Technology Policy Update
30 January 2020
By Michael Kans, Esq.

Privacy Bill Revived and Revised in Washington State

The Washington state legislature is again trying to pass privacy legislation after an effort to do so last session fell short. If passed, this would constitute the second major privacy and data security bill enacted in the U.S. after the "California Consumer Privacy Act" (CCPA) (AB 375) and the revised bill contains significant differences from California's now effective privacy regime. The "Washington Privacy Act" (SB 6281) generally provides protections and limits on how the personal data of Washington residents can be collected, processed, and disclosed and would apply to many companies in Washington state or doing business in the state.

Last week, the Senate Environment, Energy & Technology marked up and reported out the "Washington Privacy Act" (here are the links for the hearing agenda, documents, and video.) It is unclear whether this effort will succeed whereas last year's bill stalled in the legislature largely over provisions on facial recognition technology. Nonetheless, some of the same key stakeholders in the legislature who pushed for privacy and data security legislation are again trying to get a bill enacted even though this year's legislative session is only 60 days long.

According to the "Bill Report," SB 6281:

- Provides Washington residents with the consumer personal data rights of access, correction, deletion, data portability, and opt out of the processing of personal data for specified purposes.
- Specifies the thresholds a business must satisfy for the requirements set forth in this act to apply.
- Identifies certain controller responsibilities such as transparency, purpose specification, and data minimization.
- Requires controllers to conduct data protection assessments under certain conditions.
- Authorizes enforcement exclusively by the attorney general.
- Provides a regulatory framework for the commercial use of facial recognition services such as testing, training, and disclosure requirements.

This bill, as currently drafted, would take effect on July 31, 2021, and the intent seems to be that it would become effective 18 months after passage and so this date may be pushed back depending on when it is enacted.

Personal data is defined broadly to include all information that can be linked or can reasonably be linked to a person aside from deidentified data and publicly available information. Undoubtedly, these two exceptions will be interpreted as widely as possible, so they bear further discussion. "Deidentified data" are "data that cannot reasonably be used to infer information about, or otherwise be linked to, an identified or identifiable natural person, or a device linked to such person, provided that the controller that possesses the data:

> (a) Takes reasonable measures to ensure that the data cannot be associated with a natural person;

(b) publicly commits to maintain and use the data only in a deidentified fashion and not attempt to reidentify the data; and
(c) contractually obligates any recipients of the information to comply with all provisions of this subsection."

These deidentification provisions track with language in other federal and state privacy bills, and the inclusion of inference strengthens the standard entities must meet before data are considered deidentified.

And, "publicly available information" is "information that is lawfully made available from federal, state, or local government records." Some states allow the sale or accessing of information provided to the agency that licenses drivers and cars, and if Washington is one of these states, some personal information such as height, weight, ethnicity, and other data could be obtained through this exception.

Like most privacy legislation, there is an even more sensitive set of information. The "Washington Privacy Act" creates a category of "personal data:" "sensitive data," which are:
(a) personal data revealing racial or ethnic origin, religious beliefs, mental or physical health condition or diagnosis, sexual orientation, or citizenship or immigration status;
(b) the processing of genetic or biometric data for the purpose of uniquely identifying a natural person;
(c) the personal data from a known child [defined in the bill as all people 12 years of age and younger]; or
(d) specific geolocation data.

This category of personal data would be subject to extra protection in many but not all instances.

The Washington Privacy Act's definition of process or processing data is very broad and would cover almost all activities undertaken by an entity manipulating data: "any operation or set of operations which are performed on personal data or on sets of personal data, whether or not by automated means, such as the collection, use, storage, disclosure, analysis, deletion, or modification of personal data." Therefore, unlike a number of other bills which discuss collection and processing as separate terms, any such references to processing will encompass all the collection activities of entities covered by the bill.

A final definition to examine. The legislation defines "sale," "sell," or "sold" as "the exchange of personal data for monetary or other valuable consideration by the controller to a third party." The latter phrase is crucial, for many entities do not collect money for disclosing or sharing data but rather receives data in return or other things of value. Consequently, folding into the definition of sale those transactions in which personal data is given to another entity in exchange for something of value would ensure that many data transfers are considered sales. However, a sale would not include the following:
(i) The disclosure of personal data to a processor who processes the personal data on behalf of the controller;
(ii) the disclosure of personal data to a third party with whom the consumer has a direct relationship for purposes of providing a product or service requested by the consumer;
(iii) the disclosure or transfer of personal data to an affiliate of the controller;
(iv) the disclosure of information that the consumer

(A) intentionally made available to the general public via a channel of mass media, and

(B) did not restrict to a specific audience; or

(v) the disclosure or transfer of personal data to a third party as an asset that is part of a merger, acquisition, bankruptcy, or other transaction in which the third party assumes control of all or part of the controller's assets.

Obviously exception (iv) would place outside the definition of sell anything a person transmits from a public account on social media such as Twitter, Facebook, and the like.

Like other privacy bills such as the CCPA, data collection and processing related to employment would be exempt. The definition of "consumer" provides for this exemption but seems to go further in stipulating that Washington state residents "acting in a commercial...context" are also outside the scope of the definition. The definition of consumer is used throughout the bill and is the term upon which a number of the rights, protections, and obligations turn. Therefore, these employment and commercial exemptions may become the avenue by which some argue that their data collection and processing activities are outside the scope of some of the bill's requirements.

Like the General Data Protection Regulation (GDPR), the bill divides those entities covered by its requirements into two groups: controllers and processors. The former are entities that determine the purposes and means of the processing of personal data and the latter are those that process data on behalf of controllers. However, the scope of those controllers and processors subject to the bill hinges on whether the entity has a presence in Washington or is selling products and services to Washington state residents. Moreover, an entity must also satisfy one of two other criteria before they are subject to the law. They must either have collected or processed the personal data of 100,000 or more Washingtonians in a calendar year or earn 50% or more their gross revenue from selling personal data and also control or process the personal data of 25,000 or more people.

Moreover, the bill makes clear that controllers and processors working together will not automatically be deemed liable for the misdeeds of the other should there be alleged violations of the statute. By the same token, when a controller and processor are "involved in the same processing…in violation of this chapter, the liability must be allocated among the parties according to principles of comparative fault." Moreover, the bill requires that "[p]rocessing by a processor shall be governed by a contract between the controller and the processor that is binding on both parties and that sets out the processing instructions to which the processor is bound, including the nature and purpose of the processing, the type of personal data subject to the processing, the duration of the processing, and the obligations and rights of both parties." What's more, a processor and controller may not be held liable for a third party's violations in processing personal data sold by one of the former to the latter "provided that, at the time of disclosing the personal data, the disclosing controller or processor did not have actual knowledge that the recipient intended to commit a violation." It bears noting that "actual knowledge" is a higher standard than a should have known or constructive knowledge standard, opening the possibility that some controllers or processors may sell personal data in situations where a reasonable person would have known that violations by a third-party were likely.

However, a number of entities are carved out of the bill's scope. For example, activities subject to "Health Insurance Portability and Accountability Act" (HIPAA) Gramm-Leach-Bliley, "Fair Credit Reporting Act" (FCRA), or "Family Educational Rights and Privacy Act" (FERPA) regulations are

exempted to the extent they are in compliance. However, a closer read of these provisions suggest that just because an entity may be subject to and compliant with these and other federal privacy statutes does not mean all their data collection and processing activities are exempted. Rather, it appears any such activities outside the scope of those laws may be covered by the Washington state privacy and data security statute.

In terms of new responsibilities for covered entities, controllers must draft and make available "reasonably accessible, clear, and meaningful" privacy notices that inform people of

- The categories of personal data processed by the controller;
- The purposes for which the categories of personal data are processed;
- How and where consumers may exercise the rights...including how a consumer may appeal a controller's action with regard to the consumer's request;
- The categories of personal data that the controller shares with third parties, if any; and
- The categories of third parties, if any, with whom the controller shares personal data.

Controllers would only be allowed to collect the bare minimum of personal data necessary for processing in light of notice provided to people and the activities the controller is undertaking. Generally, a controller "may not process personal data for purposes that are not reasonably necessary to, or compatible with, the purposes for which such personal data are processed, as disclosed to the consumer, unless the controller obtains the consumer's consent."

Controllers would be barred from processing personal data in ways that violate federal and Washington state laws prohibiting discrimination. However, controllers may discriminate with respect to "offering a different price, rate, level, quality, or selection of goods or services to a consumer, including offering goods or services for no fee, if the offering is in connection with a consumer's voluntary participation in a bona fide loyalty, rewards, premium features, discounts, or club card program." There are limits on when and how controllers may sell personal data with third parties (who are defined under the bill to be neither controller, processor, nor a subsidiary of either) unless the sale of personal data is clearly disclosed in the privacy notice, is reasonable necessary "to enable the third party to provide a benefit to which the consumer is entitled," and "the third party uses the personal data only for purposes of facilitating such benefit to which the consumer is entitled and does not retain or otherwise use or disclose the personal data for any other purpose."

And yet, controllers "may not process sensitive data concerning a consumer without obtaining the consumer's consent, or, in the case of the processing of personal data concerning a known child, without obtaining consent from the child's parent or lawful guardian, in accordance with the children's online privacy protection act requirements." As noted earlier, sensitive data include information indicating the race, national origin, sexual orientation, biometric data, and specific geolocation data. And while controllers and processors may not process in ways that violate federal and state law prohibiting discrimination, once consent is fairly obtained from a Washington state resident, they may process in virtually any way short of discrimination.

Finally, people cannot be forced to waive their rights. The Washington Privacy Act makes clear that "[a]ny provision of a contract or agreement of any kind that purports to waive or limit in any way a consumer's rights under this chapter shall be deemed contrary to public policy and shall be void and unenforceable."

As noted, like many privacy bills, there are myriad exceptions to the obligations placed on controllers and processors which do not block either's ability to:

- Comply with federal, state, or local laws, rules, or regulations;
- Comply with a civil, criminal, or regulatory inquiry, investigation, subpoena, or summons by federal, state, local, or other governmental authorities;
- Cooperate with law enforcement agencies concerning conduct or activity that the controller or processor reasonably and in good faith believes may violate federal, state, or local laws, rules, or regulations;
- Investigate, establish, exercise, prepare for, or defend legal claims;
- Provide a product or service specifically requested by a consumer, perform a contract to which the consumer is a party, or take steps at the request of the consumer prior to entering into a contract;
- Protect the vital interests of the consumer or of another natural person; or
- Prevent, detect, protect against, or respond to security incidents, identity theft, fraud, harassment, malicious or deceptive activities, or any illegal activity; preserve the integrity or security of systems; or investigate, report, or prosecute those responsible for any such action;

There are additional carve outs to the standards controllers and processors must meet under the Washington Privacy Act with respect their "ability to collect, use, or retain data" including

- Conducting internal research to improve, repair, or develop products, services, or technology;
- Identifying and repairing technical errors that impair existing or intended functionality; or
- Performing internal operations that are reasonably aligned with the expectations of the consumer based on the consumer's existing relationship with the controller, or are otherwise compatible with processing in furtherance of the provision of a product or service specifically requested by a consumer or the performance of a contract to which the consumer is a party.

Such an exemption may result in the acquisition and processing of personal data against the wishes of people in a number of circumstances given how expansive the conditions under which the normal obligations do not apply.

Nonetheless, the legislature included language to limit processing under an exception and the controller bears the burden of demonstrating that the processing fits an exception.

Moreover, "[c]ontrollers must conduct and document a data protection assessment of each of the following processing activities involving personal data:

- The processing of personal data for purposes of targeted advertising;
- The sale of personal data;
- The processing of personal data for purposes of profiling, where such profiling presents a reasonably foreseeable risk of:
    - Unfair or deceptive treatment of, or disparate impact on, consumers;
    - financial, physical, or reputational injury to consumers;
    - a physical or other intrusion upon the solitude or seclusion, or the private affairs or concerns, of consumers, where such intrusion would be offensive to a reasonable person; or (iv) other substantial injury to consumers;
- The processing of sensitive data; and

- Any processing activities involving personal data that present a heightened risk of harm to consumers."

Controllers would have to keep these on file and then turn them over to the attorney general if requested during an investigation.

Under the "Washington Privacy Act" consumers would be given a number of rights they could exercise by contacting controllers who hold their personal data:

> (1) Right of access. A consumer has the right to confirm whether or not a controller is processing personal data concerning the consumer and access such personal data.
> (2) Right to correction. A consumer has the right to correct inaccurate personal data concerning the consumer, taking into account the nature of the personal data and the purposes of the processing of the personal data.
> (3) Right to deletion. A consumer has the right to delete personal data concerning the consumer.
> (4) Right to data portability. When exercising the right to access personal data pursuant to...a consumer has the right to obtain personal data concerning the consumer, which the consumer previously provided to the controller, in a portable and, to the extent technically feasible, readily usable format that allows the consumer to transmit the data to another controller without hindrance, where the processing is carried out by automated means.
> (5) Right to opt out. A consumer has the right to opt out of the processing of personal data concerning such consumer for purposes of targeted advertising, the sale of personal data, or profiling in furtherance of decisions that produce legal effects concerning a consumer or similarly significant effects concerning a consumer.

The last right bears further elucidation on account of the use of a key phrase: "decisions that produce legal effects concerning a consumer or similarly significant effects concerning a consumer." The bill defines this to mean "decisions that include, but are not limited to, the denial of consequential services or support, such as financial and lending services, housing, insurance, education enrollment, criminal justice, employment opportunities, health care services, and access to basic necessities, such as food and water." These provisions would seem to be aimed at practices deemed "digital redlining" by the Obama Administration top describe practices or policies that would use data collected and processed to discriminate against people on the basis of real or perceived characteristics. Consequently, if an insurance company is processing the personal data of Washington state residents and on the basis of this processing is offering different rates to similarly situated people, a person could opt of the processing on the front, presumably because the controller disclosed these practices in its privacy notice.

Controllers must respond to the individual on the action taken regarding the request within 45 days but they may delay responding for an additional 45 days where "reasonably necessary." There is to be an internal appeals process at the controller for requests that are denied and at a certain point in that process the individual or the controller may inform the state attorney general's office.

However, as with many of the federal privacy bills, there are a number of circumstances under which these, and other consumer rights, do not have to be respected, including but not limited to complying with federal or state law or a government inquiry, protecting the "vital interest" of a person, protecting against fraud or theft and a range of other crimes, and other stated reasons or purposes.

Like an increasing number of federal privacy bills, there are provisions requiring controllers and processors to implement and maintain data security for the personal data being held. Controllers "shall establish, implement, and maintain reasonable administrative, technical, and physical data security practices to protect the confidentiality, integrity, and accessibility of personal data. Such data security practices shall be appropriate to the volume and nature of the personal data at issue." Likewise, processors would need to "[i]mplement and maintain reasonable security procedures and practices to protect personal data, taking into account the context in which the personal data are to be processed." Additionally, processors must "[e]nsure that each person processing the personal data is subject to a duty of confidentiality with respect to the data."

The Washington attorney general alone would be able to enforce the "Washington Privacy Act" as there is no private right of action in the bill for privacy violations and the legislature goes even further to stipulate there is no right to sue for violations under any Washington state law. The attorney general may seek injunctions and civil penalties of up to $7,500 per violation with no limit on the size of a total fine. As with all of the privacy and data security bills, enforcement will drive much of the actions taken by entities subject to the new statute.

While Washington state is not among the most populous states and theoretically the impact of any privacy law would be limited, it is the home of corporate headquarters for both Microsoft and Amazon. Hence, these, and other firms, may decide to adhere to these standards with respect to the privacy of people throughout the U.S. However, this new regulatory structure for privacy would be inconsistent with California's, requiring entities subject to both state's laws to navigate the different standards. Possibly, passage of a second major privacy statute could provide further impetus to Congress to act on privacy legislation that creates a national approach. Moreover, passage of a privacy law in Washington may affect the positions of Washington state lawmakers in the capital, particularly two key stakeholders: Senator Maria Cantwell (D-WA) and Representative Cathy McMorris Rodgers (R-WA) who are the ranking members of the Senate Commerce and House Energy and Commerce's Consumer Protection and Commerce Subcommittee respectively. Both are involved in drafting their committee's privacy bills, and a Washington state statute may affect their positions in much the same the CCPA has informed a number of California Members' position on privacy legislation, especially with respect to bills being seen as weaker than the CCPA.

As noted earlier, the bill also addresses facial recognition technology, a policy area not usually joined to privacy legislation, and sets limits on the use of this new technology. The "Washington Privacy Act" defines "facial recognition service" as "technology that analyzes facial features and is used for the identification, verification, or persistent tracking of consumers in still or video images." Processors that provide these technologies must also make available an application programming interface that would allow researchers to independently access and determine whether the facial recognition technology in question is accurate and fair. Processors must mitigate any negative results. Additionally, "[c]ontrollers must provide a conspicuous and contextually appropriate notice whenever a facial recognition service is deployed in a physical premise open to the public." Controllers must also "must obtain consent from a consumer prior to enrolling an image of that consumer in a facial recognition service used in a physical premise open to the public" except if "for a security or safety purpose." Additionally, "[c]ontrollers using a facial recognition service to make decisions that produce legal effects on consumers or similarly significant effects on consumers must ensure that those decisions are subject to meaningful human review."

Final Rules Released To Govern U.S. Review of Foreign Ownership That Threatens National Security

The Department of the Treasury (Treasury) has released final regulations required by the "Foreign Investment Risk Review Modernization Act of 2018" (FIRRMA) (P.L. 115-232) to revamp and expand the Committee on Foreign Investment in the United States (CFIUS) process for reviewing transactions that takes effect on February 13, 2020. Notably, the CFIUS review process has been broadened to include transactions in which foreign persons or entities acquire a minority stake in another entity deemed to be important for national security. Additionally, the types of transactions covered by the CFIUS process have been expanded.

The FY 2019 National Defense Authorization Act (NDAA) (P.L. 115-32) contained a significant rewrite of the statutory basis for CFIUS that gave the inter-agency process more latitude, tools, and direction in evaluating deals with national security implications, particularly in light of the People's Republic of China's ambitions to displace the U.S. in a number of existing technology fields and to take the lead in a number of cutting-edge fields. Notably, should a company or entity seek less than a controlling interest, it may be subject to the CFIUS process and now CFIUS may take into account "critical technologies," "critical infrastructure," or "sensitive personal data" when evaluating transactions. These final regulations put in place these changes.

In a fact sheet, Treasury explained that "FIRRMA expands CFIUS's jurisdiction beyond transactions that could result in foreign control of a U.S. business to also include non-controlling investments, direct or indirect, by a foreign person in certain U.S. businesses that affords the foreign person:

- access to any material nonpublic technical information in the possession of the U.S. business;
- membership or observer rights on, or the right to nominate an individual to a position on, the board of directors or equivalent governing body of the U.S. business; or
- any involvement, other than through voting of shares, in substantive decisionmaking of the U.S. business regarding—
    - the use, development, acquisition, safekeeping, or release of sensitive personal data of U.S. citizens maintained or collected by the U.S. business;
    - the use, development, acquisition, or release of critical technologies; or
    - the management, operation, manufacture, or supply of critical infrastructure.

Treasury added that "[t]his new authority applies only to non-controlling investments in U.S. businesses that:

- produce, design, test, manufacture, fabricate, or develop one or more critical technologies;
- own, operate, manufacture, supply, or service critical infrastructure; or
- maintain or collect sensitive personal data of U.S. citizens that may be exploited in a manner that threatens national security."

In the rule, Treasury explained that

> FIRRMA maintains the Committee's jurisdiction over any transaction which could result in foreign control of any U.S. business, and it broadens the authorities of the President and CFIUS under section 721 [of the Defense Production Act of 1950 (DPA)] to review and to take action to address any national security concerns arising from certain non-controlling investments and real estate transactions. Additionally, FIRRMA modernizes CFIUS's processes

> to better enable timely and effective reviews of transactions falling under its jurisdiction. In FIRRMA, Congress acknowledged the important role of foreign investment in the U.S. economy and reaffirmed the United States' open investment policy, consistent with the protection of national security.

Treasury explained the ambit of the revised CFIUS regulations:

> These provisions specifically relate to CFIUS's authorities and the process and procedures to review: (1) A merger, acquisition, or takeover by or with a foreign person that could result in foreign control of a U.S. business; (2) a non-controlling "other investment" that affords a foreign person specified access to information in the possession of, rights in, or involvement in the substantive decisionmaking of certain U.S. businesses related to critical technologies, critical infrastructure, or sensitive personal data; (3) any change in a foreign person's rights if such change could result in foreign control of a U.S. business or an "other investment" in certain U.S. businesses; or (4) any other transaction, transfer, agreement, or arrangement, the structure of which is designed or intended to evade or circumvent the application of section 721.

The regulations provide CFIUS with the authority to review "any covered transaction...and to mitigate any risk to the national security of the United States that arises as a result of such transactions" with the definition of what constitutes a covered transaction having been radically expanded. The regulations also reference the authority granted to the President under Section 721 of the DPA "to suspend or prohibit any covered transaction when, in the President's judgment, there is credible evidence that leads the President to believe that the foreign person engaging in a covered transaction might take action that threatens to impair the national security of the United States." However, before CFIUS can present a determination to the President on a covered transaction, it must conduct a risk-based analysis, including "credible evidence demonstrating the risk and an assessment of the threat, vulnerabilities, and consequences to national security related to the transaction."

The new CFIUS regulations include a number of key definitions that dramatically expand the scope of transactions that can now be reviewed and possibly blocked on national security grounds. For example, what constitutes a "covered transaction" is broadened to encompass:

> (a) A covered control transaction;
> (b) A covered investment;
> (c) A change in the rights that a foreign person has with respect to a U.S. business in which the foreign person has an investment, if that change could result in a covered control transaction or a covered investment; or
> (d) Any other transaction, transfer, agreement, or arrangement, the structure of which is designed or intended to evade or circumvent the application of section 721 [of the DPA].

Likewise, there are new definitions of "control," "covered control transaction," "covered investment," and "covered investment critical infrastructure." However, while the final regulations do not change the definition of "critical technologies" promulgated in October in the interim final rule, this definition includes "[e]merging and foundational technologies controlled under section 1758 of the Export Control Reform Act of 2018." And, these terms will be defined in a still to come rulemaking. To date, the Department of Commerce has issued an advanced notice of proposed rulemaking to identify only emerging technologies in November 2018 and has begun the rulemaking process on

foundational technologies by submitting an ANPRM to the Office of Management and Budget (OMB) for review. Consequently, the CFIUS process for deals involving these two types of critical technology may be impeded in the absence of action from the Department of Commerce.

FISA Reform Bill Released

A bipartisan bill has been introduced to end the Section 215 program the National Security Agency (NSA) had used in the past to collect bulk telephone records and metadata and implement other changes to current intelligence practices. This program was shut down last year by the NSA but its underlying authority, Section 215 of the USA PATRIOT Act, expires on March 15, 2020 along with three other authorities extended in December. Despite widespread Republican and Democratic misgivings about the Foreign Intelligence Surveillance Act (FISA) procedures and FISA Court, it is not yet clear whether this sweeping bill stands a chance at enactment or is being laid down as a marker to try and influence the debate over these authorities. Senators Ron Wyden (D-OR) and Steve Daines (R-MT) and Representatives Zoe Lofgren (D-CA), Warren Davidson (R-OH), and Pramila Jayapal (D-WA) introduced the "Safeguarding Americans' Private Records Act of 2020" in both chambers.

In their press release, the sponsors claimed "[t]he bill includes a host of reforms:

- It would permanently end the flawed phone surveillance program, which secretly scooped up Americans' telephone records for years.
- It would close loopholes and prohibit secret interpretation of the law, like those that led to unconstitutional warrantless surveillance programs.
- It would prohibit warrantless collection of geolocation information by intelligence agencies.
- It would respond to issues raised by the Inspector General's office by ensuring independent attorneys, known as amici, have access to all documents, records and proceedings of Foreign Intelligence Surveillance Court, to provide more oversight and transparency.

Notably, beyond revoking the authority for the NSA to restart the telephone collection program, the bill would also exclude from the definition of "tangible thing" in the Section 215 business records exception: Cell site location information, Global positioning system information, Internet website browsing information, and Internet search history information. The bill also contains language that would limit the use of Section 215 to only counterterrorism and foreign intelligence matters and limit the retention of any such material to three years unless it includes foreign intelligence. Moreover, the bill would increase the justification requirements the government must meet before a nondisclosure requirement (aka gag order) can be placed on a company subject to a Section 215 order. The bill also expands the role and powers of the lawyers (aka amici curiae) assigned to argue against FISA warrants and warrantless surveillance. The government would need to submit a report on the use of its roving wiretap authority, which is incidentally one of the expiring authorities. The bill would also set sunset dates for National Security Letter authorities, another means by which surveillance has been conducted by the U.S. government.

As noted, tucked into the month-long FY 2020 continuing resolution (CR) (H.R. 3055) that extended government funding through December 20 was language extending provisions of the FISA set to expire on December 15, 2019. The three-month extension has allowed the Intelligence Community (IC) to continue to use the following authorities: the 1) call detail records provisions; 2) roving wiretap authority; 3) the lone wolf provision; and the 4) business records provisions. These extensions

kicked a contentious legislative issue into next year as none of the committees of jurisdiction have produced legislative proposals on how to reauthorize these programs.

The Trump Administration asked that Congress permanently extend these programs instead of reauthorizing them for a period of years as has been the custom since passage of the USA PATRIOT Act in 2001. In an August letter sent before he stepped down, former Director of National Intelligence Dan Coats asked the Senate and House Intelligence and Judiciary Committees for "the permanent reauthorization of the provisions of the USA FREEDOM Act of 2015 that are currently set to expire in December…[that] provide the IC with key national security authorities." However, a number of stakeholders have balked at a permanent reauthorization of these programs, especially the call detail records program because the NSA has shut down the program. Nonetheless, the Administration is requesting those authorities in the event there is a need in the future.

ICO Issues Statement After London Police Start Using Live Facial Recognition

This week, the United Kingdom's Information Commissioner's Office (ICO) released a statement on the use of facial recognition technology by London's Metropolitan Police Service (MPS). The ICO referenced its previous work on the legal and ethical use of facial recognition technology but notably called on the British government to enact a statute to specifically regulate the use of this new technology. At present, the MPS is operating its system under other authority.

In a blog posting, the ICO stated

> In October 2019 we concluded our investigation into how police use live facial recognition technology (LFR) in public places. Our investigation found there was public support for police use of LFR but also that there needed to be improvements in how police authorised and deployed the technology if it was to retain public confidence and address privacy concerns. We set out our views in a formal Opinion for police forces.

The ICO noted that "[t]he Metropolitan Police Service (MPS) has incorporated the advice from our Opinion into its planning and preparation for future LFR use." The ICO claimed that "[o]ur Opinion acknowledges that an appropriately governed, targeted and intelligence- led deployment of LFR may meet the threshold of strict necessity for law enforcement purposes…[and] [w]e have received assurances from the MPS that it is considering the impact of this technology and is taking steps to reduce intrusion and comply with the requirements of data protection legislation." The ICO stated that "[w]e expect to receive further information from the MPS regarding this matter in forthcoming days…[and] [t]he MPS has committed to us that it will review each deployment, and the ICO will continue to observe and monitor the arrangements for, and effectiveness of, its use."

The ICO cautioned that

> This is an important new technology with potentially significant privacy implications for UK citizens. We reiterate our call for Government to introduce a statutory and binding code of practice for LFR as a matter of priority. The code will ensure consistency in how police forces use this technology and to improve clarity and foreseeability in its use for the public and police officers alike. We believe it's important for government to work with regulators, law enforcement, technology providers and communities to support the code.

In its Opinion titled "The use of live facial recognition technology by law enforcement in public places," the ICO explained it drafted the document "in relation to our regulation of the processing of personal data which takes place whenever law enforcement organisations deploy facial recognition technology in public spaces." The ICO stated that the Opinion "is primarily for police forces or other law enforcement agencies using live facial recognition technology (LFR) in public spaces on how to comply with the provisions of the [Data Protection Act] 2018." The ICO stated that "[i]t aims to guide law enforcement through all the stages of that processing…[and] [h]ere are the key messages in this Opinion:

- The use of live facial recognition (LFR) involves the processing of personal data and therefore data protection law applies, whether it is for a trial or routine operational deployment.
- The processing of personal data by 'competent authorities' (s30 DPA 2018) for 'the law enforcement purposes' (s31 DPA 2018) is covered by Part 3 of the DPA 2018.
- Specifically, the use of LFR for the law enforcement purposes constitutes 'sensitive processing' (s35 (8)(b) DPA 2018) as it involves the processing of biometric data for the purpose of uniquely identifying an individual.
- Such sensitive processing relates to **all** facial images captured and analysed by the software; and must pay particular attention to the requirements of s35, s42 and s64 DPA 2018. As such, a Data Protection Impact Assessment (DPIA) and an 'appropriate policy document' must be in place.
- Sensitive processing occurs **irrespective** of whether that image yields a match to a person on a watchlist or the biometric data of unmatched persons is subsequently deleted within a short space of time.
- Data protection law applies to the whole process of LFR, from consideration about the necessity and proportionality for deployment, the compilation of watchlists, the processing of the biometric data through to the retention and deletion of that data.
- Controllers must identify a lawful basis for the use of LFR. This should be identified and appropriately applied in conjunction with other available legislative instruments such as codes of practice.
- The Commissioner intends to work with relevant authorities with a view to strengthening the legal framework by means of a statutory and binding code of practice issued by government. In the Commissioner's view, such a code would build on the standards established in the Surveillance Camera Code (issued under the Protection of Freedoms Act (POFA 2012) and sit alongside data protection legislation, but with a clear and specific focus on law enforcement use of LFR and other biometric technology. It should be developed to ensure that it can be applicable to current and future biometric technology.
- The Commissioner intends to provide more detailed guidance on what is required for police and other law enforcement agencies to comply with the obligations set out in the High Court's decision in *R (on the application of E. Bridges) v The Chief Constable of South Wales Police, The Secretary of State for the Home Department* and taking note of the Court's recommendation for her to provide guidance on what is required to meet s42 DPA 2018.

Sasse, Rubio, and Cotton Question DOD's Objection To Commerce's Huawei Rule

Senators Ben Sasse (R-NE), Marco Rubio (R-FL), and Tom Cotton (R-AR) have written Secretary of Defense Mark Esper regarding media reports that the Department of Defense (DOD) blocked a proposed rule the Department of Commerce (Commerce) had submitted to the Office of

Management and Budget (OMB) to tighten the de minimis exception that has allowed some U.S. firms to continue selling to Huawei without export licensing under the May 2019 rulemaking. Currently, the percentage threshold that subjects non-U.S. made electronics and goods to the general ban on selling to Huawei stands at 25%, meaning that so long as the U.S.-made components of the item in question are below 25% of the total value, then the ban does not apply. Reportedly, Commerce sought to lower this number to 10% through proposed regulations that required sign off from DOD and other agencies, and the DOD decided to object, which have now been withdrawn from OMB.

In their letter, Sasse, Rubio, and Cotton asked "for a member-level briefing on the [DOD's] rationale for its reported objection...to discuss the following:

> 1. Whether the Department issued a nonconcurrence to the proposed change as publicly reported.
> 2. The rationale for the reported nonconcurrence, including an assessment of the benefits and costs of the Commerce Department proposal on our ability to maintain a technological edge over our adversaries as outlined in either official memoranda and interagency discussion.
> 3. How the Department's reported nonconcurrence affects the Department's simultaneous attempts to persuade allies and partners to bar Huawei from their networks.

The Senators asserted

> Based on public reporting, pursuant to a Department of Commerce proposal, the Office of Management and Budget circulated a proposed rule change that would reduce the maximum percentage of U.S.-origin content, from 25 percent to 10 percent, in permitted sales to Huawei. This change to the De Minimis Rule for sales to Huawei would have effectively disrupted the supply chain of the Chinese Communist Party's tech puppet, which depends on valuable contracts with American companies. The Department reportedly objected over concerns about how the rule would affect U.S. companies' competitiveness and their ability to continue to invest in research and development which allows the United States to maintain a technological edge over our adversaries.

Sasse, Rubio, and Cotton contended that "Huawei is an arm of the Chinese Communist Party and should be treated as such...[and] [w]e are concerned that the Defense Department is not appropriately weighing the risks."

While the DOD has not officially commented on the media reports, at a Center for Strategic and International Studies (CSIS) event on January 24, after being asked about media reports on DOD's action, Esper said

> Look, I've been working these issues for 20-plus years and they're never black and white. So you have to be very conscious of not just your first-order effect – that's the easy thing – it's the second- and third-order effects. And so we got to weigh those out very carefully. As I said, we have to play a strong offense. That includes increased R&D. That includes, you know, better IP policies, as we were talking about beforehand. But it also means a strong defense, whether it's export controls and other defensive measures that we can take to ensure that our technology is protected. But we also have to be conscious of sustaining those companies' supply chains and those innovators. So that's the balance we

> have to strike. There's always a good interagency process that debates that back and forth. And I think more often than not we get it right.

Presumably, these Members could try to add language to the FY 2021 National Defense Authorization Act regarding the de minimis exception, but the fact that there are only three Senators who signed this letter, none of which are Democrats, makes the support for legislation an open question. Moreover, media accounts indicate serious opposition among tech companies, which represents another significant obstacle to trying to force the Administration's hand.

UK Proposes Tightened Privacy and Data Standards for Children

United Kingdom's Information Commissioner's Office (ICO) released a revamp of how online services must be designed if they are aimed at or accessible by children. The "final Age Appropriate Design Code – a set of 15 standards that online services should meet to protect children's privacy" still needs to be passed by the Parliament before it takes effect. Nonetheless, the ICO was directed by and relied on the Data Protection Act 2018 (DPA2018) that revised the privacy standards and rights in the U.K.

The ICO claimed that "[t]he code is the first of its kind, but it reflects the global direction of travel with similar reform being considered in the USA, Europe and globally by the Organisation for Economic Co-operation and Development (OECD)."

The ICO explained

> The code is a set of 15 flexible standards – they do not ban or specifically prescribe – that provides built-in protection to allow children to explore, learn and play online by ensuring that the best interests of the child are the primary consideration when designing and developing online services.
> Settings must be "high privacy" by default (unless there's a compelling reason not to); only the minimum amount of personal data should be collected and retained; children's data should not usually be shared; geolocation services should be switched off by default. Nudge techniques should not be used to encourage children to provide unnecessary personal data, weaken or turn off their privacy settings. The code also addresses issues of parental control and profiling.

The ICO stated that the new Code "applies to you if you provide online products or services (including apps, programs, websites, games or community environments, and connected toys or devices with or without a screen) that process personal data and are likely to be accessed by children in the UK."

In terms of future steps, the ICO stated

> The ICO submitted the code to the Secretary of State in November and it must complete a statutory process before it is laid in Parliament for approval. After that, organisations will have 12 months to update their practices before the code comes into full effect. The ICO expects this to be by autumn 2021.

Trump Administration Releases Report and Recommendations To Fight Counterfeit and Pirated Goods

The Department of Homeland Security (DHS) released a report required by a presidential memorandum regarding counterfeit and pirated goods in electronic commerce. DHS contended that its report "identified a set of strong government actions that DHS and other federal agencies can begin executing immediately to address a crisis that is undermining America's trust in e-commerce even as it is exposing the American public to undue and unacceptable risks…[and] has proposed a set of best practices for private sector stakeholders that DHS believes should be adopted swiftly.

The issues presented by counterfeit and pirated goods is a growing problem. The Government Accountability Office (GAO) published its most recent assessment of counterfeit and pirated goods in 2018 and found

> Counterfeit goods provide a lucrative market for criminal activity and can pose serious risks to consumers. Growth in e-commerce has changed the way counterfeiters interact with consumers, and the accompanying increase in the volume and sophistication of counterfeit goods has created challenges for U.S. Customs and Border Protection (CBP) and U.S. Immigration and Customs Enforcement (ICE) enforcement.

In April 2019, the White House issued a Memorandum on Combating Trafficking in Counterfeit and Pirated Goods that required DHS in consultation with other agencies to draft a report "on the State of Counterfeit and Pirated Goods Trafficking and Recommendations."

DHS explained

> The problem has intensified to staggering levels, as shown by a recent Organisation for Economic Cooperation and Development (OECD) report, which details a 154 percent increase in counterfeits traded internationally — from $200 billion in 2005 to $509 billion in 2016. Similar information collected by the DHS between 2000 and 2018 shows that seizures of infringing goods at U.S. borders have increased 10-fold, from 3,244 seizures per year to 33,810.

Homeland Security stated that "[r]elevant to the President's inquiry into the linkages between e-commerce and counterfeiting, OECD reports that "E-commerce platforms represent ideal storefronts for counterfeits and provide powerful platform[s] for counterfeiters and pirates to engage large numbers of potential consumers."

DHS stated that "[t]he scale of counterfeit activity online is evidenced as well by the significant efforts e-commerce platforms themselves have had to undertake…[and] [a] major e-commerce platform reports that its proactive efforts prevented over 1 million suspected bad actors from publishing a single product for sale through its platform and blocked over 3 billion suspected counterfeit listings from being published to their marketplace." DHS stated that "[d]espite efforts such as these, private sector actions have not been sufficient to prevent the importation and sale of a wide variety and large volume of counterfeit and pirated goods to the American public."

DHS said that "[t]he projected growth of e-commerce fuels mounting fears that the scale of the problem will only increase, especially under a business-as-usual scenario…[and] [c]onsequently, an effective and meaningful response to the President's memorandum is a matter of national import."

DHS offered "Immediate Actions" it and other federal agencies could take:

- Ensure Entities with Financial Interests in Imports Bear Responsibility
- Increase Scrutiny of Section 321 Environment
- Suspend and Debar Repeat Offenders; Act Against Non-Compliant International Posts
- Apply Civil Fines, Penalties and Injunctive Actions for Violative Imported Products
- Leverage Advance Electronic Data for Mail Mode
- Anti-Counterfeiting Consortium to Identify Online Nefarious Actors (ACTION) Plan
- Analyze Enforcement Resources
- Create Modernized E-Commerce Enforcement Framework
- Assess Contributory Trademark Infringement Liability for Platforms
- Re-Examine the Legal Framework Surrounding Non-Resident Importers
- Establish a National Consumer Awareness Campaign

DHS also suggested "Best Practices for E-Commerce Platforms and Third-Party Marketplaces:

- Comprehensive "Terms of Service" Agreements
- Significantly Enhanced Vetting of Third-Party Sellers
- Limitations on High Risk Products
- Rapid Notice and Takedown Procedures
- Enhanced Post-Discovery Actions
- Indemnity Requirements for Foreign Sellers
- Clear Transactions Through Banks that Comply with U.S. Enforcement Requests for Information (RFI)
- Pre-Sale Identification of Third-Party Sellers
- Establish Marketplace Seller ID
- Clearly Identifiable Country of Origin Disclosures

Further Reading

- "Your online activity is now effectively a social 'credit score'" – *Endgadget*. Airbnb is allegedly using artificial intelligence to scrap social media sites and other publicly available information to compile profiles of all users with the goal of predicting future behavior and locating threats. Consequently, a number of sex workers and other people claim that Airbnb no longer allows them to rent units. Airbnb is reportedly not the only platform that limits or blocks people with what some may see as objectionable viewpoints and lifestyles. Absent legislation or extension of existing federal and state civil rights laws, this model could be the future as it is in China with its "social credit system."
- "Is the CCPA working? Early results are ambiguous." – *The Washington Post*. Early reports from privacy and civil liberties advocates and some people suggest companies potentially subject to the "California Consumer Privacy Act" (CCPA) (AB 375) have radically different interpretations of what the new privacy framework requires. Apparently, there are vast differences between companies and certainly between what privacy proponents claim the new statute mandates. Some are arguing companies are either misinterpreting the new

privacy requirements, especially in regard to accessing and obtaining one's personal information, or are outright defying the law. The California Attorney General still needs to finalize regulations and enforcement begins July 1, 2020, so it remains to be seen how the potentially understaffed and under resourced office will implement the new law.

- "YouTube moderators are being forced to sign a statement acknowledging the job can give them PTSD" – *The Verge*. Following a December expose on how YouTube content moderators may be experiencing Post Traumatic Stress Disorder (PTSD) from viewing disturbing and questionable content, a YouTube contractor, Acccenture, is reportedly having such employees sign waivers acknowledging the mental health risks of the job. The December article quoted former and current content moderators who say they have been fighting PTSD sometimes after leaving the job. Accenture also is offering mental health services of a sort but apparently short of providing access to licensed medical professionals like doctors or therapists. A labor attorney quoted in the articles said the waiver language suggests that any employee who experiences PTSD as a result of their employment may be fired, which violates labor law. Moreover, a requirement for employees to disclose their mental health status as part of this process may also violate labor law. Accenture and Google declined to comment on the waiver except generally and on the effect of viewing extreme material on content moderators. The issue of how to screen and takedown extreme, objectionable and illegal content on social media platforms will continue to be an issue in the U.S. and elsewhere throughout the world.
- "Exclusive: Apple dropped plan for encrypting backups after FBI complained – sources" – *Reuters*. Two years ago, Apple was developing a plan to encrypt all Apple user's data in ICloud such that the company could no longer access the information. However, this plan was subsequently scrapped sometime after the company's representatives met with the Federal Bureau of Investigation (FBI). As this article discusses, unnamed sources inside Apple say the company frequently cooperates with law enforcement and intelligence agencies in granting them access to iCloud data. Also of interest in the article is the service Google started quietly offering Android users to encrypt their data in the cloud, but thus far the company has not been attacked like Apple has been by the U.S. government.
- Saudi Crown Prince Hacks Aamazon Head? – According to multiple media outlets, in May 2018 Saudi crown prince Mohammed bin Salman sent malware to Amazon founder and CEO Jeff Bezos via WhatsApp that likely led to the compromise of his phone within hours. Was this related to the murder of *Washington Post* journalist Jamal Khashoggi since Bezos owns the paper? It is not clear at this point, but if Bezos was hacked, it fits a pattern of the Saudi regime going after its enemies. In a stranger twist, it is also being alleged that the NSO Group's Pegasus spyware may have been used. A United Nations report lays out its findings and a timeline, and a documentary about Saudi treatment of dissidents is being released that discusses the hack. Here are the articles: "Revealed: the Saudi heir and the alleged plot to undermine Jeff Bezos" and "Jeff Bezos hack: Amazon boss's phone 'hacked by Saudi crown prince'" – *The Guardian*; "Saudi crown prince implicated in hack of Jeff Bezos's phone, U.N. report will say" – *The Washington Post*.