, the threats to the financial sustainability of publishers, the impact of search engines and social media platforms, and the role of digital advertising. The Cairncross Review reached a number of important conclusions and recommendations. These include that, given the evidence of a market failure in the supply of public interest news, public intervention may be the only remedy, and that measures are required to tackle the uneven balance of power between news publishers and the online platforms that disseminate their output. In particular, this review recommended that leading digital platforms be required to set out codes of conduct to govern their commercial arrangements with news publishers in order to rebalance the relationships between publishers and online platforms.
- In March 2019, the House of Lords Select Committee on Communications published a report 'Regulating in a digital world'. This report found that the regulation of the digital world has not kept pace with its role in people's lives and that a comprehensive and holistic strategy for regulation needed to be developed.

- In March 2019, the report of the UK Digital Competition Expert Panel (led by Professor Jason Furman) 'Unlocking Digital Competition' was published (the Furman Report). This report was commissioned by the Chancellor of the Exchequer to inform the work of HM Treasury, the Department for Digital, Culture, Media and Sport, and the Department for Business, Energy and Industrial Strategy. The Furman Report made a number of significant recommendations. These include the creation of a digital markets unit tasked with developing a code of competitive conduct to apply to digital companies with strategic market status, taking steps to enable greater personal data mobility and open standards, and advancing data openness in order to tackle the key barriers to entry in digital markets. A number of other specific recommendations were made including in relation to UK merger policy.
- In 2018, the European Commission's Commissioner for Competition, Margrethe Vestager, asked Jacques Crémer, Yves-Alexandre de Montjoye and Heike Schweitzer to consider how competition policy should evolve to continue to promote pro-consumer innovation in the digital age. Their report 'Competition policy for the digital era', published in February 2019, concluded that there was no need to rethink the fundamental goals of competition law in light of digitalisation, but identified specific characteristics of platforms and the data economy which meant established concepts, doctrines and methodologies should be revised. The report also identified that in some areas, a regulatory regime may be required.

The ACCC stated that

> In February 2019, the US Federal Trade Commission launched a task force to monitor technology markets. The Technology Task Force will examine industry practices in technology markets, conduct law enforcement investigations and review completed mergers in technology markets. In addition, in June 2019, the European Council of the European Union adopted a regulation that seeks to improve relationships between digital platforms and businesses, by providing businesses with a more transparent, fair and predictable online business environment, as well as an efficient system for seeking redress.

The ACCC stated that "[t]hese steps demonstrate the commonality of the issues explored by the ACCC in this Inquiry, and the shared momentum and direction to address the concerns identified." The ACCC asserted that it "will continue to share and discuss its findings and recommendations with fellow regulators and enforcement agencies overseas." The ACC contended "[c]oordination across national borders is critical to address competition and consumer concerns that arise from the conduct of the leading digital platforms, given their global operations."

Further Reading

"FBI tells lawmakers it can't access Dayton gunman's phone" – *The Hill*
"Oregon Joins States' Antitrust Suit to Bar T-Mobile Sprint Deal" – *Bloomberg*
"Senators ask Jeff Bezos to explain how Amazon recommends products" – *CNBC*
"Exclusive: Google's jobs search draws antitrust complaints from rivals" – *Reuters*
"FTC Chief Says He's Willing to Break Up Big Tech Companies" – *Bloomberg*
"Warren calls for probe into whether FTC 'misled' Americans into thinking they'd receive $125 from Equifax settlement" – *The Washington Post*
"Microsoft Admits Humans Listen to Skype and Cortana in Privacy Policy Update" – *Motherboard*
"Huawei Technicians Helped African Governments Spy on Political Opponents" – *The Wall Street Journal*

"Senator challenges Zuckerberg testimony as 'at best, incomplete' after report of Facebook's audio transcription" – *CNBC*
"Contractors have questions about DOD's cyber requirements" – *FCW*
"Russia Suspected by Some in Giant Bulgaria Hack" – *The New York Times*
"Hackers just found serious vulnerabilities in a U.S. military fighter jet" – *The Washington Post*
"Trump: Voter ID must play 'very strong part' in deal on election security" – *The Hill*