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

EC Evaluates GDPR After One Year

The European Commission (EC) has released its assessment of the General Data Protection Regulation (GDPR or Regulation) after a bit more than a year after the European Union (EU) wide data processing regime took effect. The EC explained that its "preliminary assessment is that the first year of application of the Regulation has been overall positive...[but] further progress is necessary in a number of areas." The EC explained that it is "tak[ing] stock of the results achieved so far as in relation to the consistent implementation of the data protection rules across the EU, the functioning of the new governance system, the impact on citizens and businesses and the EU's efforts in promoting global convergence of data protection regimes." The EC makes clear in this assessment that the GDPR will tie into current and future EU action on related policy areas such as artificial intelligence, health care, transportation, energy, and others.

The EC placed the GDPR "at the centre of a coherent and modernised EU data protection landscape that also includes the Data Protection Law Enforcement Directive and the Data Protection Regulation for EU institutions and bodies." The EC added that "[t]his framework is to be completed by the [draft] e-Privacy Regulation which is currently in the legislative process." The EC claimed that "[s]trong data protection rules are essential to guarantee the fundamental right to the protection of personal data...[and] are central to a democratic society and an important component of an increasingly data-driven economy." The EC stated that "[t]he EU aspires to seize the many opportunities that the digital transformation offers in terms of services, jobs and innovation, while at the same time tackling the challenges these bring." The EC stated that "[m]any countries have adopted or are in the process of adopting comprehensive data protection rules based on principles similar to those of the Regulation, resulting in a global convergence of data protection rules." The EC claimed that "[t]his offers new opportunities to facilitate data flows, between commercial operators or public authorities, while improving the level of protection for the personal data in the EU and across the globe."

In terms of compliance, the EC claimed that "[w]hile companies report a number of challenges in adjusting to the new rules, many emphasise that it was also an opportunity to bring the issue of data protection to the attention of the company boards, put their house in order in terms of the data they hold, improve security, be better prepared for incidents, reduce exposure to unnecessary risks and build more trusting relationships with their customers and commercial partners." The EC asserted that "[o]n transparency, business and civil society organisations mention the delicate balance to be struck between giving to individuals all required information under the Regulation while also using clear and plain language and a form that individuals can understand...[and] [o]perators are developing innovative solutions in this direction." The EC stated that "[i]n general, businesses indicated that they were able to implement the new data subject rights, although it was sometimes challenging to meet deadlines due to an increased number of requests and their more wide-ranging character, or to check the identity of the person making the request."

The EC stated that "[c]ontrary to fears expressed by some stakeholders before May 2018, national data protection authorities have adopted a balanced approach to enforcement powers." The EC claimed that national data protection authorities "have focused on dialogue rather than sanctions,

in particular for the smallest operators which do not process personal data as a core activity...[and] [a]t the same time, they did not shy away from using their new powers effectively whenever this was necessary, including by launching investigations in the area of social media and imposing administrative fines ranging from a few thousand euros to several million, depending on the gravity of the infringements of data protection rules."

The EC stated that "[t]he EU data protection legislative framework is a cornerstone of the European human-centric approach to innovation...[and] is becoming part of the regulatory floor for a widening range of policies including health and research, artificial intelligence, transport, energy, competition and law enforcement." The EC claimed that "a lot of progress had been made...although more work is certainly needed for the Regulation to become fully operational."

EU Doubts Whether EU Entities Can Comply With U.S. Law

Two key regulatory bodies of the European Union (EU) have released a joint initial legal assessment of the "Clarifying Lawful Overseas Use of Data (CLOUD) Act" (P.L. 115–141) and how it might run afoul of the General Data Protection Regulation (GDPR) and other EU regulations or directives controlling the storage, processing, and sharing of the personal data of EU citizens. Generally speaking, the EU's European Data Protection Board (EDPB) and the European Data Protection Supervisor (EDPS) highlight what they consider a number of problems with this new U.S. legal regime that permits the U.S. to compel the production of data stored outside the U.S. by a service provider that may not be a U.S. entity. Instead of compliance with the CLOUD Act, the EDPB and EDPS articulated their position that "an international agreement containing strong procedural and substantive fundamental rights safeguards appears the most appropriate instrument to ensure the necessary level of protection for EU data subjects and legal certainty for businesses." It also bears noting that neither the EDPB and the EDPS lack the authority to direct data controllers, data protection authorities, or EU nations to follow this legal assessment. Rather the opinions of both entities are advisory in nature even though they are often very persuasive and even considered authoritative.

The CLOUD Act was impelled forward in large part by the Supreme Court case, the *United States v. Microsoft*, in which the U.S. Department of Justice wanted Microsoft to hand over the email of a U.S. national that were being stored on servers in Ireland as part of a criminal investigation. In concert with stakeholders and the Obama Administration, Congress sought a legislative solution, which was ultimately tacked onto the FY 2018 omnibus appropriations act and enacted. The EDPB and EDPS characterized the CLOUD Act thusly: the statute that "according to US law, US authorities have the right to require the production of data stored abroad by a service provider subject to US jurisdiction." However, the EDPB and EDPS noted that the "CLOUD Act therefore entails the possibility that such electronic communication or remote computer service providers are compelled to answer a request by US law enforcement authorities for the disclosure of personal data that are subject to the provisions of the GDPR." The EDPB added in a footnote "that, in most cases, where request from a US court or authority which, by virtue of the CLOUD Act, would require the disclosure of personal data that are subject to the GDPR, such personal data being in possession, custody, or control of a provider of electronic communication service or remote computing service is likely to be subject to the provisions of Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector."

The EDPB and EDPS asserted that "[i]n the absence of such framework provided by an international agreement (such as the EU US MLAT or a MLAT between a Member State and the US in the context

of a US CLOUD Act request) or another legal basis under the GDPR, service providers subject to EU law cannot legally base the disclosure and transfer of personal data to the US on such requests." The EDPB but not the EDPS reiterated "its position expressed in its guidelines on Article 49 GDPR that: "In situations where there is an international agreement such as a mutual legal assistance treaty (MLAT), EU companies should generally refuse direct requests and refer the requesting third country authority to an existing mutual legal assistance treaty or agreement." The EDPB and EDPS stated that "we consider that where disclosure of personal data is compelled by a third-country authority, the MLAT process must ensure that data is disclosed in compliance with EU law, and under the supervision of the courts in the EU." The agencies also claimed that law enforcement requests for data stored in the EU are not controlled by the EU-US Privacy Shield adequacy decision nor the EU-US Umbrella Agreement. The EDPB and EDPS claimed "that any order under the CLOUD Act for transfer of personal data from the EU could only be lawful if there is a legal basis under Article 6 and Article 49 of the GDPR," neither of which form adequate bases in their analysis. Rather, an MLAT or international agreement would be more appropriate legal vehicles under which U.S. law enforcement agencies would make these sorts of requests of entities subject to U.S. jurisdiction.

The agencies explained that "[w]e wish to recall that this initial assessment is valid in particular in relation to US CLOUD Act requests and we recognise the need for further analysis with regard to the issues raised in this legal assessment." The EDPB and EDPS recommended "to [data] controllers [i.e. entities holding and using the personal data of EU citizens] and competent authorities that they follow this initial assessment in particular in relation to US CLOUD Act requests." As noted above, this assessment does not carry legal force and is rather highly persuasive and influential. Those entities subject to the GDPR would be wise to give it consideration in the event they face a U.S. subpoena or warrant under the CLOUD Act.

The EDPB and EDPS issued this legal analysis of the CLOUD Act at a time when the EU and U.S. are in talks about an international agreement "on cross-border access to electronic evidence for judicial cooperation in criminal matters and negotiating directives." The agencies claimed that "[i]n order to comply with EU primary law, the conclusion of an international agreement must in any case provide for appropriate safeguards for transfers and ensure that enforceable data subject rights and effective legal remedies for data subjects are available." The extent to which EU negotiators press the position of the EDPB and EDPS remains unseen as does the willingness of U.S. negotiators to heed these points. Of course, the CLOUD Act has provisions allowing for and encouraging "executive agreements" between the U.S. and other nations to streamline the process by which a signatory of the agreement could use a process to access data held in the the other signatory's country.

Not surprisingly, the Trump Administration holds a different view of the CLOUD Act. In an April 2019 white paper on the "Purpose and Impact" of the statute, the Department of Justice (DOJ) claimed

> The CLOUD Act thus represents a new paradigm: an efficient, privacy and civil liberties-protective approach to ensure effective access to electronic data that lies beyond a requesting country's reach due to the revolution in electronic communications, recent innovations in the way global technology companies configure their systems, and the legacy of 20th century legal frameworks.

The DOJ concluded that "[a] framework of executive agreements among rights-respecting countries under the CLOUD Act will support those countries' efforts to investigate serious crime—efforts that are vital to protecting our societies and keeping our citizens safe."

GAO Faults Federal Cybersecurity…Again

The Government Accountability Office (GAO) released an assessment of the civilian agencies' cybersecurity risk management programs and found them all lacking in at least one key metric and a number of agencies lacking in a number of key metrics. The GAO's findings are not novel or unprecedented, and, again, to no great surprise, the GAO concluded that "agencies will face an increased risk of cyber- based incidents that threaten national security and personal privacy" unless they address the issues turned up in the report. However, this is one of the GAO's first assessments of government-wide cybersecurity after most, if not all, of the tasks spelled out in the May 2017 Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure, Executive Order 13800, have been completed. Yet, many of the key practices the GAO found many agencies have not put in place predate the executive order (e.g. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-39) and have been agency responsibilities for years. Ultimately, the GAO made "57 recommendations to the 23 agencies and one to Office of Management and Budget (OMB), in coordination with Department of Homeland Security (DHS), to assist agencies in addressing challenges."

The GAO looked at 23 of the 24 Chief Financial Officers Act agencies with the Department of Defense being excluded because of the classified nature of much of its cybersecurity measures. The GAO were asked to review the following:

> (1) the extent to which agencies established key elements of a cybersecurity risk management program;
> (2) what challenges, if any, agencies identified in developing and implementing cybersecurity risk management programs; and
> (3) what steps the OMB and DHS have taken to meet their risk management responsibilities under Executive Order (EO) 13800 and to address any challenges agencies face in implementing cybersecurity risk management practices.

The GAO stated that "[k]ey practices for establishing an agency-wide cybersecurity risk management program include designating a cybersecurity risk executive, developing a risk management strategy and policies to facilitate risk-based decisions, assessing cyber risks to the agency, and establishing coordination with the agency's enterprise risk management (ERM) program." The GAO found that while almost all the 23 agencies had designated a risk executive, "they often did not fully incorporate other key practices in their programs:

- Twenty-two agencies established the role of cybersecurity risk executive, to provide agency-wide management and oversight of risk management.
- Sixteen agencies have not fully established a cybersecurity risk management strategy to delineate the boundaries for risk-based decisions.
- Seventeen agencies have not fully established agency- and system-level policies for assessing, responding to, and monitoring risk.
- Eleven agencies have not fully established a process for assessing agency- wide cybersecurity risks based on an aggregation of system-level risks.
- Thirteen agencies have not fully established a process for coordinating between their cybersecurity and ERM programs for managing all major risks.

In terms of its overall assessment, the GAO noted that "without developing an agency-wide cybersecurity risk management strategy, agencies may lack a consistent approach to managing cybersecurity risks." The GAO added that "without a process for an agency-wide cybersecurity risk assessment, agencies may be missing opportunities to identify risks that affect their entire organization, and to implement solutions to address them." The GAO further claimed that "establishing processes for coordinating cybersecurity risk information with the entity responsible for enterprise risk management would help ensure that cyber risks are being considered by senior leadership in the context of other risks facing the agency." The GAO explained that "OMB and DHS did not establish initiatives to address the other challenges on managing conflicting priorities, establishing and implementing consistent policies, developing risk management strategies, and incorporating cyber risks into ERM...[and] [w]ithout additional guidance or assistance to mitigate these challenges, agencies will likely continue to be hindered in managing cybersecurity risks."

GAO recommended that OMB "should, in coordination with the [DHS], establish guidance or other means to facilitate the sharing of successful approaches for agencies to address challenges in the areas of

> (1) managing competing priorities between cybersecurity and operations, such as when operational needs appear to conflict with cybersecurity requirements;
> (2) implementing consistent cybersecurity risk management policies and procedures across an agency;
> (3) incorporating cyber risks into enterprise risk management, and
> (4) establishing agencies' cybersecurity risk management strategies. (Recommendation 1)

The GAO is "also making a total of 57 recommendations to the 23 civilian CFO Act agencies in our review to fully address key practices in their cybersecurity risk management policies and procedures."

OMB possesses much if not all the legal authority needed to implement the GAO's recommendations and then ensuring that the agencies actually put in place policies to meet these recommendations. The GAO conceded that "[c]larified or updated guidance, along with sharing successful practices or lessons learned, could help agencies more fully establish their cybersecurity risk management capacity." The key question is whether the OMB will do so given that OMB may have priorities that are perceived to be higher priority. As we often note in email and on calls whenever the White House or OMB rolls out a new cybersecurity initiative, implementation and follow through will ultimately determine the success of those GAO recommendations the Administration opts to implement. In a related vein, the agencies could, by their own initiative, make the changes recommended by GAO. Yet, this would require consistency and focus on cybersecurity from leadership at the top of the agency that has been lacking even during Administrations with less churn than the Trump Administration.

However, the GAO's follow up in reiterating its findings to Congress and in future reports will likely spur some action from OMB, DHS, and the agencies themselves and possible Congressional action. The report was requested by Senate Homeland Security Committee Chair Ron Johnson (R-WI), former committee chairs Tom Carper (D-DE) and Susan Collins (R-ME), and House Oversight and Reform Committee Chair Elijah Cummings (D-MD) and Ranking Member Jim Jordan (R-OH), and they may propose a legislative response either in the form of report language in an appropriations bill or standalone legislation with the latter being less likely given that many of the key practices

agencies are not following were put in place under general or specific grants of authority to OMB and DHS.

DOD OIG Finds Major Vulnerabilities in Both Commercial IT The Pentagon Buys and Its Processes For Evaluating These Risks

The Department of Defense's (DOD) Inspector General (IG) released an audit of "whether the DOD assessed and mitigated cybersecurity risks when purchasing commercial off-the-shelf (COTS) information technology items." The IG focused mostly on Government purchase card (GPC) purchases but also examined "risks affecting traditional acquisition processes." The IG found that "the DOD purchased and used COTS information technology items with known cybersecurity risks...[and] [s]pecifically, Army and Air Force GPC holders purchased at least $32.8 million of COTS information technology items, such as Lenovo computers, Lexmark printers, and GoPro cameras, with known cybersecurity vulnerabilities in FY 2018." The IG asserted that "[i]f the DOD continues to purchase and use COTS information technology items without identifying, assessing, and mitigating the known vulnerabilities associated with COTS information technology items, missions critical to national security could be compromised." The IG made further findings that have been redacted.

The IG stated that "[t]he DOD purchased and used COTS information technology items with commonly known cybersecurity risks because the DOD did not establish:

- responsibility for an organization or group to develop a strategy to manage the cybersecurity risks of COTS information technology items;
- acquisition policies that proactively address the cybersecurity risks of COTS information technology items;
- an approved products list to prevent unsecure items from being purchased; and
- controls to prevent the purchase of high-risk COTS information technology items with known cybersecurity risks similar to the controls implemented through the use of the national security systems-restricted list.

The IG noted that "[f]ederal agencies have reported cybersecurity risks associated with using COTS information technology items, such as:

- third-party service providers and manufacturers with physical or logical access to sensitive Government information systems, software code, or intellectual property;
- poor personnel information security practices, such as using applications on mobile devices that provide the location of troops or ongoing DOD operations;
- counterfeit software or hardware with embedded malware, such as viruses or malicious code, that could allow adversaries remote access to DOD systems and networks; and
- a contractor's inability to protect data and mitigate vulnerabilities on systems and networks that store and transmit sensitive information.

The IG stated that "[c]omponents of COTS information technology items, such as hardware, firmware, and software, can come from globally distributed supply chains that are complex and limit the purchaser's understanding and control over how the components of COTS information technology items are developed, integrated, and deployed. The IG stated that "[a]ccording to the Committee on National Security Systems, adversaries and malicious actors use the supply chain to introduce cybersecurity vulnerabilities into DOD weapon systems and information technology networks that use COTS information technology products."

The IG took the DOD to task for buying Lenovo "despite known cybersecurity risks." The IG noted that "Lenovo is the largest computer company in China...[and] Congress and the Department of Homeland Security, among other Government agencies, have issued multiple warnings about the cybersecurity risks of using Lenovo products." The IG conceded that "[i]n 2018, 12 years after the State Department ban, the DOD ordered an operational risk assessment of Lenovo products throughout the DOD Information Network to identify and understand the risks Lenovo products posed to the network." The IG also pointed out that "[i]n the meantime, the Army purchased another 195 Lenovo products, totaling just under $268,000, and the Air Force purchased 1,378 Lenovo products for $1.9 million in FY 2018."

The IG made the following unclassified recommendations:

> We recommend that the Secretary of Defense direct an organization or group to develop a:
>
> > a. Risk-based approach to prioritize commercial off-the-shelf items for further evaluation.
> > b. Process to test high-risk commercial off-the-shelf items.
> > c. Process to prohibit the purchase and use of high-risk commercial off-the-shelf items, when necessary, until mitigation strategies can limit the risk to an acceptable level.
>
> We recommend that the Under Secretary of Defense for Acquisition and Sustainment update:
>
> > a. Existing DOD acquisition policies or develop and implement new policy to require organizations to review and evaluate cybersecurity risks, including supply chain and counterintelligence risks, for high-risk commercial off-the-shelf items prior to purchase, regardless of purchase method.
> > b. Government purchase card program policy and training to include training on common cybersecurity risks, including supply chain and counterintelligence risks, for commercial off-the-shelf information technology items and the impact of the risks to the mission.
>
> We recommend that the DOD Chief Information Officer revise DOD Instruction 8100.04, "DOD Unified Capabilities (UC)," December 9, 2010, to require an assessment of supply chain risks as a condition for approval to be included on the Unified Capabilities approved products list.
>
> We recommend that the Under Secretary of Defense for Acquisition and Sustainment and the DOD Chief Information Officer identify and implement administrative solutions, such as expanding the DOD's implementation of its current section 2339a, title 10, United States Code, 2018, authorities and, if those solutions are insufficient to address the issues identified in this report, seek legislative authority to expand the national security system-restricted list DOD-wide to include high-risk commercial off-the-shelf information technology items used for non-national security systems.

Big picture, the IG chose to examine the COTS sold by two Chinese-owned companies, Lenovo and Lexmark, and to stress that parts sourced from other countries can and do compromise the cybersecurity of the DOD's COTS. In other words, the IG all but focused on Chinese goods and components being used by the DOD. Given that the IG found a lack of DOD-wide policies to address the cybersecurity of COTS before they are bought, it is pretty easy to see Congress folding language into an NDAA, requiring that this and other recommendations made in this report and others be implemented. This IG report may impact the Section 846 Procurement Through Commercial e-Commerce Portals program that the General Services Administration (GSA) and the

Office of Management and Budget (OMB) have begun the process of piloting. In the Phase 2 report, GSA and OMB were ambivalent on the cybersecurity of COTS, and the agencies contended that "[w]hile all commercial e-commerce portal provider RFI responders indicated they have robust cybersecurity practices and solutions, few were willing to publicly share their proprietary capabilities—therefore the specific details of how commercial e-commerce portal providers will meet the stated protection needs will be fleshed out during the acquisition for the initial proof of concept."

GAO Finds Faulty Federal Information Security

As part of its responsibilities under the "Federal Information Security Modernization Act of 2014" (FISMA) (P.L. 113-283), the Government Accountability Office (GAO) has released an assessment of how well federal agencies have discharged their information security responsibilities and how well the Office of Management and Budget (OMB), Department of Homeland Security (DHS), and National Institute of Standards and Technology (NIST) have executed their responsibilities to help agencies. The answer, to no great surprise, is so-so, at best. GAO notably stressed that OMB failed to submit its annual FISMA report to Congress which was due on March 1 and has radically cut back on the number of Cyberstat meetings as compared to the Obama Administration. The report was sent to the committees of jurisdiction, Senate Homeland Security and House Oversight and Reform, either of whom presumably could press the Administration to address the recommendations GAO is making.

The GAO stated that "[d]uring fiscal year 2018, many federal agencies were often not adequately or effectively implementing their information security policies and practices." The GAO claimed that "most of the 16 agencies GAO selected for review had deficiencies related to implementing the eight elements of an agency-wide information security program required by the FISMA." The GAO added that "inspectors general (IGs) reported that 18 of the 24 Chief Financial Officers (CFO) Act of 1990 agencies did not have effective agency-wide information security programs." The GAO noted that it and the "IGs have previously made numerous recommendations to agencies to address such deficiencies, but many of these recommendations remain unimplemented." However, the GAO also found that "[w]ith certain exceptions, OMB, DHS, and NIST "were generally implementing their government-wide FISMA requirements, including issuing guidance and implementing programs that are intended to improve agencies' information security."

The GAO noted that OMB missed the March 1 deadline for submitting its annual FISMA report to Congress that should include the following:

- a summary of incidents described in the agencies' annual reports;
- a description of the threshold for reporting major information security incidents;
- a summary of results from the annual IG evaluations of each agency's information security program and practices;
- an assessment of each agency's compliance with NIST information security standards; and
- an assessment of agency compliance with OMB data breach notification policies and procedures.

OMB claimed the FISMA report is five months late because of the 35-day government shutdown earlier this year and could not commit to a date as to when this statutorily required report will be submitted to Congress.

As you likely recall, "CyberStats are evidence-based meetings led by OMB to ensure agencies are accountable for their cybersecurity posture, while at the same time assisting them in developing targeted, tactical actions to deliver desired results" according to an Obama Administration memorandum. Cyberstat is not a statutorily authorized program; rather it was started under OMB's existing powers in 2011 and thereafter expanded. However, the use of Cyberstat meetings to drive information security meetings at agencies peaked at 24 such meetings in FY 2016, fell to five in FY 2017, dropped further to three in FY 2018, and at the time this report was drafted, OMB has held no Cyberstat meetings in FY 2019. However, OMB and DHS touted "updates to the CyberStat process" starting in FY 2017 that "resulted in extended engagements between DHS, OMB, and the agencies that lasted 4 to 6 weeks or more." GAO asserted that "[b]y conducting fewer CyberStat engagements with agencies, OMB loses an opportunity to assist agencies with improving their information security posture...[and] will limit its ability to oversee specific agency efforts to provide information security protections for federal information and information systems."

GAO also flagged the lack of metrics for OIGs to gauge how well agencies develop and maintain system security plans. The GAO cautioned that "[u]ntil such a metric is developed and reported on, OMB will not have reasonable assurance that inspectors general evaluations appropriately address each of the required elements of an information security program."

GAO recommended the following to OMB:

- The Director of OMB should submit the statutorily required report to Congress on the effectiveness of agencies' information security policies and practices during the preceding year. (Recommendation 1)
- The Director of OMB should expand its coordination of CyberStat review meetings for those agencies with a demonstrated need for assistance in implementing information security. (Recommendation 2)
- The Director of OMB should collaborate with CIGIE to ensure that the inspector general reporting metrics include the FISMA-required information security program element for system security plans. (Recommendation 3)

As always, it is unclear whether OMB will implement the GAO's recommendations and then how extensive the follow through will be.

Five Eyes Call For Greater Cooperation From Tech On Encryption

Minsters from the Five Eyes intelligence alliance met recently in London and articulated their agreement on a number of technology-related issues. In the communiques the Five Eyes ministers released after the completion of the meetings, they detailed these areas of shared concern, and most notably, they reiterated the concerns that the U.S., Australia, and other nations have explained regarding the prevalence of default encryption on applications and devices. In fact, a recent statute enacted in Australia will allow national security and domestic law enforcement agencies to request and ultimately require technology companies and individuals assist in revealing the contents of their devices.

In one of the communiques, the Five Eyes ministers asserted that

> We are concerned where companies deliberately design their systems in a way that precludes any form of access to content, even in cases of the most serious crimes. This approach puts citizens and society at risk by severely eroding a company's ability to

> identify and respond to the most harmful illegal content, such as child sexual exploitation and abuse, terrorist and extremist material and foreign adversaries' attempts to undermine democratic values and institutions, as well as law enforcement agencies' ability to investigate serious crime.

The five nations contended that "[t]ech companies should include mechanisms in the design of their encrypted products and services whereby governments, acting with appropriate legal authority, can obtain access to data in a readable and usable format." The Five Eyes also claimed that "[t]hose companies should also embed the safety of their users in their system designs, enabling them to take action against illegal content…[and] [a]s part of this, companies and Governments must work together to ensure that the implications of changes to their services are well understood and that those changes do not compromise public safety."

The Five Eyes applauded "approaches like Mark Zuckerberg's public commitment to consulting Governments on Facebook's recent proposals to apply end-to-end encryption to its messaging services…[and] [t]hese engagements must be substantive and genuinely influence design decisions."

The Five Eyes added

> We share concerns raised internationally, inside and outside of government, about the impact these changes could have on protecting our most vulnerable citizens, including children, from harm. More broadly, we call for detailed engagement between governments, tech companies, and other stakeholders to examine how proposals of this type can be implemented without negatively impacting user safety, while protecting cyber security and user privacy, including the privacy of victims.

However, one of the Five Eyes nations has already taken legislative action to force technology companies and individuals cooperate with law enforcement investigations. In December 2018, Australia enacted the "Telecommunications and Other Legislation (Assistance and Access) Act 2018"

In an explanatory memorandum, the Parliament explained that the Assistance and Access Act "will enhance cooperation by introducing a new framework for industry assistance, including new powers to secure assistance from key companies in the communications supply chain both within and outside Australia." The Parliament stated that "[i]t will also strengthen agencies' ability to adapt to a digital environment characterised by encryption by enhancing agencies' collection capabilities such as computer access…[to] enable domestic law enforcement agencies to better assist international law enforcement partners by undertaking these powers on behalf of those partners where approved through Australia's mutual assistance framework."

However, the Australian Lawyers for Human Rights argued

> Australia is proposing legislation that would allow covert installation by government of programmes that are effectively malware into Australians' computers and phones and would penalise people who refuse to give the government their passwords with imprisonment for 10 years or 600 penalty units (being over $120,000) or both irrespective of whether or not any harm was involved.

In May, Australia's Department of Home Affairs issued a release entitled "Myths about the Assistance and Access Act" in which it argued that the new statute "creates a pathway for industry

to deliver assistance to law enforcement and intelligence agencies where necessary." The Department claimed that "[i]t does not allow for mass surveillance, the creation of decryption capabilities, the implementation of so-called 'backdoors' or the issuing of 'secret notices' on employees of communications providers." The Department asserted that "[t]he Assistance and Access Act is focused on seeking help from corporate entities that are critical to the supply of communications services and devices in Australia…[and] does not discriminate between foreign and Australian companies conducting business offshore or place obligations on persons by virtue of their Australian citizenship."

Further Reading

"White House drafting executive order to tackle Silicon Valley's alleged anti-conservative bias" – *Politico*
"Democrats stump for election security, blast McConnell at hacker conference" – *Politico*
"For the sake of the economy, California legislators must fix the flawed California Consumer Privacy Act" – *CalMatters*
"U.S. Holds Off on Huawei Licenses as China Halts Crop-Buying" – *Bloomberg*
"FBI Surveillance Proposal Sets Up Clash With Facebook" – *The Wall Street Journal*
"U.S. Holds Off on Huawei Licenses as China Halts Crop-Buying" – *Bloomberg*
"Lawmakers jump-start talks on privacy bill" – *The Hill*
"Revealed: Microsoft Contractors Are Listening to Some Skype Calls" – *Motherboard*
"Apple stands in the global antitrust crosshairs" – *Politico*
"Google and Amazon list gun accessories for sale, in apparent violation of their own policies" – *The Washington Posti*