Technology Policy Update
12 December 2019
By Michael Kans, Esq.

Privacy Bill A Week: United States Consumer Data Privacy Act of 2019

The majority staff of the Senate Commerce Committee circulated the "United States Consumer Data Privacy Act of 2019" (CDPA), a draft data privacy bill days after Ranking Member Maria Cantwell (D-WA) and her cosponsors released the "Consumer Online Privacy Rights Act" (COPRA) (S.2968). Of course, these competing proposals came before the Senate Commerce, Science, and Transportation Committee's hearing on legislative proposals on privacy.

In the main, this bill shares the same framework with COPRA with some key, significant differences, including:

- COPRA expands the FTC's jurisdiction in policing privacy harms whereas CDPA would not
- COPRA places a duty of loyalty on covered entities to people whose covered data they process or transfer; CDPA does not have any such duty
- CDPA does not allow people to sue if covered entities violate the new federal privacy and security regime; COPRA would allow such suits to move forward
- CDPA preempts state privacy and data security laws; COPRA would establish a federal floor that states like California would be able to legislate on top of
- CDPA would take effect two years after enactment, and COPRA would take effect six months after enactment.
- The bar against a person waiving her privacy rights under COPRA is much broader than CDPA
- COPRA would empower the FTC to punish discriminatory data processing and transfers; CDPA would require the FTC to refer these offenses to the appropriate federal and state agencies
- CDPA revives a concept from the Obama Administration's 2015 data privacy bill by allowing organizations and entities to create standards or codes of conduct and allowing those entities in compliance with these standards or codes to be deemed in compliance with CDPA subject to FTC oversight; COPRA does not have any such provision
- COPRA would require covered entities to conduct algorithmic decision-making impact assessments to determine if these processes are fair, accurate, and unbiased; no such requirement is found in CDPA

However, as noted the basic framework both bills create in establishing a federal privacy and data security regime are similar. Broadly, people would receive new rights, largely premised on being accurately informed of how their personal data would be used by covered entities. However, people would need to affirmatively consent before such data processing and transfers could occur.

The bills have similar definitions of what data is covered, what constitutes sensitive covered data, and the entities covered by the bill. Among the key similarities are:

- Both bills would require affirmative express consent for a range of data processing and transferring with COPRA requiring this sort of consent under more circumstances

Michael Kans, Esq. | michaelkans.com | mdk@michaelkanslaw.com | @michael_kans | michaelkans.blog

- Like COPRA, CDPA marries data security requirements to privacy requirements; however, both COPRA and CDPA would deem entities already in compliance with a number of existing federal laws (e.g. Gramm-Leach-Bliley and HIPPA) to be in compliance with their data security requirements, and yet language in both bills suggests that to the extent that these federal standards fall short of the new data security standards, these entities would need to meet additional requirements
- Both bills would allow people to request a copy of their covered data being held by a covered entity, delete or de-identify covered data, to correct or complete such data, and to port their data to another covered entity; however, COPRA would provide additional rights such as the aforementioned duty of loyalty and a right to opt-out of transfers
- COPRA and CDPA would provide additional authority for the FTC to police data security with COPRA giving the agency broad authority to promulgate regulations and providing more descriptive guidance on how to do so with CDPA provided very targeted rulemaking authority that would likely continue the current case-by-case enforcement regime at the FTC
- The FTC could seek civil fines in the first instance of $42,530 per violation along with the current range of equitable and injunctive relief it can seek under both COPRA and CDPA
- Both bills allow state attorneys general could seek the same relief in the event of alleged violations

Separately from the release of this draft, Chair Roger Wicker (R-MS) said he was willing to allow a limited right for people to sue under a federal privacy bill but only to obtain injunctive relief and not monetary damages. This is a significant concession, for Republicans, including Wicker, have long characterized a private right of action as being out of the question. Of course, Wicker does not speak for other Republicans on the committee nor those in the Senate, so it is not exactly clear how much support he has for such a proposal. In the same vein, Wicker remarked to the media that the other main sticking points with Cantwell are on preemption and on a duty of loyalty. However, he may have been making this statement with some optimism for there are other, significant differences between these two bills, suggesting more negotiating is in order.

Also, it has been reported that Senators Richard Blumenthal (D-CT) and Jerry Moran (R-KS) are still working on their privacy bill but are not yet ready to release bill text. It is possible the release of these two bills speeds them to completion on the draft so they can lay down their marker.

However, turning to the substance of the bill, let's start, as always, with definitions. Covered entities are "any person who operates in or affects interstate or foreign commerce," which is a very broad definition that would sweep almost every entity in the U.S. and some overseas into it.

Covered data is defined as "information that identifies or is linked or reasonably linkable to an individual or a device that is linked or reasonably linkable to an individual." The bill further provides "information held by a covered entity is linked or reasonably linkable to an individual if, as a practical matter, it can be used on its own or in combination with other information held by, or readily accessible to, the covered entity to identify the individual or a device associated with that individual." However, covered data does not include: aggregated data; de-identified data; employee data; or publicly available information. Aggregated data is a new term among the privacy bills we've looked at thus far and is "information that relates to a group or category of individuals or devices that does not identify and is not linked or reasonably linkable to any individual."

"Sensitive covered data" "means any of the following forms of covered data of an individual" including but not limited to:

- A unique, government-issued identifier, such as a Social Security number, passport number, or driver's license number.
- Any covered data that describes or reveals the diagnosis or treatment of past, present, or future physical health, mental health, or disability of an individual.
- A financial account number, debit card number, credit card number, or any required security or access code, password, or credentials allowing access to any such account.
- Covered data that is biometric information.
- Precise geolocation information capable of determining with reasonable specificity the past or present actual physical location of an individual or device at a specific point in time.
- The contents of an individual's private communications or the identity of the parties subject to such communications, unless the covered entity is the intended recipient of the communication;
- Covered data revealing an individual's racial or ethnic origin, or religion in a manner inconsistent with the individual's reasonable expectation regarding the processing or transfer of such information.
- Covered data revealing the sexual orientation or sexual behavior of an individual in a manner inconsistent with the individual's reasonable expectation regarding the processing or transfer of such information.
- Covered data about the online activities of an individual that relate to a category of covered data described in another subparagraph of this paragraph.
- Covered data that is calendar information, address book information, phone or text logs, photos, or videos maintained on an individual's device.
- Any other category of covered data designated by the Commission pursuant to a rulemaking under [Administrative Procedure Act] if the Commission determines that the processing or transfer of covered data in such category in a manner that is inconsistent with the reasonable expectations of an individual would be likely to be highly offensive to a reasonable individual.

This is a fairly comprehensive list of covered data that would be considered sensitive.

Additionally, the FTC would be allowed to add other types of data if the agency goes through a rulemaking, providing flexibility and allowing the agency to address any future, unforeseen uses of personal data.

De-identified data is "information held by a covered entity that…does not identify, and is not linked or reasonably linkable to an individual or device" only if the covered entity publicly commits not to not re-identify the person or device. The covered entity would also need to put in place technical and organizational procedures to stop any possible linkage. Additionally, covered entities may not disclose de-identified data to any other entities without a contract or legal instrument barring the re-identification of the data.

CDPA defines affirmative express consent as "upon being presented with a clear and conspicuous description of an act or practice for which consent is sought, an affirmative act by the individual clearly communicating the individual's authorization for the act or practice."

Covered entities will not be able to deny goods or services to an individual because the individual exercised any of the rights established under" the CDPA. Additionally, for each service or product, a covered entity must publish a privacy policy that is "clear and conspicuous" to both the public at large and a person before or at the point of which collection of covered data begins. The CDPA spells out the elements a privacy policy must contain, among other features, the categories of covered data collected, the processing purposes for each category, the categories of third parties to whom the data is transferred and the purposes of such transfers, and a detailed description of data retention practices and data security practices. Any material changes to a covered entity's privacy policy shall require obtaining affirmative express consent anew from people before any processing or transferring of covered data may occur.

The CDPA requires covered entities to fulfill the requests of people to access, correct, complete, delete or port their covered data within 45 days after receiving a verified request. However, a person may not request to access their covered data more than two times in a 12-month period, and for any additional requests, covered entities may charge a fee for such access. Of course, if a covered entity cannot verify the identity of the requester, then it does not need to meet the request. A covered entity may also deny a request if it would require the maintenance of information solely to fulfill the request, it is impossible or demonstrably impracticable to comply, or it necessitates the re-identification of de-identified data. The CDPA stipulates that none of these rights of obligations may be waived by a person in an agreement between a covered entity and a person. The FTC must promulgate regulations under the APA to implement this section.

Regarding the right to access one's covered data, a covered entity must either provide the covered data or "an accurate representation" that is processed, any purposes for which such covered data is transferred, and a list of any third parties or service providers who have received covered data. A person has the right to request that a covered entity "correct inaccuracies or incomplete information with respect to the covered data of the individual that is processed by the covered entity; and notify any service provider or third party to which the covered entity transferred such covered data of the corrected information." A person may also ask that a covered entity delete or de-identify any covered data the covered entity is processing and alert any third parties or service providers the covered entity has transferred the person's covered data to. Finally, subject to technical feasibility, covered entities must generally provide covered data "in a portable, structured, standards-based, interoperable, and machine-readable format that is not subject to licensing restrictions."

In regard to sensitive covered data, a covered entity must obtain affirmative express consent before it can process this subset of covered data or transfer it to a third party. This section also details how covered entities are to obtain affirmative express consent. People must be provided with notice that

- includes a description of the processing purpose for which consent is sought;
- clearly identifies and distinguishes between a processing purpose that is necessary to fulfill a request made by the individual and a processing purpose that is not necessary to fulfill a request made by the individual;
- includes a prominent heading that would enable a reasonable individual to easily identify the processing purpose for which consent is sought; and
- clearly explains the individual's right to provide or withhold consent.

Covered entities will not be able to infer consent if a person does not act or in his continued use of the covered entity's services or products. Moreover, a person must be presented "with a clear and conspicuous means to withdraw affirmative express consent."

The language on the consent related to the sensitive covered data of minors is a bit confusing. Parents will be able to consent on behalf of their minor children in the same manner as they may consent for themselves (i.e. affirmative express consent). And yet, covered entities may not transfer the sensitive covered data of those 16 and younger to a third party if there is actual knowledge of the person's age and unless the individual consents or her parent does.

Generally, covered entities must minimize how they collect, process, or share covered data to what is necessary for that purpose. Specifically, covered entities "shall not collect, process, or transfer covered data beyond

- what is reasonably necessary, proportionate, and limited to provide or improve a product, service, or a communication about a product or service, including what is reasonably necessary, proportionate, and limited to provide a product or service specifically requested by an individual or reasonably anticipated within the context of the covered entity's ongoing relationship with an individual;
- what is reasonably necessary, proportionate, or limited to otherwise process or transfer covered data in a manner that is described in the privacy policy that the covered entity is required to publish…or
- what is expressly permitted by this Act or any other applicable Federal law.

There are exceptions to the rights granted to people just like all the other data privacy bills, which we will turn to momentarily. However, this section requires a bit of elaboration. The FTC will undoubtedly need to determine the broad strokes of what is "necessary, proportionate, and limited" in the different contexts that clause if used. And, yet the FTC is not broadly granted rulemaking authority under the APA to implement the CDPA, and so the agency would probably need to hash out these terms through the "common law" it is currently using to forge the federal data security and privacy regime. And, this may be the case even though the agency is required to issue guidelines recommending best practices for covered entities to minimize the collection, processing, and transfer of covered data in accordance with this section" within one year of enactment. Such guidelines will, of course, inform covered entities of the agency's thinking, but the "necessary, proportionate, and limited" formulation may present a number of close cases that may be adjudicated by courts and/or the FTC.

CDPA lays out the rights, responsibilities, and roles of service providers and third parties under the new federal privacy regime. However, as always, let's look at who would qualify as either. First service providers would be "with respect to a set of covered data, a covered entity that processes or transfers such covered data for the purpose of performing 1 or more services or functions on behalf of, and at the direction of, another covered entity that" is not a part of that covered entity. Third parties are those entities that are not service providers that receive covered data and, again, are not owned or affiliated with the covered entity. There are also definitions of "service provider data" and "third party data." Regarding the former, it shall be those data that service providers are given by covered entities or those covered data the service provider collects on behalf of the covered entity and then processed or transferred per the covered entity's instructions or direction. This could be firms that have dedicated services for processing covered data, possibly even data brokers. Third party data shall be those covered data that are not service provider data that are received from a covered entity. For example, BestBuy transferring

covered data with the proper consent to Walmart would make the latter a third party and those covered data are third party data.

The Act stipulates that service providers may process "service provider data" only at the direction of the covered entity that provided the data and may not undertake any additional processing sua sponte. Likewise, the service provider may not transfer service provider data to third parties without the covered entity having obtained affirmative express consent in the first instance. What's more service providers must delete and deidentify these data as soon as possible after the agreed upon processing has occurred or as soon after the completion of processing as is practicable.

Service providers do not need to respond to a person's request to access, correct, complete, delete, or port covered data, but they must help covered entities fulfill these requests to the degree possible and upon being notified, they must comply with the request a person has made of a covered entity. However, service providers do not need to get affirmative express consent from consumers to transfer their sensitive covered data to third parties. Nor need service providers minimize covered data. So, it would appear that once a person provides a covered entity the necessary consent to process or transfer their sensitive covered data, then this subset of covered data may be transferred onward or processed by a third party. Additionally, it appears covered entities could transfer sensitive covered data to service providers without the affirmative express consent of a people, and then service providers appear free to process such data and to transfer it onward. However, the definition of "process" may weigh against such a reading, for it covers retention and handling of covered data, so perhaps this scenario is contrary to the constraints placed on covered entities.

Third parties "shall not process third party data for a processing purpose inconsistent with the reasonable expectation of the individual to whom such data relates." Additionally, third parties "may reasonably rely on representations made by the covered entity that transferred third party data regarding the reasonable expectations of individuals to whom such data relates, provided that the third party conducts reasonable due diligence on the representations of the covered entity and finds those representations to be credible." And, like service providers third parties do not need to respond to a person's request to access, correct, complete, delete, or port covered data nor minimize data retention.

Nonetheless, covered entities must exercise reasonable due diligence in selecting a service provider or transferring covered data to a third party in order to ensure compliance with the CDPA.

A subset of covered entities would need to meet other requirements. "Large data holders" "shall conduct a privacy impact assessment that weighs the benefits of the covered entity's covered data collection, processing, and transfer practices against the potential adverse consequences to individual privacy of such practices." Those covered entities that are large data holders are those that "processed or transferred the covered data of more than 5,000,000 individuals or devices that are linked or reasonably linkable to such individuals" or "processed or transferred the sensitive covered data of more than 100,000 individuals or devices that linked or reasonably linkable to such individuals (excluding any instance where the covered entity processes the log-in information of an individual or device to allow the individual or device to log in to an account administered by the covered entity)." Covered entities would need to determine annually if they have passed either threshold and have become a large data holder that needs to conduct an

annual privacy impact assessment. Thereafter, these assessments would need to be conducted every two years and would need to be approved by the entity's privacy officer.
Like the other privacy bills, there are circumstances under which covered entities may disregard some of the responsibilities to people. In terms of exceptions to the general rights laid out for people, "a covered entity may collect, process or transfer covered data for any of the following purposes, provided that the collection, processing, or transfer is reasonably necessary, proportionate, and limited to such purpose:

- To complete a transaction or fulfilling an order or service specifically requested by an individual, including associated routine administrative activities such as billing, shipping, and accounting.
- To perform internal system maintenance and network management.
- Subject to [language governing biometrics], to detect or respond to a security incident, provide a secure environment, or maintain the safety of a product or service.
- Subject to [language governing biometrics], to protect against malicious, deceptive, fraudulent, or illegal activity.
- To comply with a legal obligation or the establishment, exercise, or defense of legal claims.
- To prevent an individual from suffering serious harm where the covered entity believes in good faith that the individual is at risk of death or serious physical injury.
- To effectuate a product recall pursuant to Federal or State law.
- To conduct internal research to improve, repair, or develop products, services, or technology.
- To engage in an act or practice that is fair use under copyright law.
- To conduct a public or peer-reviewed scientific, historical, or statistical research that—
    - is in the public interest;
    - adheres to all applicable ethics and privacy laws; and
    - is approved, monitored, and governed by an institutional review board or other oversight entity that meets standards promulgated by the Commission pursuant to [the Administrative Procedure Act]

However, in availing themselves of these exceptions to many of the rights detailed in Title I of the bill, covered entities would not be allowed to breach the ban on denying goods or services because a person exercised their rights under the CDPA nor would they be able to disregard the rights of access, correction, completion, deletion, or portability. Similarly, the covered entity must still adhere to its privacy policy.

As noted earlier, covered entities may "not process or transfer covered data of an individual that is biometric information" "to detect or respond to a security incident, provide a secure environment, or maintain the safety of a product or service" or "to protect against malicious, deceptive, fraudulent, or illegal activity" unless "these activities are "limited to real-time or short-term processing" and comply with to-be-promulgated FTC regulations. There is the further stipulation that "the covered entity does not transfer such information to a third party other than to comply with a legal obligation or to establish, exercise, or defend a legal claim."

Small businesses would be provided with a limited carve out under the CDPA from heeding requests to access, correct, complete, delete, or port covered data and from the data minimization requirements binding on other covered entities. Such exempted small businesses would be those whose gross annual revenues for the preceding three years is $25 million or less,

processing of covered data did not exceed more than 100,000 people or devices, and whose revenue from transferring covered data was less than 50% of its annual revenue.

Senate Commerce Republican staff have apparently acceded to Democratic insistence that data security be made part of a privacy bill as the CDPA contains such language. The bill provides generally that "[a] covered entity shall establish, implement, and maintain reasonable administrative, technical, and physical data security policies and practices to protect against risks to the confidentiality, security, and integrity of sensitive covered data." These data security standards should be "appropriate to the size and complexity of the covered entity, the nature and scope of the covered entity's collection or processing of sensitive covered data, the volume and nature of the sensitive covered data at issue, and the cost of available tools to improve security and reduce vulnerabilities." These standards should be designed to

- identify and assess anticipated human and technical vulnerabilities to sensitive covered data;
- take preventative and corrective action to address anticipated and known vulnerabilities to sensitive covered data; and
- delete sensitive covered data after it is no longer needed for the purpose for which it was collected unless such retention is necessary to comply with a law."

Theoretically, those covered entities processing and transferring sensitive covered data would need to implement more robust data security standards than covered entities just handling covered data.

The FTC may, but is not required to, promulgate regulations under the APA and must consult with the National Institute for Standards and Technology (NIST). However, the FTC must "issue guidance to covered entities on how to—

- identify and assess vulnerabilities to sensitive covered data, including—
    - the potential for unauthorized access to sensitive covered data;
    - human and technical vulnerabilities in the covered entity's collection or processing of sensitive covered data;
    - the management of access rights; and
    - the use of service providers to process sensitive covered data; and
- take preventative and corrective action to address vulnerabilities to sensitive covered data."

If the FTC chooses to skip regulations and instead issue guidance, covered entities might be wise to heed the FTC's views in the latter document, but they would not be required to meet any articulated standards.

And yet, those covered entities in compliance with the "Financial Modernization Act of 1999" (P.L. 106-102) (aka Gramm-Leach-Bliley) and the "Health Insurance Portability and Accountability Act of 1996" (P.L. 104-191) (HIPAA), mainly financial services and healthcare entities respectively, would be deemed to be in compliance with the CDPA. However, this compliance would be only with respect to "information security requirements." Additionally,

Covered entities must also designate privacy officers and data security officers that "shall be responsible for, at a minimum…coordinating the covered entity's policies and practices regarding the processing of covered data; and…facilitating the covered entity's compliance with this Act." Furthermore, "[a] covered entity shall maintain internal controls and reporting structures to ensure

that appropriate senior management officials of the covered entity are involved in assessing risks and making decisions that implicate compliance with this Act." Those entities in compliance with a range of federal privacy regimes regarding "data collection, processing, or transfer activities" under those statutes would be deemed to be in compliance but only with respect to "the data collection, processing, or transfer activities governed by such laws."

In terms of enforcing the CDPA, the FTC would be able to seek civil penalties in the first instance and common carriers and non-profits would be added to the universe of entities the FTC can police. Like COPRA, this bill would establish a "Data Privacy and Security Victims Relief Fund" in which the FTC shall deposit "any civil penalty obtained against any covered entity in any judicial or administrative action the Commission commences to enforce this Act or a regulation promulgated under this Act." These FTC may use these funds "to provide redress, payments or compensation, or other monetary relief to individuals affected by an act or practice for which civil penalties have been imposed under this Act."

State attorneys general may also bring actions to seek a range of remedies including to enjoin conduct in violation of the CDPA and to "obtain damages, civil penalties, restitution, or other compensation on behalf of the residents of the State." If two or attorneys general file suit against the same covered entity for the same conduct, the cases would be combined in federal court in the District of Columbia. Moreover, the FTC may intervene in an action brought by a state attorney general, and if the FTC brings an action first, state attorneys general may not bring actions until the FTC's action finishes.

The CDPA uses a concept from the Obama Administration's "Consumer Privacy Bill of Rights Act of 2015:" the creation of voluntary codes that private entities may adhere to after the FTC has signed off on them. Accordingly, the FTC "may approve certification programs developed by 1 or more covered entities or associations representing categories of covered entities to create standards or codes of conduct regarding compliance with 1 or more provisions in this Act." Consequently, "[a] covered entity that complies with a certification program approved by the Commission shall be deemed to be in compliance with the provisions of this Act addressed by such program." However, "[a] covered entity that has certified compliance with an approved certification program and is found not to be in compliance with such program by the Commission shall be considered to be in violation of the section 5 of the Federal Trade Commission Act… prohibition on unfair or deceptive acts or practices."

The CDPA would preempt state laws on privacy but not any such laws or provisions regarding data breach notification. The CDPA would take effect two years after enactment, allowing covered entities, the FTC and other time to get prepared for the new privacy standards.

The FTC would receive limited responsibility to address discriminatory data processing or transferring. Notably, if the agency receives credible evidence of possible violations of federal laws barring discrimination (e.g. the 1964 Civil Rights Act), it would not investigate and possibly bring an action. Rather, the FTC would transfer this information to federal or state regulators with explicit authority to regulate discrimination.

The FTC would need to use its current Section 6(b) authority to obtain information from entities to examine "the use of algorithms to process covered data in a manner that may violate Federal anti-discrimination laws." The FTC would send out demands for information and entities must answer upon pain of potential penalties. The agency would need to publish a report on its

findings within three years and then publish guidance "to assist covered entities in avoiding discriminatory use of algorithms."

Additionally, within six months of enactment of the CDPA, the National Institute of Standards and Technology (NIST) "shall develop and publish a definition of "digital content forgery" and accompanying explanatory materials" and no later than one year after NIST's report, the FTC must "publish a report regarding the impact of digital content forgeries on individuals and competition." The FTC must update the report at least every two years or more frequently if necessary.

The CDPA lifts a structure from the "California Consumer Privacy Act" (CCPA) (AB 375) in setting up a regime for data brokers to annually register with the FTC. The data broker would need to provide contact information and pay a $100 fee. Failure to do so could result in a fine of $50 per day and no more than $10,000 per year. The FTC would then publish the registration information on its website.

Senate Commerce Revisits Privacy In Light of Legislative Proposals

On December 4, the Senate Committee on Commerce, Science, and Transportation, held a hearing titled, "Examining Legislative Proposals to Protect Consumer Data Privacy," a week after two competing proposals were released: the "United States Consumer Data Privacy Act of 2019" (CDPA) and the "Consumer Online Privacy Rights Act" (COPRA) (S.2968).

Chair Roger Wicker (R-MS) stated "[f]or the past year, members of this committee have worked to develop a strong, national privacy law that would provide baseline data protections for all Americans." He stated that "[g]iven the 2018 implementation of the European Union's General Data Protection Regulation, the passage of the California Consumer Privacy Act, and near-daily reports of data breaches and misuse, it is clear that Congress needs to act now to provide stronger and more meaningful data protections to consumers and address the privacy risks that threaten the prosperity of the nation's digital economy." Wicker stated that "[t]he input of a large number of stakeholders, including consumer advocacy groups, state and local governments, nonprofits, and academia, have all been successful in this effort." He said that "[r]epresentatives from private industry, such as retailers and convenience stores, software, internet, and cloud service providers, technology companies, small businesses, and several other job creators in my home state of Mississippi and across the country, have also provided thoughtful insights to this committee."

Wicker stated that "[t]hroughout this process, we have heard many ideas about how best to protect data from misuse and unwanted collecting and processing." He remarked that "[t]hese ideas involve providing all Americans with more transparency, choice, and control over their data, as well as ways to keep businesses more accountable to consumers when they seek to use their data for other purposes." Wicker stated that "[w]e have heard proposals about how to strengthen the Federal Trade Commission to ensure it has the tools and resources it needs to take swift action against bad actors in the marketplace and effectively respond to changes in potentially harmful technology. That is the FTC's role as the primary enforcement authority over consumer data privacy."

Wicker stated that "[a]n important element of this conversation has been how to achieve each of these goals while preserving the economic and social benefits of data." He said that "[t]hese

benefits not only drive increased productivity, convenience, and cost savings, but they also spur job creation and promote U.S. leadership in technology developments…[and] [u]ltimately, to foster continued innovation among our country's entrepreneurs and job creators, Americans need to maintain trust and confidence that their data will be protected and secure."

Wicker stated that "[t]oday marks another step forward in the committee's efforts to create a national data privacy law…[and] [s]ome of the proposals we will cover today seek to establish consumers' rights and protections over their data in a manner that would provide certainty and clear, workable rules of the road for businesses in all 50 states." He remarked that "[t]his hearing provides an opportunity to hear from expert witnesses on ways to refine these proposals. That should include a discussion on:

> (1) The benefits of creating a strong, national, and preemptive privacy law that provides consumers with certainty that they will have the same set of meaningful data protections no matter where they are in the United States;
> (2) Secondly, the best way to make sure consumers know about, and have a right to opt-out of, the data collection practices of businesses they deal with;
> (3) How requirements on businesses to limit the amount of data they collect and retain about consumers may impact product development and innovation, or what content a consumer is able to view or engage with online;
> (4) How heightened protections over more sensitive personal data, such as information about financial records and biometric information, would help prevent fraud, identity theft, and security breaches. And, whether companies should be required to provide similar heightened protections to non-sensitive data;
> (5) The merits of creating accountability measures for businesses, including requirements to conduct privacy impact assessments when creating new products and services, and designating data privacy and security officers to oversee ongoing data practices;
> (6) How empowering consumers with rights over their data and providing additional resources and authorities to the FTC would help strengthen data protections and confidence in the safety and security of the internet marketplace; and
> (7) Finally, what enforcement mechanisms are the best way to ensure requirements in a law and see that privacy protections are enforced.

Ranking Member Maria Cantwell (D-WA) stated that "Cyber Monday was just a couple of days ago, and it set a record – nine billion in sales and an increase of 19% over last year." She said that "[f]or the first time ever, it was three billion dollars that came from people using smartphones to make those purchases." Cantwell stated that "[s]o it's not just Cyber Monday that's reminding us, because we all know that we buy groceries, fill prescriptions, pay bills, connect to home devices to the internet, apply for loans, stay connected with family and friends, and social media, and so much more of our lives are lived online." She contended that "[w]hich means more information is shared, which means deeply, sometimes personal, information is shared…[a]nd that information can be used to be targeted or to exclude consumers, to be sold, or even worse, it can be stolen." Cantwell added "[a]nd that's why we're here today…[b]ecause we want to protect consumers' privacy rights…[and] [w]e believe to do that you need strong enforcement and mechanisms to make sure that those rights are protected."

Cantwell stated that "[t]he risks that we face online are real…[and] [w]e know that companies today are using ads that might be only for the purposes of targeting what they think is a correct population – young men to work in software – but others can see those ads as discriminatory, or not making themselves available to what information is out there on a job." She claimed that

"Google's Nest camera was involved in an alarming situation where a hacker was able to hack into a couple's baby camera, shouting obscenities before they were able to disable the device." Cantwell stated that "there's the huge issue of marketed and stolen information: Social Security numbers, login information, drivers' licenses, passports, all now going in the thousands of dollars on the dark web, and in fact in 2005 more than eleven billion consumers have had their information breached."

Cantwell stated that "[i]t is Congress' job to make sure Americans are protected and that this information, that is an ever-connected, ever-evolving world, is protected…[a]nd that is why a few weeks ago Senators [Chuck] Schumer (D-NY), [Sherrod] Brown (D-OH), [Patty] Murray (D-WA), [Dianne] Feinstein (D-CA), and myself, joined together to talk about a privacy framework, legislation from all of those committees, that we think would be important for the milestones, the privacy goals that we think should be met." She noted that "[l]ast week, Senators [Brian] Schatz (D-HI), [Amy] Klobuchar (D-MN), [Ed] Markey (D-MA), and myself also introduced [COPRA], that guarantees rights to consumers and strong enforcement." Cantwell stated that "[a]s the Chairman mentioned, many of our colleagues here – Senator [Richard] Blumenthal (D-CT), Senator [John] Thune (R-SD), Senator [Marsha] Blackburn (R-TN), and others – have been involved in these privacy discussions as well, and we welcome everyone's input on how we move forward."

Cantwell explained

> The important things that we think should be there is that you should have the right to make sure your data is not sold. That you have the right to make sure your data is deleted. That you have the right to make sure that you're not discriminated against with data, and the right to have plain old transparency about what is being done on a website. All of these things are tangible and meaningful for consumers. I say they just need to be clear as a bell so that people understand what their rights are and so they know how to enforce them.

Cantwell stated that "[s]o today we're here to hear from a group of witnesses who are going to tell us how those issues might be interpreted for the future…[b]ut I think the director of the New York Law School's Innovation Center, Ari Ezra Waldman, recently made a statement that really resonated with me…[h]e said, "we can pass any laws we want, but if there's no way to enforce them, then what's the point?"

Cantwell stated that "[s]o today we also have to talk about enforcement, because enforcement is going to be the key to making sure that privacy rights are actually upheld, that the consumer is truly protected…[a]nd if we want the consumers to have that protection, then we also have to make sure that there's accountability, that there's whistleblowers, that there is cases against abuses that might happen. If your privacy rights are violated, you need to be first able to find out about it, and then you need to have the power to do something about it as well, and that is why we think our strong legislation does so."

Cantwell stated that "[b]ut I also want to say how much this issue is evolving…[and] [t]oday's Seattle Times features a very large announcement by the Knight Foundation and the University of Washington, and Washington State University, on this issue of the public being fooled by online manipulation – whether that is news stories, digital forgeries, or fakes." Cantwell stated that "[t]hey want to focus on developing research and tools to resist misinformation, promote an informed society, and strengthen the discourse and discussion in America." She added that "I'm so

proud that these institutions are taking on this challenge, and that this kind of national initiative in our legislation, with NIST, the National Institute of Standards and Technology, at the Department of Commerce, would be empowered in the legislation we introduce to help with this effort."

Former Commissioner of the Federal Trade Commission and Microsoft Corporate Vice President and Deputy General Counsel Julie Brill stated that "Microsoft believes that comprehensive federal privacy legislation should adhere to four key principles: transparency, consumer empowerment, corporate responsibility, and strong enforcement:

- Transparency. Transparency is a centerpiece of virtually all data privacy laws existing today. American consumers should have the right to be informed, in a concise and understandable manner, about what personal information companies collect about them, and how that information is used and shared. Companies should provide this information in a context-appropriate fashion at the most meaningful times during the consumer's experience.
- Consumer Empowerment. User control is also a central feature of strong privacy laws. American consumers should be empowered to control their personal information and to express their privacy choices in accordance with rapidly-emerging global norms. In particular, consumers should have rights to access, correct, and delete their personal information, and to move their data to other providers. In addition, Microsoft believes that federal privacy legislation should specifically regulate practices that consumers do not expect and that have a particularly high impact on consumer privacy, such as the collection and sharing of personal information by data brokers that operate behind the scenes, and are unknown to consumers. To ensure that consumers can meaningfully exercise their privacy rights with respect to data brokers, federal privacy legislation should build on concepts from the data broker laws enacted by Vermont and California. The federal law should require data brokers to register with the federal regulator, and to provide information about the kinds of data they collect and sell, the location of the consumers whose information is affected, and details about how consumers can exercise their data control rights.
- Corporate Responsibility. Companies should act as responsible stewards of consumers' personal information, and should be accountable for their actions. This should include affirmative obligations for companies to minimize the amount of personal information they collect—limiting it to the data that is reasonably necessary for the purposes of collection—and to apply technical and other measures to protect that information. Companies also should be required to analyze and improve their internal systems to ensure that they are using consumer data appropriately and in accordance with reasonable consumer expectations, and to document and make these assessments available to an oversight authority upon request. Ultimately, the higher the risk inherent in the proposed use of data, the greater a company's responsibility should be to protect that data. And, as noted above, companies should have affirmative duties to reasonably secure personal information from unauthorized access, and to guard against unlawful discrimination in violation of federal and state laws.
- Strong Enforcement. Congress should empower a strong central regulator, such as the FTC, to issue rules and to appropriately enforce the federal privacy law, and should provide the regulator with sufficient authority, technical capability, and funding to do so. This will help to ensure that the regulatory agency has sufficient capacity and expertise to engage in robust enforcement across the many diverse companies and industries that will be in scope. A strong federal law should also empower the State Attorneys General to enforce the provisions of the law.

Former Acting-Chair of the Federal Trade Commission, 21st Century Privacy Coalition Co-Chair, and Baker Botts Partner Maureen Ohlhausen stated that "[w]e strongly believe that Congress needs to enact federal privacy legislation that includes three key attributes:

1. Reflect consumer preferences through simple choices based on the sensitivity of data
    - We believe that an optimal approach would balance ease of use and transparency by giving consumers clear and simple privacy choices based on the nature of the relevant information itself— its sensitivity and the risk of consumer harm if such information is the subject of an unauthorized disclosure. A federal privacy law should promote consumer control and choice by imposing requirements for obtaining meaningful consent based on the risks associated with different kinds and uses of consumer data. We also believe that consumers should have certain rights of access, correction, and deletion where appropriate.
    - So-called sensitive personal information, such as health and financial information, real- time geo-location information, social security numbers, and children's information, should be subject to the highest protections. In turn, to reflect consumer expectations and preferences, there should be less-stringent requirements on *non*-sensitive personal information, as well as information that is de-identified or aggregated because such information has a lower risk of consumer harm or association with a particular individual. And, for certain types of routine operational uses, consent should be inferred. As recognized by the FTC in its 2012 Report, these uses, which include order fulfillment, fraud prevention, network management, and some forms of first-party marketing, are expected by consumers and provide them a variety of benefits, including knowing about promotions and discounts tailored to their existing services and products.
2. Provide a national and uniform set of protections and consumer rights throughout our digital economy
    - As discussed above, a new federal privacy law should provide meaningful consumer control and choice over consumers' personal data based on the sensitivity of such information. Such strong privacy protections need to apply to consumers regardless of where in the United States they live, work, or happen to be accessing information. By its very nature, the Internet connects individuals across state lines. Put simply, data (and, increasingly, commerce) knows no state boundaries. For this reason, state intervention in this quintessentially interstate issue is problematic, no matter how well intentioned it may be. A proliferation of different state privacy requirements would create inconsistent privacy protections for consumers, as well as significant compliance and operational challenges for businesses of all sizes. It also erects barriers to the kind of innovation and investment that is a lifeblood of our nation's economy and to many beneficial and consumer-friendly uses of information. Indeed, even the authors of California's 2018 privacy law recognized the wisdom of preempting municipal privacy laws.
    - Federal legislation should also be technology-neutral and apply to all entities across the internet ecosystem that make use of consumer data, whether technology companies, broadband providers, or retailers, all of whom are represented on today's panel. What matters is not who collects the data, but what data is collected, how sensitive it is, and how it is protected and used.
3. Ensure strong accountability and enforcement that best protects consumer interests
    - The Members of this Committee recognize that Congress must develop a law that guarantees strong privacy rights to consumers and adopts best practices from

state laws, while creating uniformity across the nation. But preempting state laws should not mean weakening protections for consumers. A federal consumer privacy law needs to be a strong one. The Coalition believes that states, as well as the FTC, have a critical role to play in protecting and enforcing those rights.

- The FTC should have the primary authority to enforce a national privacy law. As privacy concerns become weightier and more complex, the FTC is reaching the limits of its current tools. Under its existing legal regime, in which the FTC polices privacy under its Section 5 authority to prevent unfair and deceptive acts or practices, when the FTC goes after a company for an initial privacy violation, it can require the company to change its practices through a consent order. In very limited circumstances, the FTC can obtain (non-punitive) monetary redress for consumers if the agency can show direct consumer losses. Only if a company later violates that order—and a judge agrees there has been such a violation—can the FTC impose a financial penalty (as opposed to obtaining consumer redress).
- We believe the FTC needs to be able to fine companies for first-time violations of the new, comprehensive privacy law to provide sufficient incentives for companies to take the necessary steps to ensure responsible use and protection of consumer data. In certain cases, Congress should also give the Commission the authority to issue rules to fill in gaps in the law and to keep up with developments in technology. These rules will add clarity to the law so that companies understand what kind of behavior is out of bounds as technology and business practices evolve.
- Congress must also provide the FTC with more resources to protect consumer privacy in America. Despite the ever-growing need for privacy enforcement, the FTC's budget has been flat since 2013. The number of full-time employees lags behind where it was in the early 1980s— nearly four decades ago, when the phrase "big data" meant an encyclopedia and the United States had one hundred million fewer people. The Internet and the collection, use, and sharing of consumer data have grown enormously without a similar boost in FTC resources. We urge Congress to address that widening gap if we are serious about tackling an issue as important and complicated as consumer privacy.

Georgetown University Law School Associate Professor and Communications & Technology Law Clinic Director Laura Moy said she wanted to "make six points:

1.Congress must accept that a strong consumer privacy law will force business practices to change. That change will be costly for companies. Companies may protest a strong privacy law, but Congress should take its lead from people, not companies. Congress should accept that meaningful regulation requires an adjustment period.

2. Privacy legislation must contain use restrictions. It is not enough to require companies merely to disclose what they plan to do with consumer data; rather, they should be restricted to uses that are reasonable. And some applications of consumer data should simply be off-limits.

3. Congress must not accept legislation without civil rights protections. The most troubling use of data is to facilitate discrimination. Congress should prohibit uses of data that selectively deny access to—or awareness of—opportunities in housing, education, finance, employment, and healthcare.

4. Congress should not step on states' toes. As Congress considers establishing new privacy and data security protections for Americans' private information, it should not eliminate existing protections that already benefit Americans at the state level. Nor should it

preempt the states' right to develop new ways to protect their citizens. States are innovating in this space right now and making valuable contributions.

5. There are valuable provisions in multiple bills before this committee. The Committee should be commended for working diligently and creatively to develop legislation that meets growing demands for privacy protection.

6. If Congress cannot agree on legislation that embodies the Public Interest Privacy Legislation Principles, it should not act. One option before Congress is to hold its pen. If Congress cannot produce a bipartisan bill that synthesizes the valuable provisions across bills to embody the principles advanced by public interest organizations over a year ago, perhaps it should wait—and allow states to continue to fill the gap.

Center for Democracy and Technology Privacy and Data Director Michelle Richardson highlighted "a number of key issues" and discussed "how they can be addressed in legislation:"

- Covered entities. It's crucial that any comprehensive privacy law cover all private sector entities that collect, use, and share personal information. This includes not only the prominent tech companies that have captured our attention recently, but also not-for-profit entities and the communication providers that are currently under FCC jurisdiction for privacy and security enforcement. Creating a single federal standard will ensure that individuals can rely on the same baseline rights as they move across the digital ecosystem. To that end, Chairman Wicker's staff discussion draft is one of the more comprehensive proposals. We also recommend that legislation not categorically exempt small businesses.
- Covered data. It is also important that legislation cover all personal data even if the Committee decides that there may be tiers of sensitivity that warrant different substantive requirements. We strongly recommend that the committee define covered personal information consistent with current FTC guidance which is best reflected in Ranking Member Cantwell's draft bill as "information that identifies, or is linked or reasonably linkable to an individual or consumer device, including derived data." The additional qualifier that this data "can be used on its own or in combination with other information held by, or readily accessible to, the covered entity" as proposed in the Wicker staff draft may be overly restrictive. Distinguishing between data that is linkable and that which is not serves two purposes. First, to discourage first parties from unnecessarily associating information with real people, but second, to offer down stream protections when information is shared with affiliates, third parties, or even in the instance of a data breach. These additional reasons for storing and using data in de-identified format will be frustrated by a definition that so heavily focuses on first party linkability.
- Data use. Both Chairman Wicker and Ranking Member Cantwells' bills begin to address the exceptionally hard question of whether and how to regulate the use of data beyond any opt-in requirement. The FTC continues to develop a body of common law to prohibit certain data uses on a case by case basis, but a federal privacy law can and should go one step further to categorically prohibit some of the riskiest data uses.
- Data use limitations exist to some extent in Chairman Wicker's minimization section and Ranking Member Cantwell's loyalty section. The committee could also borrow from legislation sponsored by Senators Blunt and Schatz on facial recognition technology and Senator Markey's comprehensive privacy bill. Ultimately, data use limitations must go beyond limiting data use to what a company *says* it will do with data, to creating an objective limitation regardless of what any one privacy policy entails. While there are a number of ways to craft this, a clear purpose limitation on sensitive data will make great strides towards aligning consumer knowledge and expectations with corporate behavior. To the extent that some provisions peg data use to what a company believes is a

"reasonable" consumer expectation, they may be subject to bad faith arguments or protracted litigation about what exactly a "reasonable consumer" is.

- Artificial intelligence and civil rights. Both bills recognize the importance of providing oversight of artificial intelligence programs and reinforcing longstanding discrimination laws that may be undercut by current data practices. Despite their differences, we hope this signals a commitment to addressing these issues in any final privacy and security legislation. CDT prefers the breadth and depth of Ranking Member Cantwell's approach and looks forward to working with the committee on refining these requirements as necessary as the legislation moves forward.
- Data security. CDT commends Chairman Wicker and Ranking Member Cantwell for including data security requirements in their draft bills. Close to half of US states do not have a general purpose data security law, and FTC enforcement under its Section 5 authority will always be limited to what its resources allow. We recommend combining the two and adding one additional provision. First, the committee should adopt Chairman Wicker's base text in section 204 regarding the requirements of a reasonable data security program. Second, the committee should adopt Ranking Member Cantwell's scoping of data to be covered. Her draft protects not only sensitive information, but all personal information. Because both bills impose a reasonableness standard that will peg to the size and complexity of the organization and the sensitivity and use of the data, it is unnecessary to exempt certain data sets from the overall security requirement. Third, this section should provide overall rulemaking for the FTC. Right now, the Wicker and Cantwell bills require guidance or limited rulemaking, but it is time for the longstanding guidance of the FTC to be written into regulation. To the extent that some in the corporate sector have criticized the FTC's data security requirements as too vague despite long-standing guidance in this space, they will benefit from having regulations on the books to better describe requirements.
- Opt in requirements for sensitive data. Both bills include a comprehensive list of sensitive data that is subject to affirmative, express consent. The differences are minimal but the definitions should be amended in a few key ways. First, the committee should adopt an expansive definition of health information, and we recommend borrowing from CDT's model legislation which incorporates not only data that reflects a person's mental and physical status, but data that is processed for health or wellness purposes. As Senator Klobuchar and Murkowski recognize in their Protecting Personal Health Data Act, apps, wearables, and devices are creating and collecting intensely personal information that can be used in ways that greatly affect a person's mental and physical well-being. Any definition should ensure that these resulting data sets receive heightened protection.
- Product development exception . In general, the list of exceptions to the opt-in right contains reasonable data use that is core to offering the product an individual signs up for. They fairly recognize that some data processing is absolutely necessary to offer safe and effective products and cannot be opted out of either individually or at scale. However product development as listed in Chairman Wicker's staff discussion draft is meaningfully different from the rest of the data uses. It permits companies to collect data without someone's consent even if they have no understanding of how it will be used or whether they will benefit from the use at some point in the future. Since product development is solely for the benefits of the companies who collect the data - unlike everything else on this list of exceptions-- it should not be done without an individual's consent. To the extent the Committee does not want to inhibit innovation, it should further explore why the de-identification carve out is insufficient for product development, and whether some middle ground should be created for processing data this way.

- Access correction deletion portability. The individual controls are comprehensive. Our only suggestion is that the Committee include the timelines drafted into Wicker's staff discussion draft to ensure that rights are afforded on a reasonable timeframe.
- Data broker registry. We commend the Wicker staff draft for including a data broker registry housed at the FTC. A registry will ensure that individuals can discover and exercise their rights against data brokers who have amassed incredible amounts of sensitive data on the average American. While many of the provisions in both the Cantwell and Wicker drafts may slim down the amount of information that eventually ends up in data broker databases, these entities are likely to continue collecting information and will still be holding data that has been accrued over decades of largely unregulated data use. That someone can exercise their access, correction, and deletion rights against these entities is the best protection against future data abuse.
- Enforcement. Both Chairman Wicker and Ranking Member Cantwell's drafts include meaningful enforcement mechanisms, but they differ in a few important ways. First, Ranking Member Cantwell includes a private right of action (PROA) for all violations of the law. CDT believes a targeted private right of action is necessary for meaningful enforcement. This is not only because the number of entities that will be swept under new regulations will necessarily dwarf the resources of the FTC and state attorney generals, but because our history is full of instances where government actors simply did not have the wherewithal to be first movers on important social issues. Because private litigation has served such an important function in civil and consumer rights enforcement in the past, it should be reserved in some form in federal privacy legislation. It is important to note that all 50 state unfair and deceptive practice laws include some form of a private right of action, even if substantially limited. If a privacy bill seeks to categorically move privacy and data security out of these laws, it should ensure that consumers are at least equally positioned to defend their rights as they are now. The proper balance likely lies between the Cantwell and Wicker drafts in a specific delineation of what provisions can be enforced by PROA and under what conditions. State and federal laws are full of examples where PROAs are crafted to limit litigation to the most important harms. We recommend that the Committee consider this approach to find the right way to maximize accountability and minimize nuisance litigation. Such litigation controls could include opportunities to cure, harm requirements, reduced or nonexist damages or prior agency review, for example. We look forward to working with the Committee further on finding the right way forward on PROAs.

FCC Oversight Hearing

On December 5, the House Energy and Commerce Committee's Communications and Technology Subcommittee held a hearing titled "Accountability and Oversight of the Federal Communications Commission" (FCC) with the agency's chair and the other four commissioners.

In a memorandum, Democratic staff explained:

> The Federal Communications Commission (FCC) is considering several spectrum bands for licensed wireless broadband services or unlicensed use. In the mid-band, the FCC is focused on five bands: The Educational Broadband Service (EBS) 2.5 GHz; the Citizens Broadband Radio Service (CBRS) 3.5 GHz; the 5.9 GHz band; the 6 GHz band; and the C-Band 3.7 - 4.2 GHz band. Regarding the EBS band, the FCC adopted a Report and Order in July, announcing new opportunities for entities to obtain unused spectrum for next

> generation wireless broadband, including 5G. The Commission also adopted a priority application filing window for native tribes and tribal organizations. The Commission is expected to auction the remaining unused EBS spectrum in 2020.

Chair Frank Pallone Jr (D-NJ) contended that "this FCC, under Chairman Pai, continues to turn its back to consumers - in favor of big corporate interests." He said "[t]ime and time again, this Commission has ignored the voice of the people and has taken a different path laid out by billion-dollar companies." Pallone said that "[t]he prime example of this was the FCC's action turning control of the Internet over to large corporations by eliminating strong net neutrality safeguards that protected a free and open internet." He said "[b]ut that was just the beginning… [and] [a]s part of an effort to expedite the rollout of 5G service, the FCC stripped away vital protections that help safeguard important religious and cultural tribal sites." He stated that "[l]uckily the courts struck down this effort."

Ranking Member Greg Walden (R-OR) stated "[w]e learned from a press release yesterday that the FCC is establishing a new, $9 billion fund, with $1 billion specifically for precision agriculture." He said that "[i]t sounds good…[and] I support the build out in 5G for rural areas, but I have no details on this plan." Walden stated that "I do have a lot of questions…[and] I'm also unclear as to where the $9 billion dollars came from and while still waiting for the maps to be adequately be updated." He stated that "I'd also like to note the importance of ensuring that Federal programs outside of the Energy and Commerce Committee's jurisdiction remain consistent with the Committee's goal of promoting private investment in broadband infrastructure deployment." He said that "[s]ometimes, various programs trying to achieve the same goal are not always in sync as you all know." Walden said that "[l]ast Congress, we appropriated more than $600 million toward broadband funding programs…[and] [a]s that money begins making its way out the door, I welcome an update from the Commissioners here today as to how the FCC is consulting with other agencies as we required by legislation last year."

FCC Chair Ajit Pai stated

> we adopted two measures at our November meeting to protect national security and promote public safety. The first was a decision to ban the use of funds from the FCC's Universal Service Fund (USF) for the purchase of equipment or services from companies posing a national security threat to the integrity of communications networks or the communications supply chain. We also initially designated two Chinese companies—Huawei and ZTE—as "covered" companies for purposes of this rule, and we set up a process for designating additional such companies in the future. Given the threats posed by Huawei and ZTE to America's security and our 5G future, this FCC will not sit idly by and hope for the best. Looking forward, we also proposed a process to remove equipment already deployed in USF-funded networks. Specifically, we proposed to require certain carriers receiving USF funds, known as eligible telecommunications carriers, to remove from their networks existing equipment from covered companies, starting with Huawei and ZTE. To mitigate the financial impact of this requirement, particularly on small, rural carriers, we proposed to establish a reimbursement program to help offset the cost of transitioning to more trusted vendors. This effort to secure our communications networks has strong bipartisan support, including Attorney General Bill Barr, U.S. Chief Technology Officer Michael Kratsios, Senators Mark Warner and Tom Cotton, and my FCC colleagues testifying alongside me.

FCC Commissioner Jessica Rosenworcel said that "the bipartisan leadership of the United States Senate Committees on Intelligence, Homeland Security and Government Affairs, Foreign Affairs, and Armed Services wrote the White House expressing concern that we do not have a coordinated, national strategy in place for 5G—and we need one." She stated that "I agree… [and] [h]ere's what I think a national strategy should include:

- First, we need an approach to supply chain security that considers how we can build secure networks that can withstand insecure equipment abroad—because no network stands by itself. So I suggested the FCC explore opportunities to unlock and diversify communications by supporting efforts with open radio access networks, or open RAN. This idea has garnered support from staff of the Department of Homeland Security, the Department of Commerce, and the Department of State.
- Second, we need to transform the Internet of Things into the Internet of Secure Things. With the advent of 5G, we are going to see billions and billions of new connected devices. To ensure that they are secure, the FCC should use its equipment authorization process creatively and encourage all device manufacturers to build security into new products.
- Third, we need smarter spectrum policy. To date, the FCC has focused its early efforts to support 5G wireless services by bringing only high-band spectrum to market. This is a mistake. The sheer volume of antenna facilities needed to make this service viable will limit deployment to the most populated areas. And continuing to simply auction millimeter wave spectrum while the rest of the world is already working with mid-band airwaves has security consequences because so much of this equipment is available from only one Chinese vendor. So we need to pivot away from auctioning high-band spectrum and prioritize mid-band spectrum. Our next auction should feature the 3.5 GHz band and we should focus on a C-band auction thereafter.

Ahead of the hearing on December 4, FCC Chair Ajit Pai announced "that he intends to establish the 5G Fund, which would make up to $9 billion in Universal Service Fund support available to carriers to deploy advanced 5G mobile wireless services in rural America." He claimed that "[t]his major investment in rural America would be allocated through a reverse auction and would target hard-to-serve areas with sparse populations and/or rugged terrain…[and] [t]he $9 billion Fund also would set aside at least $1 billion specifically for deployments facilitating precision agriculture needs. "

Pai added

> The 5G Fund would replace the planned Mobility Fund Phase II, which would have provided federal support for 4G LTE service in unserved areas. Pursuant to the Mobility Fund Phase II rules, wireless providers were required to submit 4G LTE coverage data in order to help the Commission target federal subsidies to unserved parts of the country. The Mobility Fund Phase II challenge process gave stakeholders an opportunity to dispute these coverage maps by submitting speed tests to the Commission. But in a report released today, Commission staff finds that the 4G LTE coverage data submitted by providers is not sufficiently reliable for the purpose of moving forward with Mobility Fund Phase II.

CISA Briefs Senate On Menace Of Ransomware To States and Municipalities

This week, Cybersecurity and Infrastructure Security Agency (CISA) Director Christopher Krebs conducted a classified briefing of the Senate Cybersecurity Caucus the growing threat ransomware poses to states, cities, and localities. In a statement issued afterwards, Caucus co-chairs Senators Mark Warner (D-VA) and Cory Gardner (R-CO) claimed "[t]he continued prevalence of ransomware should really capture our attention." They stated that "[i]t's costly, devastatingly high-impact, growing, and, in most cases, easily preventable with basic responsible cybersecurity practices." Warner and Gardner stated that "[r]ansomware and its destructive cousin wiperware are designed to inflict fear and uncertainty, disrupt vital services, and sow distrust in public institutions." They added that "[w]hile often viewed as basic digital extortion, ransomware has had materially adverse impacts on markets, social services like education, water, and power, and on healthcare delivery, as we have seen in a number of states and municipalities across the United States."

In August CISA released a Cyber Insight on ransomware that laid out "three sets of straightforward steps any organization can take to manage their risk." CISA claimed that "[t]hese recommendations are written broadly for all levels within an organization." CISA stated that "[i]t's never as easy as it should be, so if you need help, we urge you to reach out for assistance – CISA is here to help, but so is the FBI, numerous private sector security firms, state authorities, and others."

More recently, the Homeland Security Advisory Council (Council) released its final report on how the Department of Homeland Security (DHS) could better help Federal, State, Local, Tribal, and Territorial (SLTT) face and manage cyber risks.

The Council stated that

> Our nation faces serious and evolving cyber threats. As cyber and physical systems become more interconnected, the digital attack surface is extending further into our daily lives, with the potential for malicious cyber actors to create dangerous, real-world effects. Federal, State, Local, Tribal, and Territorial (SLTT) entities must collaborate and coordinate extensively with critical infrastructure private sector owners, operators, and stakeholders to identify and address these cybersecurity challenges.

The Council noted "[s]ix ways DHS can support states to improve SLTT capabilities…[b]y identifying and leveraging zones of excellence within a range of functions and geographic constructs, DHS can raise the baseline for SLTT cybersecurity and enhance cybersecurity for the nation…[and] can support states by improvement in these six ways:

- DHS can empower cyber mutual assistance for SLTT entities. SLTT stakeholders can benefit from strong cyber mutual assistance agreements, plans, and exercises. Those with greater capabilities can help the less robust SLTT stakeholders.
- DHS can create a dedicated grant program for state cybersecurity, and support raising the defined baseline through bulk purchase vehicles for commonly used cyber essentials. The SLTT community can achieve a higher baseline of cybersecurity in a more efficient manner if they can readily access a pre- negotiated, cost-effective body of basic hygiene and other essential offerings.
- DHS can strengthen regional resilience, situational awareness, and preparedness. Disasters do not respect state lines: cyber compromise can halt functionality without heed for geography, and natural disasters tend to have regional impact. States and localities are

stronger when they share awareness and resources, thereby fostering resilience beyond any individual legal jurisdiction.

- DHS can empower existing Fusion Centers to become centers of cyber situational awareness and Security Operations Centers (SOCs) for the SLTT ecosystem. While some states have sophisticated cyber programs, many still need a focal point for understanding and assessing the cyber threat.
- DHS can unify efforts to empower SLTT election officials more comprehensively and to protect the nation's election infrastructure.
- DHS can lead the nation toward managing the risks introduced by Smart Cities. Many cities are adopting smart technology without understanding and managing the risks that these new technologies present to public safety and critical infrastructure functions.

GAO Reports and Ruling

The Government Accountability Office (GAO) released a pair of reports on the Department of Defense's (DOD) contracting practices and a decision on a contracting vehicle Congress directed the DOD to use more judiciously.

In its report on the ownership structure of some DOD contractors, the GAO found the Pentagon "faces several types of financial and nonfinancial fraud and national security risks posed by contractors with opaque ownership." The GAO stated that "[t]hese risks, identified through GAO's review of 32 adjudicated cases, include price inflation through multiple companies owned by the same entity to falsely create the appearance of competition, contractors receiving contracts they were not eligible to receive, and a foreign manufacturer receiving sensitive information or producing faulty equipment through a U.S.-based company." The GAO undertook this assessment per a provision in the House Armed Services Committee's committee report for the FY 2018 National Defense Authorization Act.

The GAO acknowledged that the "DOD has taken some steps that could address some risks related to contractor ownership in the procurement process but has not yet assessed these risks across the department." The agency added that the "DOD, in coordination with other agencies, revised the Federal Acquisition Regulation in 2014 to require contractors to self-report some ownership information." The GAO said that the "DOD has taken steps to identify and use ownership information—for example, as part of its supply-chain risk analysis when acquiring critical components." The GAO stated that the "DOD has also begun a department-wide fraud risk management program, but it has neither assessed risks of contractor ownership across the department nor identified risks posed by contractor ownership as a specific area for assessment." The agency asserted that "[a]ssessing risks arising from contractor ownership would allow DOD to take a strategic approach to identifying and managing these risks, make informed decisions on how to best use its resources, and evaluate its existing control activities to ensure they effectively respond to these risks."

The GAO recommended:

> The Office of the Undersecretary of Defense (Comptroller) (OUSD[C]) should include an assessment of risks related to contractor ownership as part of its ongoing efforts to plan and conduct a department-wide fraud risk assessment. As part of this assessment, consistent with leading practices, DOD should involve relevant stakeholders with

> knowledge of emerging risks and use this information to help inform other types of risk assessments across the department, including for national security concerns.

In the other report, the GAO examined the DOD's use of a contract vehicle to engage entities that are developing cutting edge technologies and do not usually contract with the federal government. The GAO, however, did not draw conclusions or make any explicit recommendations. And yet, the GAO did note previous reports that turned up risks inherent in contract vehicles that deviate from those laid in regulation.

The GAO noted that "Congress gave DOD the authority to use agreements known as other transactions, which allows DOD to attract companies or other entities that have not done business with DOD…[and] [t]hese could include, for example, commercial science and technology companies and non-profit research institutions, which we refer to as non-traditional companies." The GAO said that "[w]hile DOD can use other transactions for research, prototyping, and production purposes, this report is focused only on other transactions used to support prototyping efforts, which, among other things,demonstrate whether technologies and products developed by companies can be adapted for DOD's use." The GAO explained that "[w]e refer to these other transactions as prototype other transactions and the DOD officials who award these transactions are known as agreements officers…[and] [w]ith a few exceptions, Congress requires that non-traditional companies participate to a significant extent on prototype other transactions."

The GAO asserted

> Other transactions enable DOD and companies to negotiate terms and conditions specific to a project without requiring them to comply with most federal regulations that apply to government procurement contracts. This flexibility can also help DOD address non-traditional companies' concerns about establishing a government-unique cost accounting system or intellectual property rights, among other concerns. We and others have previously reported, however, that the use of other transactions carries the risk of reduced accountability and transparency, in part because such transactions are exempt from the Federal Acquisition Regulation (FAR) and related controls and oversight mechanisms that apply to government procurement contracts.

In denying a bid protest, the GAO found that Congress did not bar the Department of Defense from using past performance of contracts as a tradeoff with price factors despite language limiting the Pentagon's use of lowest-priced, technically acceptable (LPTA) contacts. Inserso Corporation had filed a protest regarding the "terms of request for quotations (RFQ) No. 1369887, issued by the Department of the Air Force for information technology (IT) and cybersecurity services." The company claimed "the agency is using LPTA award criteria in violation of section 813(c) of the National Defense Authorization Act (NDAA) for Fiscal Year 2017…as amended by the NDAA for Fiscal Year 2018…" Specifically, the company claimed the Air Force "is violating the NDAA for Fiscal Year 2017 by using LPTA source selection criteria to make its award determination…because the RFQ fails to provide for a tradeoff between price and technical factors." The GAO stated that "[a]lthough Inserso's interpretation of the statute may be considered reasonable, we find the agency's interpretation of section 813(c) is also reasonable." The GAO stated that "neither section (a) nor section (b) of the statute suggests that Congress specifically intended to preclude the use of past performance as a technical tradeoff factor with price." The GAO further found that "[t]he statute does not specifically define either the

term LPTA process or the term LPTA criteria, and the parties have not provided any controlling definition of the terms."

Draft Order Released Requiring Civilian Agencies To Set Up Process To Accept Vulnerability Reports

The Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) has released for comment a Binding Operational Directive (BOD) that would require civilian agencies to publish and implement vulnerability disclosure policies (VDP) that is intended to encompass all information systems on the civilian side of the federal government. A VDP would allow people not affiliated with the agency or the federal government to report vulnerabilities without fear of legal liability provided the agency's policy is followed. This marks the first instance DHS or CISA have released a BOD for comment, but the agency reasoned "it's the public that will provide those reports and will be the true beneficiaries of vulnerability remediation." Civilian agencies must follow BODs per the "Federal Information Security Modernization Act of 2014" (FISMA) but they do not apply to "national security systems" and other systems in the Department of Defense (DOD) and Intelligence Community (IC). Comments on this BOD are due on December 27, 2019.

All civilian agencies must publish their VDPs on their website within 180 days of issuance of the BOD, explain which information systems are subject to the VDP, the types of vulnerability testing allowed, how interested parties can submit vulnerability reports, and then gradually expand the scope of those systems such that within two years of issuance of a final BOD all the agencies systems will be part of VDP. As a vital part of these forthcoming VDPs, agencies must announce "[a] commitment to not recommend or pursue legal action against anyone for security research activities that the agency concludes represents a good faith effort to follow the policy, and deem that activity authorized." Ultimately, the VDP process will become part of FISMA reporting and data will be aggregated on the number of vulnerability reports, the time it takes an agency to validate a report, and to remediate or mitigate an identified vulnerability.

After an agency has a VDP in place it has a number of reporting responsibilities to CISA, including:

- Valid or credible reports of newly discovered or not publicly known vulnerabilities on agency systems that use commercial software or services that affect or are likely to affect other parties in government or industry.
- Vulnerability disclosure, coordination, or remediation activities the agency believes CISA can assist with or should know about, particularly as it relates to outside organizations.

CISA explained that "[i]n preparing this directive, we've worked with several agencies that have VDPs and made an effort to align the directive with federal guidance, international standards, and good practices." CISA added that "this directive is slightly different from others we've issued, where agencies are directed to take an action and then CISA verifies the action has taken place." The agency stated that "[h]ere, while agencies must maintain VDPs and are the beneficiaries of vulnerability reports, it's the public that will provide those reports and will be the true beneficiaries of vulnerability remediation." CISA stated that "[w]e want to hear from people with personal or institutional expertise in vulnerability disclosure...[and] also want to hear from organizations that have a VDP and manage coordinated vulnerability disclosures." The agency claimed that "[i]n seeking public comment, we're also nodding to the fact that, to our knowledge,

a requirement for individual enterprises to maintain a vulnerability disclosure policy has never been done before, and certainly not on this scale."

CISA provided a summary of what the draft BOD does:

- Lights a fire. Each agency must publish a VDP and maintain handling procedures, and the directive outlines a set of required elements for both.
- Draws a line in the sand. Systems "born" after publication of a VDP must be included in scope of an agency's VDP.
- Expands the circle. Until everything is included, at least one new system or service must be added every 90 days to the scope of an agency's VDP.
- Starts the clock. There's an upper bound – 2 years from issuance, in this draft – for when all internet-accessible systems must be in scope.
- All are welcome. Anyone that finds a problem must be able to report it to an agency.
- No "catch and keep". An agency may only request a reasonably time-limited restriction against outside disclosure to comply with their VDP.
- Defense, not offense. Submissions are for defensive purposes; they don't go to the Vulnerabilities Equities Process.

CISA explained that the BOD does not

- Establish a "federal bug bounty". A bug bounty is a program that pays researchers for valid and impactful findings. Nothing in the directive prevents individual agencies from establishing a bug bounty of their own, though.
- Create a "national VDP". The directive is an executive branch policy instruction that requires federal civilian executive branch agencies to have a VDP. The difference might appear slight but they're very different things.

This draft BOD on VDP must be distinguished from the process by which the Administration decides whether to share vulnerabilities it has discovered with private sector entities or use them for intelligence or military purposes. As you may recall, in November 2017, the Trump Administration released a Vulnerabilities Equities Process (VEP) Charter, which governs how the "Federal Government will handle the process that determines whether the Government will notify a private company about a cybersecurity flaw in its product or service or refrain from disclosing the flaw so it can be used for operational or intelligence-gathering purposes." The Administration stated that "[t]he primary focus of this policy is to prioritize the public's interest in cybersecurity and to protect core Internet infrastructure, information systems, critical infrastructure systems, and the U.S. economy through the disclosure of vulnerabilities discovered by the [U.S. government], absent a demonstrable, overriding interest in the use of the vulnerability for lawful intelligence, law enforcement, or national security purposes." The Administration claimed that "[i]n the vast majority of cases, responsibly disclosing a newly discovered vulnerability is clearly in the national interest."

In the draft BOD CISA pledges that it "will not submit any vulnerabilities it receives or may help coordinate under this directive to the Vulnerabilities Equities Process," meaning that any flaws turned up in private sector software or systems will not be passed along to the IC for future, possible exploitation while allowing civilian agencies and the public at large to remain vulnerable.

In conjunction with CISA release for comment a Binding Operational Directive (BOD) that would require civilian agencies to publish and implement vulnerability disclosure policies (VDP), the

Office of Management and Budget (OMB) has also released for comment a draft policy in order to help civilian agencies broadly comply with the BOD and to coordinate the establishment and reformation of VDPs generally. OMB explained the draft memorandum "provides Federal agencies with guidance on CVD programs and mandates a baseline of government-wide coordinate vulnerability disclosure requirements," and like with all OMB-helmed government-wide policies, follow through by OMB and buy-in from agencies will likely determine how robustly this program is implemented. Comments are due by December 27, 2019.

By way of a policy backdrop, OMB explained that "Coordinated Vulnerability Disclosure (CVD) programs seek to mitigate security risks by authorizing security researchers and the public at large with a way to safely and responsibly report security vulnerabilities they uncover...[and] [w]hen implemented effectively, these programs enable organizations to improve the security of Federal information systems using supplemental information approaches." OMB stated

> Federal agencies are currently incorporating two types of CVD programs into their security efforts: vulnerability disclosure policies (VDPs) and bug bounties. VDPs, which are processes for the intake and addressing of security vulnerabilities uncovered by security researchers and the public, are among the most effective methods for obtaining new insights regarding security vulnerability information. They also provide protection for those who uncover these vulnerabilities by differentiating between acceptable and unacceptable means of gathering security information (also known as "authorizing good faith security research"). VDPs make it easier for the security research community to report vulnerabilities to appropriate agency contacts, who can then use the reports to address vulnerabilities of which they may not have been aware. Bug bounty programs go a step further than VDPs by offering financial compensation based on established parameters to security researchers who report the vulnerabilities.

OMB claimed that "[t]he Federal Government remains committed to finding new and innovative ways to leverage top talent to help agencies meet critical cybersecurity needs, and CVD will continue to offer a unique lever in securing the Federal enterprise." OMB states that "[i]mplementing VDPs and, where feasible, running bug bounty programs, will help agencies more effectively align resources to achieve the greatest return on their cybersecurity investments."

OMB laid out the general parameters civilian agencies will need to meet. The agency explained that "[i]n order to maintain the interest of vulnerability reporters in reporting observed vulnerabilities in Federal information systems, agency VDPs must address the following areas:

- Clearly Identified Reporting Mechanism: Each Federal agency will clearly and publicly identify where and how vulnerabilities should be reported to it.
- Timely Feedback: Federal agencies will provide timely feedback to good-faith vulnerability reporters. Once a vulnerability is reported, those who report them deserve to know they are being taken seriously and that action is being taken. Agencies should establish clear expectations for follow-up communications with the vulnerability reporter.
- Clearly Worded VDPs: Federal agencies will provide clear assurances that good-faith security research is welcomed and authorized. Many government information systems are accompanied by strongly worded statements warning visitors against unauthorized use and implying legal reprisal. Agency VDPs should clearly articulate which systems are in scope and the set of vulnerability research activities that can be performed against them to protect those who would report vulnerabilities.

OMB stated that "[w]ith a clear VDP in place that addresses the above considerations, agencies make it easy for the public to know where to send a report, explicitly authorize types of testing allowed for a defined set of systems, and set an expectation of communication with vulnerability reporters regarding timely remediation and consultation with the researcher."

OMB would also task CISA with meeting certain implementation milestones. Under the draft policy, OMB directs CISA to undertake the following:

- Within 60 calendar days, CISA, in consultation with the Department of Justice (DOJ) and the National Institute of Standards and Technology (NIST) of the Department of Commerce (Commerce), will publish immediate actions agencies shall take to begin instantiating a VDP into agency's information security programs in an effective, responsible, and tailored manner.
- Within 150 calendar days, CISA will publish a Federal-wide strategy and implementation plan, which will stipulate how CISA will coordinate with agencies to identify and address persistent and common challenges that have emerged related to vulnerability reporting and remediation, or common threat or vulnerability findings.
- Within 240 calendar days, CISA will work with the Office of the Federal Chief Information Officer (OFCIO) and Federal agencies on the appropriate methods or mechanisms to coordinate the tracking of submitted vulnerabilities across the Federal enterprise, including where centralized CISA programs or services can help address common vulnerabilities.

OMB stated that "[i]n order to support the implementation work required by this memorandum, Federal agencies will need to take affirmative steps to put in place an initial VDP as a baseline for accepting reports from researchers." OMB said that "[b]eyond these initial actions, agencies will work with CISA to improve the maturity and scope of their VDPs, and integrate those policies into their overall risk management and information security programs." OMB explained that "[t]he following applies to all Federal agencies:

- Within 180 calendar days of the publication of this memorandum, each Federal agency shall publish a VDP, consistent with the requirements. Thereafter, agencies will work with OFCIO and CISA to continue maturing the processes developed for their VDPs and incorporate their VDP findings and remediation activities into their overall information security program.
- Within 180 calendar days of the publication of this policy, each Federal agency shall develop or update its internal vulnerability handling procedures to incorporate actions required by CISA pursuant to the previous section.
- Each Federal agency's CISO, or equivalent senior official of a different title, is responsible for implementing the above policy requirements.
- Agencies will use the quarterly Federal Information Security Modernization Act (FISMA) reporting to meet the requirements above, pursuant to additional guidance by OFCIO, in coordination with CISA.

Further Reading

- "Tech's liability shield becomes trade-deal flashpoint" – *Axios*. Speaker of the House Nancy Pelosi (D-CA) announced her late opposition to including language in the U.S.-Mexico-Canada Agreement (USMCA) of language granting liability protection for social media platforms akin to Section 230. Pelosi echoed House Energy and Commerce Committee Chair Frank Pallone (D-NJ) and Ranking Member Greg Walden's (R-OR)

objections lodged earlier this year to extending the provisions to the USMCA. However, given Pelosi's usual savvy approach, why did she wait until the end of negotiations?

- "We asked 2020 Democratic candidates 7 key questions on technology" – *Vox*. The following questions were put to the Democratic contenders, most of whom answered:
    - Should Facebook, Google, Apple, and/or Amazon be broken up? Why or why not?
    - How should platforms be held responsible for misinformation or hate speech on their sites?
    - In the event of a crime, should the government be able to access Americans' encrypted conversations?
    - Who should control Americans' online data, and how should tech companies be punished when they fail to properly protect and steward this data?
    - How, if at all, should tech companies be held responsible for the jobs they eliminate with their innovations?
    - Facial recognition is largely unregulated in the US. How, if at all, would you regulate facial recognition technology for surveillance and policing?
    - What's the most important tech-related issue that Americans are facing in the next four years?
- "American trash: How an e-waste sting uncovered a shocking betrayal" – *The Verge*. An organization dedicated to ensuring ethical e-recycling finds out a trusted partner was shipping e-waste off to China contrary to its commitments. This article explains the policy considerations arising from American's use and discarding of so many electronic devices.
- "Our Brains Are No Match for Our Technology" – *The New York Times*. The executive director of the Center for Humane Technology argues that radical government policies will be needed to address the challenges presented by big tech, for the human brain is proving no match.
- "Oracle allegedly underpaid women and minorities by $400 million. Now the details are set to come out in court." – *The Washington Post*. Despite a different culture from traditional corporate America, big tech seems to have a lot of the same issues regarding discrimination against women and minorities in terms of pay.
- "A Facebook rumor about white vans is spreading fear across America" – *CNN*. Social media posts alleging that men in white vans were kidnapping women to either harvest organs or sell them in slavery ran rampant and caused the mayor of Baltimore to issue a warning. Not a single such case has turned up.
- "TikTok settles children's data lawsuit one day after it was filed" – *The Verge*. The suit arose from the Federal Trade Commission's $5.7 million fine of TikTok for violating the privacy of children.
- "Evernote Gave Dark Web Dealer's Notes to the DEA" – *Vice's Motherboard*. Pursuant to a warrant, the Drug Enforcement Agency accessed the notes a drug dealer had left for himself in Evernote.
- "Phone logs in impeachment report renew concern about security of Trump communications" – *The Washington Post*. Incidental to the House's impeachment inquiry, the president's use of a cellphone is again posing security issues as it is possible and even likely that other countries are listening in. This revelation comes a few months after a story that Israel may have been targeting Trump's cellphone usage.
- "Britain's Boris Johnson took a selfie with a Huawei phone, a day after suggesting a tougher stance on the Chinese company." – *The Washington Post*. Even though he uses a

Huawei phone, British Prime Minister Boris Johnson may soon have his country join the U.S., Australia, and New Zealand in banning Huawei.