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

Facebook Braces for $3-5 Billion FTC Fine

In Facebook's "First Quarter 2019 Results," the company revealed that it has set aside $3 billion to cover an expected fine from the Federal Trade Commission (FTC) for violating the terms of its 2012 consent decree related to Facebook's interactions with Cambridge Analytica during the 2016 election. The company added the FTC fine could be as high as $5 billion.

In its press release, Facebook stated

> In the first quarter of 2019, we reasonably estimated a probable loss and recorded an accrual of $3.0 billion in connection with the inquiry of the FTC into our platform and user data practices, which accrual is included in accrued expenses and other current liabilities on our condensed consolidated balance sheet. We estimate that the range of loss in this matter is $3.0 billion to $5.0 billion. The matter remains unresolved, and there can be no assurance as to the timing or the terms of any final outcome.

In November 2011, the FTC and Facebook agreed on a draft consent order regarding the agency's allegations that Facebook violated Section 5 of the FTC Act through its privacy practices, and the FTC issued a final order in August 2012. The 20-year final order required Facebook "establish and implement, and thereafter maintain, a comprehensive privacy program that is reasonably designed to (1) address privacy risks related to the development and management of new and existing products and services for consumers, and (2) protect the privacy and confidentiality of covered information." Violations of consent orders can allow the FTC to request that U.S. District Court levy civil fines of more than $16,000 per violation.

However, there have been media reports that the FTC is considering naming Facebook CEO Mark Zuckerberg in the settlement, which would result in greater scrutiny for him as part of the consent decree. Moreover, should the FTC name Zuckerberg, the thinking of those favoring this approach inside and outside the agency is that other technology companies might have pause before embarking on questionable or illegal practices if executives could be held liable by the FTC. Commissioner Rohit Chopra called on the FTC to "hold individual executives accountable for order violations in which they participated, even if these individuals were not named in the original orders" and Senator Richard Blumenthal (D-CT) "'[h]olding Mark Zuckerberg and other top Facebook executives personally at fault and liable for further wrongdoing would send a powerful message to business leaders across the country: You will pay a hefty price for skirting the law and deceiving consumers." According to materials obtained through FOIA requests, the FTC considered naming Zuckerberg in the 2012 settlement but opted against doing so.

GAO Reiterates Priority Recommendations on Technology Issues To OMB and DHS

In April, the Government Accountability Office (GAO) highlighted previously made recommendations that federal agencies had partially fulfilled or failed to fulfill. The GAO deemed these recommendations "priority," which are those it "believes warrant priority attention from heads of key departments or agencies…because, upon implementation, they may significantly improve

government operation, for example, by realizing large dollar savings; eliminating mismanagement, fraud, and abuse; or making progress toward addressing a High Risk or duplication issue." Given that cybersecurity, information technology development and acquisition, cybersecurity workforce, and coordinating public and private cybersecurity efforts are perennial policy areas the GAO finds wanting, it was no surprise recommendations were made to the Office of Management and Budget (OMB) and the Department of Homeland Security (DHS).

GAO released "update on the overall status of the OMB's implementation of GAO's recommendations and to call your personal attention to critical open recommendations that should be given high priority." Again, the GAO pointed to how the federal government develops and buys information technology (IT) as an area in which OMB has not fulfilled GAO's recommendations. The GAO stated:

> Improving acquisition management and reducing costs. Implementing four priority recommendations related to federal acquisitions would help agencies improve the management of high-priority information technology (IT) projects and achieve billions of dollars in other potential savings. For instance, the federal government planned to spend nearly $96 billion on IT investments in fiscal year 2018. However, too often these investments have cost overruns and schedule delays. To enhance the oversight of high-priority IT projects, in November 2017 we recommended the Federal Chief Information Officer (CIO) become more directly involved in the oversight of these projects, an approach that improved results and produced significant savings when used in the past.

OMB also identified its recommendations on Category Management as having gone unfilled. OMB stated that:

> Category management is an approach based on industry leading practices to streamline and manage entire categories of spending across government like a single enterprise to leverage the government's buying power. Setting goals and assessing agencies' progress in implementing category management should help OMB hold agencies accountable, reduce contract duplication, and increase cost savings. In October 2016, we made two priority recommendations to use category management for land mobile radio equipment. The Department of Homeland Security is establishing a contract vehicle for this equipment from which all federal agencies can order, and OMB's support of efforts to finalize this contract vehicle and fully implement these recommendations could help agencies reap billions of dollars in potential savings.

The GAO added that OMB has yet to address cybersecurity and technology issues turned up in its biennial High-Risk List: "(1) ensuring cybersecurity of the nation" and "(2) improving management of IT acquisitions and operations."

GAO released a similar list of unmet recommendations it has made to the Department of Homeland Security (DHS), and the agency explained it wanted to highlight those areas "where open recommendations should be given high priority.

GAO identified the following priority recommendations:

- Recommendations: To more fully address the requirements identified in the National Cybersecurity Protection Act of 2014 and the Cybersecurity Act of 2015, we recommended that the Secretary of Homeland Security should:

    - develop metrics for assessing adherence to applicable principles in carrying out statutorily required functions, and
    - establish methods for monitoring the implementation of cybersecurity functions against the principles on an ongoing basis.
- Action Needed: DHS agreed with the recommendations and has taken the initial steps to address them. Specifically, DHS stated that it continues to determine the applicability of key performance indicators and performance targets, which is intended to enable National Cybersecurity and Communications Integration Center (NCCIC) to assess its effectiveness performing cybersecurity functions in adherence of applicable principles. Specifically, the agency stated that it continues to work towards finalizing Mission Essential Functions and Tasks, and continues to refine applicable program-level measures and metrics. Further, DHS said it is continuing to update NCCIC Strategic Objectives that is intended to align and verify each of the center's goals and reestablish performance reviews to ensure mission effectiveness. The target date for completion of these activities is November 2018 and January 2019, respectively.

- Recommendations: To help ensure that DHS effectively complete workforce assessment activities to identify, categorize, and assign codes to its cybersecurity positions, we recommend that the Secretary of Homeland Security should:
    - ensure that the Office of the Chief Human Capital Officer collects complete and accurate data from its components on all filled and vacant cybersecurity positions when it conducts its cybersecurity identification and coding efforts, and
    - develop guidance to assist DHS components in identifying their cybersecurity work categories and specialty areas of critical need that align to the National Initiative for Cybersecurity Education Framework.
- Action Needed: DHS agreed with the recommendations. DHS had plans to issue memorandums that include instructions, guidance, and plans to address these recommendations by periodically reviewing compliance and cybersecurity workforce data concerns with component leads to ensure data accuracy, and disseminating a reporting schedule for identifying cybersecurity critical needs by June 2018. Although DHS has taken some steps towards addressing the recommendations such as developing timeframes and a process for identifying critical needs, it has not yet provided complete evidence that it has fully implemented the recommendations. If implemented, DHS's planned actions would fully address the recommendations.

- Recommendation: The Secretary of Homeland Security, in cooperation with the co-sector-specific agencies as necessary, should take steps to consult with respective sector partner(s), such as the sector coordinating councils, and National Institute of Standards and Technology, as appropriate, to develop methods for determining the level and type of framework adoption by entities across their respective sectors.
- Action Needed: DHS agreed with the recommendations and has taken the initial steps to address them. The agency stated it has continued to promote the Framework and gather feedback on Framework use among its critical infrastructure stakeholders. Specifically, DHS stated it has hosted outreach and awareness engagements, including webinars, road shows, conferences, briefings, and regular working group meetings to help organizations understand and use the Framework. Further, DHS stated it has taken steps to determine usage amongst members of the Information Technology Sector. For example, agency officials stated they are collaborating with the Information Technology Sector Coordinating Council (SCC) Small and Midsize Business (SMB) Working Group in a coordinated effort

> between government and industry to evaluate Framework use and promote continued adoption within the broader Information Technology SMB community. DHS stated that following Office of Management and Budget approval, the Information Technology Sector will administer the SMB Cybersecurity Survey and the DHS Information Technology SCC SMB Working Group will create a formal deliverable for the Information Technology SMB Community. However, DHS has yet to provide evidence regarding efforts to coordinate with the other sectors for which it serves as the sector lead. DHS needs to address Framework adoption in its other sectors. In addition, if the results of the survey yield a methodology for determining the level and type of use of the Framework, DHS should consider the applicability of taking a similar approach with other sector partners to more adequately satisfy the recommendation.

GAO on Data Center Optimization

In a report requested by four committees, the Government Accountability Office (GAO) provided its most recent annual report on the federal government's efforts to consolidate and make more efficient its use of data centers. As has happened annually, the GAO found that the Office of Management and Budget's (OMB) Data Center Optimization Initiative (DCOI) "reported mixed progress toward achieving OMB's goals for closing data centers and realizing the associated savings by September 2018." Additionally, the GAO determined that "agencies reported limited progress against OMB's five data center optimization targets for server utilization and automated monitoring, energy metering, power usage effectiveness, facility utilization, and virtualization."

The Senate Armed Services Homeland Security and Governmental Affairs Committees and the House Armed Services and Oversight and Reform Committees requested this report, and considering they were the committees that folded the "Federal Information Technology Acquisition Reform Act" (FITARA) into the "Carl Levin and Howard P. 'Buck' McKeon National Defense Authorization Act (NDAA) for Fiscal Year 2015" (P.L. 113-239), it is possible that this report could give rise to new language in this year's NDAA. FITARA codified and expanded the Obama Administration's Federal Data Center Consolidation Initiative (FDCCI). In late November 2018, the Trump Administration proposed changes to the DCOI in its draft memorandum, "Data Center Optimization Initiative," in part, because Congress extended the sunset for the DCOI provisions in FITARA from FY 2018 to FY 2020.

The GAO noted that

> Federal data center consolidation efforts have been underway since 2010 and OMB's fiscal year 2018 targets provided clear and transparent goals that helped define the tangible benefits that DCOI was expected to provide. However, most agencies continue to report mixed progress against those targets. Although agencies have taken action to close about half of the data centers in their combined inventories, 11 agencies did not plan to meet all of their closure targets.

Regarding data center closures and associated savings and data center optimization, the GAO stated that

- As of August 2018, 13 agencies reported that they had met, or had plans to meet, all of their OMB-assigned closure goals by the deadline. However, 11 agencies reported that they did not have plans to meet their goals. Further, 16 agencies reported that, as of August 2018, they had met, or planned to meet, their cost savings targets, for a total of $2.36

billion in cost savings for fiscal years 2016 through 2018…about $0.38 billion less than OMB's DCOI savings goal of $2.7 billion.

- [T]he 24 agencies reported limited progress against OMB's five data center optimization targets for server utilization and automated monitoring, energy metering, power usage effectiveness, facility utilization, and virtualization. As of August 2018, the agencies reported that 3 had met three targets, 9 had met one target, and 10 met none of the targets. Two agencies did not have a basis to report on progress as they do not own any data centers. Further, as of August 2018, 20 agencies did not plan to meet all of OMB's fiscal year 2018 optimization goals. Specifically, only 2 agencies reported plans to meet all applicable targets; 6 reported that they did not plan to meet any of the targets

The GAO did find some success in the DCOI. The GAO stated

> Although many agencies have struggled to meet their individual DCOI targets, other agencies have successfully met OMB's goals for data center closures, savings, and optimization. Six such agencies that we identified reported on the importance of gathering leadership support, effective communication, and alignment with the core tenets of DCOI. Key practices such as these can play an important role in helping agencies better meet the overall goals and mission of DCOI.

In May 2018, GAO found "mixed progress" with fewer data centers closed and less savings realized than originally projected. GAO did not, however, offer any recommendations because OMB is currently talking to agencies about revising their goals and so many of the GAO's recommendations in previous assessments remain unacted upon.

OMB Looks To Reform "Shared Services"

The Office of Budget and Management (OMB) has released a memorandum that proposes to change how the federal government will buy certain core services that almost all agencies use (e.g. human resources). This revamp of the Shared Services initiative is a part of the President's Management Agenda (PMA) and is closely related in spirit to the Category Management initiative the Trump Administration also reformed a few weeks ago. In relevant part, if implemented as planned, federal agencies may look to the Department of Homeland Security for buying cybersecurity services as opposed to each agency buying its own. All Chief Financial Officers Act agencies would be subject to this memorandum, meaning independent agencies are excluded (e.g. the SEC or FTC), but the Department of Defense is included.

Of course, there is a process under which an agency could make the case that the shared service they might normally expected to buy does not meet their particular needs. And, as with all government-wide initiatives, the key will be in follow through from OMB in enforcing the new regime and buy-in at the top of agencies and among key personnel in components, for, as we have seen, without these, these changes, like many other recent changes to acquisition practices, will likely affect marginal changes.

OMB explained that "[t]his memorandum is a strategy based on industry experiences, and lessons learned from other central governments that will reduce duplication, improve accountability, and improve Federal shared services." OMB claimed that "[t]his updated strategy will enable the delivery of an innovative, flexible, and competitive set of solutions and services."

OMB stated that "[t]his memorandum:

- Describes the process and desired outcomes for shared services;
- Establishes a process for designating agencies as Quality Services Management Offices (QSMOs);
- Establishes the governance and accountability model that will be used to engage customers and enable QSMO performance excellence, including the Shared Services Governance Board (SSGB) and the Business Standards Council (BSC);
- Requests that all CFO Act agencies appoint a Senior Accountable Point of Contact (SAPOC) to coordinate actions across the agency to support adoption of the shared service strategies; and
- Rescinds previous OMB memoranda that are no longer aligned to this strategy.

OMB stated that "[i]mmediate implementation of this strategy requires the Government to define and execute an integrated approach to shared services including:

1. Developing inter-agency standards and priorities for shared services;
2. Creating centralized capabilities, shared governance, and performance expectations; and
3. Continuing to expedite the adoption of existing quality services that currently perform well and provide demonstrated value to agency customers.

OMB stated that "[o]nce an opportunity for centralization or sharing is identified, OMB will designate a lead agency as the QSMO to take responsibility for establishing and/or managing such capabilities." OMB noted that "[t]he Government's current shared services model relies on a network of legacy providers (designated or self-selected) to deliver specific shared services...[and] [a]s QSMOs become operational, there may be technology or services that are beneficial for legacy providers to continue offering to agencies for a finite period." In this case, the agency would need to clear the use of legacy services with OMB. The memorandum also details a process under which an agency might "issue new solicitations for new or modernized technology or services" outside the new shared service (e.g. human resources IT), and the agency must make the business case approved by a number of stakeholders in the agency and OMB.

OMB stated that "[o]ne of the PMA's primary focus areas centers on the Sharing Quality Services Cross Agency Priority Goal (CAP Goal) and improvements to Government mission-support services, enabling the delivery of high-quality outcomes to the American people." OMB asserted that "[i]n the past, agencies took steps to consolidate common mission-support functions internally, and in some cases, to leverage common technology or services offered by other agencies." OMB stated that "[t]he Government endeavors to utilize lessons from previous successes and failures to provide a new, enhanced strategic blueprint for sharing quality services within the Federal enterprise…[and] [i]n addition to improving service quality and performance, private sector experience suggests the potential for significant productivity gains and cost savings over time. " OMB claimed that this intiative has the potential to "realize financial benefits by as much as 5-30 percent" and "[c]ommon mission-support services such as processing hiring transactions or managing Federal finances, travel, and payroll costs taxpayers more than $25 billion annually."

In the April 2019 update on the Sharing Quality Services CAP Goal, the team working on this initiative, and one of the first shared services they intend to revamp is "Cybersecurity Services." As mentioned earlier, DHS will be the lead (i.e. the QMSO) and they will work with the Office of the Federal Chief Information Officer on this initiative. Cybersecurity Services are defined as:

> Network Defense, Vulnerability Management, Security Operations, Incident Management, Threat Intelligence, Enterprise Intrusion Detection/Prevention, Cyber Supply Chain Risk Management, DNS Services, Hardware/Software Asset Management, Digital Identity and Access Management, Data Protection, Mobile Security Services.

Incidentally, Federal Chief Information Officer Suzette Kent and General Services Administration (GSA) Administrator Emily Murphy are the leads for this CAP Goal.

In March 2019, the Government Accountability Office (GAO) evaluated OMB and GSA's "previous shared services initiatives for HR and financial management activities" and the 10-year, $2.5 billion NewPay agreement awarded to two commercial teams to provide payroll, and work schedule and leave management services using Software-as-a-Service." GAO's report "(1) identifie[d] the progress and challenges associated with federal shared services initiatives for selected HR and financial management activities, and (2) assesse[d] OMB and GSA's actions to address those challenges." GAO noted that "for more than two decades, the federal government has taken actions aimed at increasing agencies' use of shared services…[and] [w]hen properly implemented, a shared services model for HR and financial management activities has the potential to help the federal government cut costs and modernize aging IT systems." GAO noted that "there have also been persistent governance and marketplace challenges that have impeded more widespread adoption of shared services."

The GAO found that "OMB and GSA do not have a plan to monitor NewPay's implementation…[and] also have not documented key decision-making roles and responsibilities related to the implementation of NewPay." GAO stated that "[u]ntil they develop a monitoring plan which includes performance goals and milestones, transparent reporting tools, and a process for capturing lessons learned, and documenting key roles, they risk implementation challenges that could cause gaps in service or costly delays." GAO asserted that "OMB and GSA also do not have a process to provide information to customers about provider services, pricing, and performance…[and] [d]eveloping such a process would help minimize the challenges of transitioning to shared services on key stakeholders." GAO stated that "OMB and GSA do not have a process for collecting and tracking cost-savings data…[and] [u]ntil OMB and GSA finalize their plan for collecting the related data and evidence to measure their cost savings goal of an estimated $2 billion over 10 years, they will not be able to determine and report progress made."

In 2016, the United Kingdom's National Audit Office (NAO) found that the British government's "programme to transfer back-office functions to two shared service centres has made savings but has not achieved value for money to date." The NAO stated that

> In 2012, we reported on five central government shared service centres. We found that the government had not achieved value for money and that complex services were tailored too much to individual departments, increasing costs and reducing flexibility. In 2014, we reported on the Cabinet Office's Next Generation Shared Services strategy (the Strategy). This involved creating two independent shared service centres to provide back-office functions for up to 14 departments and their arm's-length bodies.

Further Reading

"Who Owns Huawei? The Company Tried to Explain. It Got Complicated." – *The New York Times*
"Classified data key to new acquisition approach, Federal CISO says" – *cyberscoop*

"Made in China, Exported to the World: The Surveillance State" – *The New York Times*
"NSA Recommends Dropping Phone-Surveillance Program" – *The Wall Street Journal*
"Amazon's Alexa Team Can Access Users' Home Addresses" – *Bloomberg*
"May to ban Huawei from providing 'core' parts of UK 5G network" – *The Guardian*
"How Nest, designed to keep intruders out of people's homes, effectively allowed hackers to get in" – *The Washington Post*