COPRA and CDPA: Similarities, Gray Areas and Differences

Müge Fazlioglu, CIPP/E, CIPP/US, Senior Westin Research Fellow

iapp

Two noteworthy proposals for a comprehensive federal data privacy law have entered the fray as the debate in U.S. Congress continues. They were introduced in the lead-up to the committee hearing scheduled for Dec. 4 at 10:00 a.m., "Examining Legislative Proposals to Protect Consumer Privacy." As lawmaking continues, it is worth looking into the similarities and differences between these proposals to see where bipartisan consensus exists, as well as the remaining points of controversy.

Introduced last week by Ranking Member of the Commerce, Science, & Transportation Committee Sen. Maria Cantwell, D-Wash., and sponsored by several Senate Democrats, the Consumer Online Privacy Rights Act aims to "provide consumers with foundational data privacy rights, create strong oversight mechanisms, and establish meaningful enforcement."

From the other side of the aisle, a "Staff Discussion Draft" of the United States Consumer Data Privacy Act, which is Sen. Roger Wicker's, R-Miss., proposal for a comprehensive federal data privacy law, was also released over Thanksgiving. Once introduced, the bill is likely to have the backing of several other Senate Republicans.

These two proposals provide the best available indication of where the two parties currently stand on federal data privacy legislation. While many of their provisions are nearly identical, there are also several notable differences between the two texts. This piece compares these two legislative proposals to better understand the places where clear-cut similarities, clear-cut differences and gray areas are found within these two bills.

Clear-cut similarities between COPRA and CDPA

Generally speaking, COPRA and CDPA share many things in common. In addition to their similarities in scope, both would require covered entities to obtain "affirmative express consent" from individuals before processing or transferring their sensitive covered data. Additionally, under both bills, covered entities must:

- Provide transparent privacy policies.
- Maintain "reasonable data security practices."
- Designate privacy officers and data security officers.
- Conduct annual privacy impact/risk assessments.
- Not deny goods or services to individuals who seek to exercise a privacy right.

Moreover, the two bills place similar obligations on federal agencies, such as the Federal Trade Commission and National Institute of Standards and Technology. These include obliging agencies to create:

- A report about digital content forgeries (by NIST).
- A study of algorithmic decision-making (by the FTC).
- A fund, called the Data Privacy and Security Victims Relief Fund (within the Department of Treasury).

Lastly, these two bills also contain a similar list of exceptions to the rules, rights and obligations they put in place. Namely, covered entities would not need to obtain affirmative express consent from an individual to process or transfer their covered data if it is "reasonably necessary, proportionate" and limited to a purpose such as to protect against illegal activity, comply with a legal obligation or conduct scientific, historical or statistical research in the public interest.

To provide a full sense of where COPRA and CDPA overlap, the sections below expound upon each of the main areas of similarity between the two texts.

Scope

Foremost among the commonalities between COPRA and CDPA is the scope of coverage and privacy rights outlined in the bills. COPRA applies to all entities that are subject to the jurisdiction of the FTC and process covered data, while CDPA takes it one step further, also folding in common carriers subject to the Communications Act of 1934 and nonprofits. The privacy protections outlined in each would provide, for the first time at the federal level, individuals of all ages with widely recognized privacy rights based on the fair information practice principles.

Consent to process/transfer sensitive data

Both COPRA and CDPA would require covered entities to obtain "prior, affirmative express consent" before processing or transferring an individual's sensitive covered data to a third party. The bills also require that covered entities provide individuals with "a clear and conspicuous means" (CDPA) or "a consumer-friendly means" (COPRA) to withdraw their consent.

Prohibition on denial of goods and services

Diving a bit deeper, COPRA and CDPA both contain a clear prohibition on the denial of goods and services to any individual who seeks to exercise a privacy right. That is, both bills would make it unlawful to require a consumer to waive their privacy rights to obtain a good or service. CDPA refers to these obligations under the section on "Consumer Loyalty."

Right to transparency

Both COPRA and CDPA also place nearly identical obligations on covered entities to make their privacy policies "publicly and persistently available," to disclose them "in a clear and conspicuous manner" or "in a conspicuous and readily accessible manner." The bills enact nearly identical requirements for the content of privacy policies, which must include contact information, the identity of any affiliate to which covered data is transferred, the categories of covered data collected, the processing purposes for each category, whether covered data is transferred, the categories of recipients, the purposes of the

transfers, a description of data retention practices, the purposes for such retention, information on how individuals can exercise their rights, a description of data security practices and the effective date of the privacy policy.

Right to data security

The bills contain a nearly identical "right to data security," which requires covered entities to maintain "reasonable data security practices" or "reasonable administrative, technical, and physical data security policies and practices to protect against risks to the confidentiality, security, and integrity of sensitive covered data." The specific, minimum requirements for these vary slightly between the two texts but generally include assessing vulnerabilities, taking preventative and corrective actions, and disposing of data after it is no longer needed.

Designation of privacy and data security officers

Both COPRA and CDPA would require covered entities to "designate [one] or more qualified employees as privacy officers; and [one] or more qualified employees … as data security officers." One difference, however, is that CDPA would allow the privacy officer and data security officer to be a contractor instead of an employee.

Neither bill assigns job-specific tasks to the privacy officer and data security officer roles. That is, aside from the difference in their titles, these roles have nearly identical responsibilities under these two laws. Under COPRA, both the privacy officer and data security officer would be responsible for: "implementing a comprehensive written data privacy program and data security program to safeguard the privacy and security of covered data throughout the life cycle of development and operational practices of the covered entity's products or services; annually conducting privacy and data security risk assessments, data hygiene, and other quality control practices; and facilitating the covered entity's ongoing compliance with this [act]." Similarly, under CDPA, both would be responsible for "coordinating the covered entity's policies and practices regarding the processing of covered data; and facilitating the covered entity's compliance with this [act]." Under CDPA, the privacy officer is also solely responsible for approving the findings of the mandated privacy impact assessment.

Codifying these roles in legislation is formal recognition that professionals already serving in such capacities are a critical component of privacy oversight and accountability mechanisms.

Privacy impact/risk assessments

Another area where the two bills largely agree is around the conduct of privacy impact/risk assessments. Both would require these to be completed on an annual basis and approved by the privacy officer or data security officer.

CDPA contains more details, however, on the requirements of privacy impact assessments. For example, CDPA specifies that these need to be "reasonable and appropriate in scope," taking into consideration the nature and volume of the covered data that is collected, processed or transferred, as well as the potential risks posed to individuals.

Digital content forgeries

Both COPRA and CDPA mandate that NIST publish a report about digital content forgeries within six months (CDPA) or one year (COPRA) after the enactment of the law. CDPA specifies that the report should

be concerned with their "impact … on individuals and competition" and would also require this report to be updated at least once every two years. In terms of the content of these reports, both COPRA and CDPA would require them to include a definition of digital content forgeries, a description of common and commercial sources of digital content forgeries in the U.S., an assessment of their "uses, applications, and adverse consequences," and "an analysis of the methods available to consumers to identify digital content forgeries," as well as a description of commercially available counter-measures and any other remedies available to protect individuals against them.

In addition, CDPA establishes a "Digital Content Forgery Prize Competition" whereby the director of NIST, in coordination with the FTC, would create "a prize competition to spur the development of technical solutions to assist individuals and the public in identifying on digital content forgeries and related technologies."

Data Privacy and Security Victims Relief Fund

Both bills would also establish a "Data Privacy and Security Victims Relief Fund" to which all civil penalties obtained by the FTC and the attorney general through enforcement of these acts would be deposited. The funds would be available to the FTC "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 COPRA/CDPA. If victims "cannot be located" or providing relief would be "otherwise not practical," the FTC could also use the funds "for the purpose of consumer or business education relating to data privacy and security or for the purpose of engaging in technological research that the Commission considers necessary to enforce" COPRA/CDPA.

FTC study of algorithmic decision-making

COPRA and CDPA would both require the FTC to conduct a study, using its authority under Section 6(b) of the FTC Act (15 U.S.C. 46(b)), to examine "the use of algorithms" to process data in ways that may violate federal anti-discrimination laws. CDPA would also require the FTC to publish a report of its findings within three years, to use those findings to "develop guidance to assist covered entities in avoiding discriminatory use of algorithms," and to publish an updated report within five years of the publication of the original.

Exceptions

Both bills agree on exceptions to the rules, rights and obligations they lay out when processing or transferring covered data is "reasonably necessary, proportionate, and limited" to purposes such as completing a transaction or fulfilling an order, performing internal system maintenance, detecting or responding to security incidents, protecting against "malicious, deceptive, fraudulent, or illegal activity," complying with a legal obligation, preventing individuals from suffering harm, effectuating product recalls, and conducting public or peer-reviewed scientific, historical or statistical research that is in the public interest.

COPRA also contains an explicit "journalism exception" by which none of the data privacy rights should apply to "the publication of newsworthy information of legitimate public concern to the public." In the same vein, CDPA contains a "constitutional avoidance" section that states the provisions of the law "shall be construed, to the greatest extent possible, to avoid conflicting with the Constitution of the United States, including the protections of free speech and freedom of the press established under the First Amendment to the Constitution of the United States."

The gray areas: Similar, yet different

In several ways, such as regarding the definitions of "covered data" and "sensitive covered data," COPRA and CDPA are neither in lock-step nor completely out of sync. Within these gray areas, the two bills employ similar or even identical language up to a point but then diverge in ways that would be critical to how they would likely be enforced. Some of these gray areas include:

- How "covered data" and "sensitive covered data" are defined.
- Level of protection for the rights to access, correction, deletion and data portability.
- Ability of consumers to opt out of transfers of covered data.

The following sections describe these issues, where a mix of similarities, as well as important differences between COPRA and CDPA, can be found.

Definition of "covered data"

The definitions of "covered data" under CDPA and COPRA share commonalities while possessing some key differences. In particular, COPRA's definition of "covered data" is broader as it also includes "derived data," which is any data "that is created by the derivation of information, data, assumptions, or conclusions from facts, evidence, or another source of information about an individual, household, or device used by an individual or household." COPRA's definition is also broader given that less data is excluded from its definition. Both COPRA and CPDA exclude deidentified data, employee data, and publicly available information or public records from the definition of "covered data," CDPA also excludes aggregated data.

Otherwise, there is an agreement between the two bills on the definition of "covered data" as any "information that identifies or is linked or reasonably linkable to an individual or a device."

Definition of "sensitive covered data"

While similar in many respects, the definitions of "sensitive covered data" diverge in COPRA and CDPA in several ways, specifically regarding geolocation information, data about online activities, telephone numbers and depictions of nudity.

For example, geolocation information is defined in COPRA as data "that reveals the past or present actual physical location of an individual or device," while in CDPA it is data that is "capable of determining with reasonable specificity the past or present actual physical location of an individual or device at a specific point in time." Thus, for geolocation data to be considered "sensitive covered data" under CDPA, it would need to contain temporal metadata.

Another difference is that the COPRA definition of "covered sensitive data" includes a broad description of data about online activities, which is any "information revealing online activities over time and across third-party website or online services." In contrast, CDPA only considers data about online activities to be sensitive if the information is "relate[d] to a category of covered data described" elsewhere in the definition. Thus, browsing history related to holiday films from the 1990s would likely fall under the definition of sensitive covered data under COPRA but not under CDPA. Browsing history related to flu vaccinations, however, likely would meet the definition under both bills.

Lastly, only COPRA includes photographs, films, video recordings, or other similar media that shows the naked or undergarment-clad private area of an individual, as well as telephone numbers, under its definition of "sensitive covered data."

Apart from these differences, the categories of "sensitive covered data" in the two bills overlap. Both of them include government-issued identifiers; data related to the diagnosis or treatment of past, present or future physical health, mental health or disability; financial account numbers, including debit card numbers, credit card numbers or any related security or access codes, passwords or credentials; biometric information; the content or metadata of an individual's private communications or the identity of the parties to such communication; account log-in credentials, such as a username or email address; information that reveals an individual's race, ethnicity, national origin, religion or union membership; information revealing the sexual orientation or sexual behavior of an individual; calendar information, address book information, phone or text logs, photos or videos maintained on an individual's device; and "any other covered data processed or transferred for the purpose of identifying the above data types" under the definition of "sensitive covered data." Both COPRA and CDPA also grant rulemaking authority to the FTC to determine other types of data that should fall within this definition.

Right to object/opt out of transfers

Although they bear a resemblance to one another, the "right to opt-out of transfers" of covered data to third parties established in COPRA is worded stronger than its counterpart "right to object" in CDPA. COPRA states explicitly that a covered entity "shall not transfer" data to a third party if an individual objects to it. COPRA would also require the FTC within 18 months to issue a rule "establishing one or more acceptable processes for covered entities to follow in allowing individuals to opt-out of transfers of covered data," which would have a number of requirements attached to it, including being "privacy protective," as well as informed by the FTC's experience with the National Do Not Call Registry.

CDPA, meanwhile, states that a covered entity "shall provide an individual with the right to object" to the processing and transfer of their covered data but does not tie in a similar prohibition on transferring data in those cases in which a person objects. Indeed, allowing consumers to object to something is not the same as allowing them to opt out of it.

Access, deletion, correction and data portability

Although both COPRA and CDPA provide protections for several individual rights around access, deletion, correction and data portability, there are differences — both subtle and obvious — in the extent to which they would protect these rights. In particular, COPRA places greater obligations on covered entities with respect to each of these individual rights. Indeed, under COPRA, each of these are each explicitly guaranteed, while CDPA instead guarantees the right to request these actions, with little or no obligations placed on covered entities to respond to or respect these requests.

Individual rights under COPRA

Sections 102 through 105 of COPRA establish the "right to access," "right to delete," "right to correct inaccuracies" and "right to controls," which includes the "right to data portability" and the "right to opt-out of transfers."

COPRA's right to access would require the covered entities provide individuals "in a human-readable format that a reasonable individual can understand, with a copy or accurate representation" of the data it has processed or transferred, as well as the name of any third party to whom the data has been transferred and a description of the purpose for the transfer.

COPRA's right to delete places the obligation on covered entities, upon receiving a verified request from an individual to "delete, or allow the individual to delete, any information in the covered data of the individual that is processed by the covered entity; and inform any service provider or third party to which the covered entity transferred such data of the individual's deletion request."

Similarly, the "right to correct inaccuracies" under COPRA requires covered entities to "correct, or allow the individual to correct, inaccurate or incomplete information" and inform any service providers or third party to whom the entity has transferred such data upon the receipt of a verified request.

Lastly, the right to data portability requires covered entities to "export the individual's covered data … in a human-readable format that allows the individual to understand such covered data of the individual; and in a structured, interoperable, and machine-readable format that includes all covered data or other information that the covered entity collected to the extent feasible."

Exceptions to these obligations include it being "demonstrably impossible" to comply with the request, although the volume of requests a covered entity receives cannot be considered as a factor in this demonstration. Another exception is when complying with the request would prevent the covered entity from performing an internal audit or accounting function, such as processing a refund or warranty claim. Publicly available information would also be exempted. Moreover, covered entities can decline to comply with requests that would impair "the publication of newsworthy information of legitimate public concern" or "the privacy of another individual or the rights of another to exercise free speech."

Individual rights under CDPA

Title I, Section 103 of CDPA describes the obligations of covered entities with respect to rights to access, correction, deletion and data portability. The right to access under CDPA requires covered entities to provide individuals access to their covered data "or an accurate representation" of their covered data that it and its service providers process.

Regarding the right to correction, CDPA requires covered entities to provide individuals with the "right to … request that the covered entity … correct inaccuracies or incomplete information." A unique feature of CDPA's language in this part is that it seems to merely establish a "right to request" correction rather than a "right to correction" itself. Similarly, under CDPA, covered entities are obligated to provide individuals with "the right to … request that the covered entity … delete or deidentify covered data" pertaining to the individual that it processes. Again, the literal wording of this section does not place any explicit obligation on a covered entity to delete or deidentify data only for it to provide individuals with the right to make such a request. Moreover, CDPA does not specify any conditions under which covered entities must comply with these requests, only that they must provide individuals with the right to make such a request.

Another key clause within CDPA would require covered entities to "provide an individual with the opportunity to exercise the rights … not less than twice in any 12-month period … free of charge." Presumably, after providing an individual with a right to access and request correction of inaccuracies, a covered entity would not seem to be obligated to provide either of these rights again or one of the others (deletion/deidentification and data portability) free of charge, at least not for another 12 months. In other words, the CDPA as currently written seems to allow covered entities to charge individuals if they want to exercise more than two of these individual rights within a 12-month period.

CDPA also contains several exceptions to the requirements regarding individual rights. Perhaps the most broadly worded exception would allow a covered entity to deny a request if it is "impossible or demonstrably impracticable to comply with." The statutory interpretation of "demonstrably impracticable" would seem to determine the level of protection that this provision affords. In addition, covered entities need not comply with a request if it would "require the entity to retain any covered data for the sole purpose of fulfilling the request" or "require the covered entity to reidentify covered data that has been deidentified."

Clear-cut differences between COPRA and CDPA

The clearest cut differences between COPRA and CDPA concern issues such as the preemption of state law and a private right of action. While CDPA would preempt any state law related to data privacy or security (with the exception of data breach laws), COPRA would leave in place state laws that afford a greater level of protection than it does. The private right of action is another issue in which the two bills sit on opposite sides of the fence.

In addition, numerous rights and/or obligations are only recognized in one of the two bills. For example, COPRA puts obligations on the CEOs of "large data holders" to certify to the FTC that their organizations have adequate controls in place to comply with COPRA. These obligations are absent in CDPA. Another example of this is the requirement in CDPA for covered entities that act as "data brokers" to register with the FTC, a requirement not found anywhere in COPRA.

Overall, the clearest issues of disagreement between the two bills are:

- Preemption of stricter state laws (only in CDPA).
- Private right of action (only in COPRA).
- Recognition of "harmful" data practices (only in COPRA).
- Shifting the burden of request verification to covered entities (only in COPRA).
- Protection of civil rights (only in COPRA).
- Algorithmic decision-making impact assessment (only in COPRA).
- Executive responsibilities (only in COPRA).
- Approved certification programs (only in CDPA).

- Data broker registration (only in CDPA).

- Establishment of a new FTC bureau (only in COPRA).

There are numerous clear-cut differences between the two laws, each of which are discussed in the sections below.

Duty of loyalty

COPRA includes a clause prohibiting covered entities from engaging in "deceptive" or "harmful" data practices. It defines "deceptive data practice" as an act or practice that violates Section 5(a)(1) of the FTC Act, a definition that is also found in CDPA. COPRA defines the term "harmful data practice" to mean any processing or transfer of data that causes or is likely to cause financial, physical or reputational injury to a person; physical or other offensive intrusion upon the solitude or seclusion of a person or their private affairs or concerns (using the "reasonable person" standard); or any "other substantial injury" to a person.

Preemption of state law

Not unexpectedly, the widest gulf between COPRA and CDPA can be found in the language of their pre-emption provisions. Although COPRA would supersede any state law that "directly conflicts" with its provisions, a state law would not be considered to be in direct conflict "if it affords a greater level of protection to individuals protected under this [act]." Thus, COPRA would essentially put in place a "floor" of privacy protection at the federal level and leave intact any state laws that contain stricter standards.

By contrast, CDPA includes a broad preemption provision that would prohibit states from "adopt[ing], maintain[ing], enforce[ing], or continu[ing] in effect any law, regulation, rule, requirement, or standard related to the data privacy or security and associated activities of covered entities." The only exception to the state law preemption provision in CDPA is for state laws "that directly establish requirements for the notification of consumers in the event of a data breach."

Private right of action

COPRA allows any individual who alleges a violation of it to "bring a civil action in any court of competent jurisdiction, [state] or [federal]." CDPA contains no such provision and would leave enforcement of the act entirely to the FTC and state attorneys general.

Verification of requests

COPRA contains unique provisions on the verification of requests that explicitly shift the burden of verification to companies. For example, if a covered entity cannot verify that the request for access/correction/deletion/etcetera of personal data comes from that person themselves, then it must "request additional information necessary" for verifying the identity of the individual and may not use that additional information for any other purpose. Moreover, COPRA contains a "burden minimization" clause that requires covered entities to "minimize the inconvenience to consumers relating to the verification or authentication of requests."

By contrast, under CDPA, covered entities need not comply with a request "if the covered entity cannot verify that the individual making the request is the individual to whom the covered data that is the subject of the request relate." Unlike COPRA, it does not place any additional obligations on covered entities regarding

the verification of requests. CDPA does, however, grant the FTC rulemaking authority to establish verification requirements, suggesting the legislators are leaving the details in this area to the commission.

Protection of civil rights

COPRA contains explicit civil rights protections, which prohibit covered entities from processing or transferring covered data "on the basis of an individual's or class of individuals' actual or perceived race, color, ethnicity, religion, national origin sex, gender, gender identity, sexual orientation, familial status, biometric information, lawful source of income, or disability" for several purposes, including marketing and advertising "for a housing, employment, credit, or education opportunity" in a way that "unlawfully discriminates against or otherwise makes the opportunity unavailable" to a person.

In addition, COPRA gives covered entities the right to request an advisory opinion from the FTC on the covered entity's "potential compliance with this subsection."

Algorithmic decision-making impact assessment

Unlike CDPA, COPRA would mandate the conduct of annual impact assessments for covered entities engaged in algorithmic decision-making or assisting others in doing so for the purpose of processing or transferring covered data to "facilitate advertising for housing, education, employment or credit opportunities, or an eligibility determination for housing, education, employment or credit opportunities or determining access to, or restrictions on the use of, any place of public accommodation." These impact assessments would need to describe and evaluate the development of the algorithmic decision-making process, including how it was designed and tested for accuracy, fairness, bias and discrimination, as well as to assess whether the algorithmic decision-making system produces results that are discriminatory on the basis of a set of characteristics, including actual or perceived race, color, ethnicity, religion, national origin, sex, gender, gender identity, sexual orientation, familial status, biometric information, lawful source of income, or disability.

Executive responsibility

One year after its enactment, COPRA would require the CEO or highest-ranking officer, as well as each privacy officer and data security officer of covered entities that are "large data holders," to annually certify to the FTC that the entity maintains "adequate internal controls to comply" with COPRA alongside "reporting structures to ensure that such certifying officers are involved in, and are responsible for, decisions that impact the entity's compliance" with COPRA.

Consent to transfer children's data

Obligations with respect to children's data are only found in CDPA, which requires covered entities to obtain affirmative express consent from a parent or guardian to transfer the data of an individual who is "less than 16 years of age."

Approved certification programs

Another distinguishing feature of CDPA is that it would empower the FTC to approve certification programs developed by one or more covered entities "or associations representing categories of covered entities" (e.g., the International Association of Privacy Professionals) to create standards or codes of conduct

regarding compliance with the law. CDPA lays out several requirements for these certification programs to be eligible for FTC approval, including "specify[ing] clear and enforceable requirements … that provide an overall level of privacy or data security protection that is equivalent or greater to" that provided by CDPA.

Moreover, the certification program would need to require participating covered entities to post a "clear and conspicuous public attestation of compliance" in a "prominent place." The program would also need to have a process in place for "independent assessment" of a covered entity's compliance with it. It would also need to create a website that describes the goals and requirements of the program, lists the participating entities, and allows for individuals to ask questions and file complaints. Lastly, the program would need to "take meaningful action for [noncompliance]," such as removing covered entities from the program or referring covered entities to the FTC.

Data broker registration

CDPA uniquely requires any covered entity that acted as a "data broker" in the previous calendar year to register with the FTC by January 31. Registration would entail providing a $100 fee, as well as information about its physical, email and internet addresses, and data brokers that fail to register would be subject to civil penalties. Lastly, CDPA requires the FTC to publish the registration information provided by data brokers on its website.

FTC powers and authority

Another area where COPRA and CDPA diverge is in their provision of power to the FTC. Namely, COPRA would give the FTC additional resources and authority for its enforcement, as well as for the enforcement of other federal laws regarding privacy and data security. Specifically, COPRA would require the FTC to establish within two years a new bureau that is "comparable in structure, size, organization, and authority to the existing [bureaus] with the [commission] related to consumer protection and competition." It would also give the FTC independent litigation authority, allowing it to "commence, defend, or intervene in, and supervise the litigation of any civil action under this subsection (including an action to collect a civil penalty) and any appeal of such action in its own name by any of its attorneys designated by it for such purpose." CDPA grants the FTC rulemaking authority in a number of specific areas but does not provide the significant resources envisioned under COPRA.

Other important differences

There are numerous other both minor and major language differences between the two laws, some of which would entail significant departures in terms of how they are enforced and the way that certain types of personal data are governed. For example, COPRA's requirements for "reasonable data security practices" apply to all covered data, whereas CDPA's apply only to "sensitive covered data." The data minimization requirements also differ as CDPA would allow collection, processing and transfer of covered data if it is necessary "to provide or improve a product," an exception to data minimization that is not found in COPRA.

In addition, the protections for COPRA whistleblowers are extensive. COPRA explicitly prohibits covered entities from discharging, demoting, suspending, threatening, harassing or discriminating against an individual who takes or is

suspected to take "a lawful action" in providing information about a violation of COPRA to the federal government or a state attorney general. COPRA also allows whistleblowers to bring an action alleging discharge or other discrimination against a covered entity under Section 42121(b) of Title 49, United States Code. By contrast, CDPA only requires the FTC to "consider" whether a covered entity retaliated against a whistleblower with no further elaboration.

Another difference between the text is that COPRA requires the implementation of "a comprehensive written data privacy program and data security program," while CDPA does not. To highlight another area of dissimilarity, COPRA would require the FTC to promulgate regulations regarding biometric data, while CDPA would allow but is not require it to do so. One final, small but important difference is that COPRA would go into effect 180 days after its enactment, while CDPA would go into effect two years after its passage.

Conclusion

Given the high-level similarities between the two bills and existence of several identical obligations within COPRA and CDPA, it seems possible that senators can find common ground to agree on a reconciled version of new federal data privacy legislation that would enact meaningful protections for consumer privacy. At a minimum, the definition of "sensitive covered data," the prohibition on the denial of goods and services for exercising privacy rights, consent to process sensitive data, the right to transparency, right to object/opt out of transfers, right to data security, exceptions, digital content forgeries, the designation of privacy and data security officers, privacy impact/risk assessments, an FTC study of algorithmic decision making, and the establishment of a "Data Privacy and Security Victims Relief Fund" all seem to be provisions about which Senate Democrats and Republicans mostly agree.

Yet, the differences between COPRA and CDPA, particularly on preemption of state law, a private right of action, executive responsibility and the scope of "sensitive data," indicate that Senate Democrats and Republicans still have their work cut out in the weeks and months ahead to find common ground.

The hearing scheduled for Wednesday, in which these bills will be discussed, will be an important indicator both of where negotiations stand and where they may be headed. If and when it comes to fruition, a new federal law would enhance the responsibilities of privacy professionals like nothing we have seen before, including under the EU General Data Protection Regulation and California Consumer Privacy Act.

Published 12/4/2019

SIDE-BY-SIDE COMPARISON OF THE **CONSUMER ONLINE PRIVACY RIGHTS ACT** AND **CONSUMER DATA PRIVACY ACT**

	Consumer Online Privacy Rights Act	Consumer Data Privacy Act
DEFINITION OF SENSITIVE COVERED DATA	"The term 'sensitive covered data' means the following forms of covered data: A government-issued identifier, such as a Social Security number, passport number, or driver's license number. Any information that describes or reveals the past, present, or future physical health, mental health, disability, or diagnosis 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. Biometric information. Precise geolocation information that reveals the past or present actual physical location of an individual or device. The content or metadata of an individual's private communications or the identity of the parties to such communications unless the covered entity is an intended recipient of the communication. An email address, telephone number, or account log-in credentials. Information revealing an individual's race, ethnicity, national origin, religion, or union membership in a manner inconsistent with the individual's reasonable expectation regarding disclosure of such information. Information revealing the sexual orientation or sexual behavior of an individual in a manner inconsistent with the individual's reasonable expectation regarding disclosure of such information. Information revealing online activities over time and across third-party website or online services. Calendar information, address book information, phone or text logs, photos, or videos maintained on an individual's device. A photograph, film, video recording, or other similar medium that shows the naked or undergarment-clad private area of an individual. Any other covered data processed or transferred for the purpose of identifying the above data types. Any other covered data that the [commission] determines to be sensitive covered data through a rulemaking pursuant to section 553 of title 5, United States Code."	"The term 'sensitive covered data' means any of the following forms of covered data of an individual: 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; Account log-in credentials such as a user name or email address, in combination with a password or security question and answer that would permit access to an online account. 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 covered data collected or processed by a covered entity for the purpose of identifying covered data described in another paragraph of this paragraph. Any other category of covered data designated by the [commission] pursuant to a rulemaking under section 553 of title 5, United States Code, 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."

	Consumer Online Privacy Rights Act	Consumer Data Privacy Act
DUTY OF LOYALTY	"A covered entity shall not engage in a deceptive data practice or a harmful data practice; or process or transfer covered data in a manner that violates any provision of this [act]." "The term 'deceptive data practice' means an act or practice involving the processing or transfer of covered data in a manner that constitutes a deceptive act or practice in violation of section 5(a)(1) of the Federal Trade Commission Act (15 U.S.C. 45(a)(1))." "The term 'harmful data practice' means the processing or transfer of covered data in a manner that causes or is likely to cause any of the following: Financial, physical, or reputational injury to an individual. Physical or other offensive intrusion upon the solitude or seclusion of an individual or the individual's private affairs or concerns, where such intrusion would be offensive to a reasonable person. Other substantial injury to an individual."	N/A
PROHIBITION ON DENIAL OF GOODS AND SERVICES	"A covered entity shall not condition the provision of a service or product to an individual on the individual's agreement to waive privacy rights guaranteed by sections 101, 105(a), and 106 through 109 of this [act]; and sections 102 through 104, and 105(b) and (c) of this [act] …"	"A covered entity shall not deny goods or services to an individual because the individual exercised any of the rights established under this title."
RIGHT TO TRANSPARENCY	"A covered entity shall make publicly and persistently available, in a conspicuous and readily accessible manner, a privacy policy that provides a detailed and accurate representation of the entity's data processing and data transfer activities."	"A covered entity that processes covered data shall, with respect to each service or product provided by the covered entity, publish a privacy policy that is disclosed, in a clear and conspicuous manner, to an individual prior to or at the point of the collection of covered data from the individual; and made available, in a clear and conspicuous manner, to the public."

	Consumer Online Privacy Rights Act	Consumer Data Privacy Act
RIGHT TO OBJECT/ OPT-OUT OF TRANSFERS	"A covered entity shall not transfer an individual's covered data to a third party if the individual objects to the transfer; and shall allow an individual to object to the covered entity transferring covered data of the individual to a third party through a process established under the rule issued by the [commission] pursuant to paragraph (2)." "Not later than 18 months after the date of enactment of this [act], the [commission] shall issue a rule under section 553 of title 5, United States Code, establishing one or more acceptable processes for covered entities to follow in allowing individuals to opt out of transfers of covered data." "The processes established by the [commission] pursuant to this subparagraph shall be centralized, to the extent feasible, to minimize the number of opt-out designations of a similar type that a consumer must make; include clear and conspicuous opt-out notices and consumer friendly mechanisms to allow an individual to opt out of transfers of covered data; allow an individual that objects to a transfer of covered data to view the status of such objection; allow an individual that objects to a transfer of covered data to change the status of such objection; be privacy protective; and be informed by the [commission's] experience developing and implementing the National Do Not Call Registry."	"A covered entity shall provide an individual with the right to object to the processing and transfer of such individual's covered data."
DATA MINIMIZATION	"A covered entity shall not process or transfer covered data beyond what is reasonably necessary, proportionate, and limited to carry out the specific processing purposes and transfers described in the privacy policy made available by the covered entity as required under section 102; to carry out a specific processing purpose or transfer for which the covered entity has obtained affirmative express consent; or for a purpose specifically permitted under subsection (d) of section 110 (on "Exceptions to Affirmative Express Consent")."	"… a covered entity 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."
RIGHT TO DATA SECURITY	"A covered entity shall establish, implement, and maintain reasonable data security practices to protect the confidentiality, integrity, and accessibility of covered data."	"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."
DESIGNATION OF PRIVACY OFFICER AND DATA SECURITY OFFICER	"A covered entity shall designate [one] or more qualified employees as privacy officers; and [one] or more qualified employees … as data security officers."	"A covered entity shall designate [one] or more qualified employees or contractors as privacy officers; and [one] or more qualified employees or contractors … as data security officers."

	Consumer Online Privacy Rights Act	Consumer Data Privacy Act
PRIVACY AND DATA SECURITY PROGRAMS, RISK/IMPACT ASSESSMENTS	"An employee who is designated by a covered entity as a privacy officer or a data security officer shall be responsible for, at a minimum implementing a comprehensive written data privacy program and data security program to safeguard the privacy and security of covered data throughout the life cycle of development and operational practices of the covered entity's products or services; annually conducting privacy and data security risk assessments, data hygiene, and other quality control practices; and facilitating the covered entity's ongoing compliance with this [act]."	"Not later than [one] year after the date of enactment of this [act] (or, if later, not later than [one] year after a covered entity first meets the definition of large data holder (as defined in section 2)), each covered entity that is a large data holder 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." "A privacy impact assessment required under paragraph (1) shall be reasonable and appropriate in scope given the nature of the covered data collected, processed, or transferred by the covered entity; the volume of the covered data collected, processed, or transferred by the covered entity; and the potential risks posed to individuals by the collection, processing, and transfer of covered data by the covered entity; shall be documented in written form and maintained by the covered entity unless rendered out of date by a subsequent assessment conducted under subsection (b); and shall be approved by the privacy officer of the covered entity." "A covered entity that is a large data holder shall, not less frequently than once every [two] years after the covered entity conducted the privacy impact assessment required under subsection (a), conduct a privacy impact assessment of the collection, processing, and transfer of covered data by the covered entity to assess the extent to which the ongoing practices of the covered entity are consistent with the covered entity's published privacy policies and other representations that the covered entity makes to individuals; any customizable privacy settings included in a service or product offered by the covered entity are adequately accessible to individuals who use the service or product and are effective in meeting the privacy preferences of such individuals; the practices and privacy settings described in subparagraphs (A) and (B), respectively meet the expectations of a reasonable individual; and provide an individual with adequate control over the individual's covered data; the covered entity could enhance the privacy and protection of covered data through technical or operational safeguards such as encryption, deidentification, and other privacy-enhancing technologies; and the processing of covered data is compatible with the stated purposes for which it was collected." "The privacy officer of a covered entity shall approve the findings of an assessment conducted by the covered entity under this subsection."

	Consumer Online Privacy Rights Act	Consumer Data Privacy Act
DATA PRIVACY AND SECURITY RELIEF FUND	"There is established in the Treasury of the United States a separate fund to be known as the 'Data Privacy and Security Relief Fund.'" "The [commission] shall deposit into the Relief Fund the amount of 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]."	"There is established in the Treasury of the United States a separate fund to be known as the 'Data Privacy and Security Victims Relief Fund.'" "The [commission] shall deposit into the Victims Relief Fund the amount of 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]."
RIGHT TO ACCESS	"A covered entity, upon the verified request of an individual, shall provide the individual, in a human-readable format that a reasonable individual can understand, with a copy or accurate representation of the covered data of the individual processed or transferred by the covered entity; and the name of any third party to whom covered data of the individual has been transferred by the covered entity and a description of the purpose for which the entity transferred such data to such third party."	"A covered entity shall provide an individual, immediately or as quickly as possible and in no case later than 45 days after receiving a verified request from the individual, with the right to access the covered data of the individual, or an accurate representation of the covered data of the individual, that is processed by the covered entity and any service provider of the covered entity."
RIGHT TO CORRECTION	"A covered entity, upon the verified request of an individual, shall correct, or allow the individual to correct, inaccurate or incomplete information in the covered data of the individual that is processed by the covered entity; and inform any service provider or third party to which the covered entity transferred such data of the corrected information."	"A covered entity shall provide an individual … with the right to … request that the 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."
RIGHT TO DELETION	"A covered entity, upon the verified request of an individual, shall delete, or allow the individual to delete, any information in the covered data of the individual that is processed by the covered entity; and inform any service provider or third party to which the covered entity transferred such data of the individual's deletion request."	"A covered entity shall provide an individual … with the right to … request that the covered entity delete or deidentify 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 individual's request."
RIGHT TO DATA PORTABILITY	"A covered entity, upon the verified request of an individual, shall export the individual's covered data, except for derived data, without licensing restrictions in a human-readable format that allows the individual to understand such covered data of the individual; and in a structured, interoperable, and machine-readable format that includes all covered data or other information that the covered entity collected to the extent feasible."	"A covered entity shall provide an individual … with the right to … to the extent that is technically feasible, provide covered data (except for inferred data) … in a portable, structured, standards-based, interoperable, and machine-readable format that is not subject to licensing restrictions."

	Consumer Online Privacy Rights Act	Consumer Data Privacy Act
VERIFICATION OF REQUESTS	"A covered entity shall not permit an individual to exercise a right described in sections 102 through 105(a) if the covered entity cannot reasonably verify that the individual making the request to exercise the right is the individual whose covered data is the subject of the request or an individual authorized to make such a request on the individual's behalf." "If a covered entity cannot reasonably verify that a request to exercise a right described in sections 102 through 105(a) is made by the individual whose covered data is the subject of the request (or an individual authorized to make such a request on the individual's behalf), the covered entity shall request the provision of additional information necessary for the sole purpose of verifying the identity of the individual and shall not process or transfer such additional information for any other purpose." "A covered entity shall minimize the inconvenience to consumers relating to the verification or authentication of requests."	"A covered entity shall not comply with a request to exercise the rights described in paragraph (1) if the covered entity cannot verify that the individual making the request is the individual to whom the covered data that is the subject of the request relates." "A covered entity shall not comply with a request to exercise the rights described in paragraph (1) if the covered entity cannot verify that the individual making the request is the individual to whom the covered data that is the subject of the request relates; and may decline to comply with a request that would require the entity to retain any covered data for the sole purpose of fulfilling the request; be impossible or demonstrably impracticable to comply with; or require the covered entity to reidentify covered data that has been deidentified." "Not later than 1 year after the date of enactment of this [act], the [commission] shall promulgate regulations under section 553 of title 5, United States Code, establishing requirements for covered entities with respect to the verification of requests to exercise rights described in subsection (a)(1)."
CONSENT TO PROCESS SENSITIVE DATA	"A covered entity shall not process the sensitive covered data of an individual without the individual's prior, affirmative express consent; shall not transfer the sensitive covered data of an individual without the individual's prior, affirmative express consent; shall provide an individual with a consumer-friendly means to withdraw affirmative express consent to process the sensitive covered data of the individual; and is not required to obtain prior, affirmative express consent to process or transfer publicly available information."	"A covered entity shall not without the prior, affirmative express consent of the individual to whom the covered data relates transfer sensitive covered data to a third party; or process sensitive covered data." "In obtaining the affirmative express consent of an individual to process the sensitive covered data of the individual as required under subsection (a)(2), a covered entity shall provide the individual with notice that shall include a description of the processing purpose for which consent is sought; clearly identify and distinguish 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; include a prominent heading that would enable a reasonable individual to easily identify the processing purpose for which consent is sought; and clearly explain the individual's right to provide or withhold consent."
CONSENT TO TRANSFER CHILDREN'S DATA	N/A	"A covered entity shall not transfer the covered data of an individual to a third-party without affirmative express consent from the individual or the individual's parent or guardian if the covered entity has actual knowledge that the individual is less than 16 years of age."
BIOMETRIC DATA	"Not later than [one] year after the date of enactment of this [act], the [commission] shall promulgate regulations pursuant to section 553 of title 5, United States Code, identifying privacy protective requirements for the processing of biometric information …"	"The [commission] may promulgate regulations pursuant to section 553 of title 5, United States Code, identifying additional privacy-protective exemptions for biometrics consent."

	Consumer Online Privacy Rights Act	Consumer Data Privacy Act
EXECUTIVE RESPONSIBILITY	"Beginning [one] year after the date of enactment of this [act], the chief executive officer of a covered entity that is a large data holder (or, if the entity does not have a chief executive officer, the highest ranking officer of the entity) and each privacy officer and data security officer of such entity shall annually certify to the [commission], in a manner specified by the [commission], that the entity maintains adequate internal controls to comply with this [act]; and reporting structures to ensure that such certifying officers are involved in, and are responsible for, decisions that impact the entity's compliance with this [act]." "A certification submitted under subsection (a) shall be based on a review of the effectiveness of a covered entity's internal controls and reporting structures that is conducted by the certifying officers no more than 90 days before the submission of the certification."	N/A
APPROVED CERTIFICATION PROGRAMS	N/A	"The [commission] 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 or more provisions in this [act]." "To be eligible for approval by the [commission], a certification program shall specify clear and enforceable requirements for covered entities participating in the program that provide an overall level of privacy or data security protection that is equivalent to or greater than that provided in the relevant provisions in this [act]; require each participating covered entity to post in a prominent place a clear and conspicuous public attestation of compliance and a link to the website . . . ; include a process for the independent assessment of a participating covered entity's compliance with the program prior to certification and on an annual basis; create a website describing the program's goals and requirements, listing participating covered entities, and providing a method for individuals to ask questions and file complaint about the program or any participating covered entity; take meaningful action for non-compliance with the relevant provisions of this [act] by any participating covered entity, which shall depend on the severity of the non-compliance and may include removing the covered entity from the program; referring the covered entity to the [commission] for enforcement; publicly reporting the disciplinary action taken with respect to the covered entity; providing redress to individuals harmed by the non-compliance; making voluntary payments to the United States Treasury; and taking any other action or actions to ensure the compliance of the covered entity with respect to the relevant provisions of this [act] and deter future non-compliance; and issue annual reports to the [commission] and to the public detailing the activities of the program and its effectiveness during the preceding year in ensuring compliance with the relevant provisions of this [act] by participating covered entities and taking meaningful disciplinary action for non-compliance with such provisions by such entities."

	Consumer Online Privacy Rights Act	Consumer Data Privacy Act
DATA BROKER REGISTRATION	N/A	"Not later than [Jan.] 31 of each calendar year that follows a calendar year during which a covered entity acted as a data broker, such covered entity shall register with the [commission] pursuant to the requirements of this section." "In registering with the [commission] as required under subsection (a), a data broker shall do the following: Pay to the [commission] a registration fee of $100. Provide the [commission] with the following information: The name and primary physical, email, and internet addresses of the data broker. Any additional information or explanation the data broker chooses to provide concerning its data collection and processing practices." "A data broker that fails to register as required under subsection (a) of this section shall be liable for a civil penalty of $50 for each day it fails to register, not to exceed a total of $10,000 for each year; and an amount equal to the fees due under this section for each year that it failed to register as required under subsection (a)." "The [commission] shall publish on the internet website of the [commission] the registration information provided by data brokers under this section."

	Consumer Online Privacy Rights Act	Consumer Data Privacy Act
WHISTLEBLOWER PROTECTIONS	"A covered entity shall not, directly or indirectly, discharge, demote, suspend, threaten, harass, or in any other manner discriminate against a covered individual of the covered entity because the covered individual, or anyone perceived as assisting the covered individual, takes (or the covered entity suspects that the covered individual has taken or will take) a lawful action in providing to the [federal government] or the attorney general of a [state] information relating to any act or omission that the covered individual reasonably believes to be a violation of this [act] or any regulation promulgated under this [act]; the covered individual provides information that the covered individual reasonably believes evidences such a violation to a person with supervisory authority over the covered individual at the covered entity; or another individual working for the covered entity who the covered individual reasonably believes has the authority to investigate, discover, or terminate the violation or to take any other action to address the violation; the covered individual testifies (or the covered entity expects that the covered individual will testify) in an investigation or judicial or administrative proceeding concerning such a violation; or the covered individual assists or participates (or the covered entity expects that the covered individual will assist or participate) in such an investigation or judicial or administrative proceeding, or the covered individual takes any other action to assist in carrying out the purposes of this [act]." "An individual who alleges discharge or other discrimination in violation of subsection (a) may bring an action governed by the rules, procedures, statute of limitations, and legal burdens of proof in section 42121(b) of title 49, United States Code. If the individual has not received a decision within 180 days and there is no showing that such delay is due to the bad faith of the claimant, the individual may bring an action for a jury trial, governed by the burden of proof in section 42121(b) of title 49, United States Code, in the appropriate district court of the United States for the following relief: (1) Temporary relief while the case is pending. (2) Reinstatement with the same seniority status that the individual would have had, but for the discharge or discrimination. (3) Three times the amount of back pay otherwise owed to the individual, with interest. (4) Consequential and compensatory damages, and compensation for litigation costs, expert witness fees, and reasonable attorneys' fees."	"In seeking penalties under section 401 for a violation of this [act] or a regulation promulgated under this [act] by a covered entity, the [commission] shall consider whether the covered entity retaliated against an individual who was a whistleblower with respect to original information that led to the successful resolution of an administrative or judicial action brought by the [commission] or the [attorney general] of the United States under this [act] against such covered entity."

	Consumer Online Privacy Rights Act	Consumer Data Privacy Act
DIGITAL CONTENT FORGERIES	"Not later than [one] year after the date of enactment of this [act], and annually thereafter, the [director] of the National Institute of Standards and Technology shall publish a report regarding digital content forgeries." "Each report under subsection (a) shall include the following: A definition of digital content forgeries along with accompanying explanatory materials. The definition developed pursuant to this section shall not supersede any other provision of law or be construed to limit the authority of any executive agency related to digital content forgeries. A description of the common sources in the United States of digital content forgeries and commercial sources of digital content forgery technologies. An assessment of the uses, applications, and harms of digital content forgeries. An analysis of the methods and standards available to identify digital content forgeries as well as a description of the commercial technological counter-measures that are, or could be, used to address concerns with digital content forgeries, which may include the provision of warnings to viewers of suspect content. A description of the types of digital content forgeries, including those used to commit fraud, cause harm or violate any provision of law. Any other information determined appropriate by the [director]."	"Not later than [one] year after the National Institute of Standards and Technology publishes the definition and materials required under subsection (a), the [commission] shall publish a report regarding the impact of digital content forgeries on individuals and competition." "Not later than [two] years after the publication of the report required under paragraph (1), and as often as the [commission] shall deem necessary thereafter, the [commission] shall publish an updated version of such report." "Each report required under this subsection shall include a description of the types of digital content forgeries, including those used to commit fraud, cause adverse consequences, violate any provision of law enforced by the [commission], or violate civil rights recognized under [federal] law; a description of the common sources in the United States of digital content forgeries and commercial sources of digital content forgery technologies; an assessment of the uses, applications, and adverse consequences of digital content forgeries, including the impact of digital content forgeries on consumers, digital identity, and competition; an analysis of the methods available to consumers to identify digital content forgeries as well as a description of commercial technological counter-measures that are, or could be, used to address concerns with digital content forgeries, which may include counter-measures that warn viewers of suspect content; a description of any remedies available to protect an individual's identity and reputation from adverse consequences caused by digital content forgeries, such as protections or remedies available under the Federal Trade Commission Act (15 U.S.C. 41 et seq.) or any other law; and any additional information the [commission] determines appropriate." "Not later than [one] year after 10 the date of enactment of this [act], the Director of the National Institute of Standards and Technology, in coordination with the Federal Trade Commission, shall establish under section 24 of the Stevenson-Wydler Technology Innovation Act of 1980 (15 U.S.C. 3719) a prize competition to spur the development of technical solutions to assist individuals and the public in identifying on digital content forgeries and related technologies." "Not later than [six] months after the date of enactment of this [act], the National Institute of Standards and Technology shall develop and publish a definition of 'digital content forgery' and accompanying explanatory materials."

	Consumer Online Privacy Rights Act	Consumer Data Privacy Act
		"In developing a definition of 'digital content forgery' under subsection (a), the National Institute of Standards and Technology shall consider the following factors: Whether the content is created with the intent to deceive viewers or listeners into believing the content was genuine. Whether the content is genuine or manipulated. The impression the content makes on a reasonable observer. Whether the production of the content was substantially dependent upon technical means, rather than the ability of another person to physically or verbally impersonate such person. The scope of technologies that may be utilized during the creation or publication of digital content forgeries, including video recording or film; sound recording; electronic image, or photograph; or any digital representation of speech or conduct." "The definition published by the National Institute of Standards and Technology under subsection (a) shall not supersede any other provision of law or be construed to limit the authority of any executive agency related to digital content forgeries."
PREEMPTION OF STATE LAW	"This [act] shall supersede any [state] law to the extent such law directly conflicts with the provisions of this [act], or a standard, rule, or regulation promulgated under this [act], and then only to the extent of such direct conflict. Any [state] law, rule, or regulation shall not be considered in direct conflict if it affords a greater level of protection to individuals protected under this [act]."	"No [state] or political subdivision of a [state] may adopt, maintain, enforce, or continue in effect any law, regulation, rule, requirement, or standard related to the data privacy or security and associated activities of covered entities." "Subsection (b) may not be construed to preempt [state] laws that directly establish requirements for the notification of consumers in the event of a data breach."
PROHIBITION ON DISRIMINATORY DATA PROCESSING	"A covered entity shall not process or transfer covered data on the basis of an individual's or class of individuals' actual or perceived race, color, ethnicity, religion, national origin, sex, gender, gender identity, sexual orientation, familial status, biometric information, lawful source of income, or disability for the purpose of advertising, marketing, soliciting, offering, selling, leasing, licensing, renting, or otherwise commercially contracting for a housing, employment, credit, or education opportunity, in a manner that unlawfully discriminates against or otherwise makes the opportunity unavailable to the individual or class of individuals; or in a manner that unlawfully segregates, discriminates against, or otherwise makes unavailable to the individual or class of individuals the goods, services, facilities, privileges, advantages, or accommodations of any place of public accommodation."	N/A
NEW FTC BUREAU	"The [commission] shall establish a new [bureau] within the [commission] comparable in structure, size, organization, and authority to the existing [bureaus] with the [commission] related to consumer protection and competition."	N/A

	Consumer Online Privacy Rights Act	Consumer Data Privacy Act
PRIVATE RIGHT OF ACTION	"Any individual alleging a violation of this [act] or a regulation promulgated under this [act] may bring a civil action in any court of competent jurisdiction, [state] or [federal]."	N/A
EXCEPTIONS	"A covered entity may process or transfer covered data without the individual's affirmative express consent for any of the following purposes, provided that the processing or transfer is reasonably necessary, proportionate, and limited to such purpose: To complete a transaction or fulfill an order or service specifically requested by an individual, such as billing, shipping, or accounting. To perform system maintenance, debug systems, or repair errors to ensure the functionality of a product or service provided by the covered entity. To detect or respond to a security incident, provide a secure environment, or maintain the safety of a product or service. 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 harm where the covered entity believes in good faith that the individual is in danger of suffering death or serious physical injury. To effectuate a product recall pursuant to [federal] or [state] law. To conduct scientific, historical, or statistical research in the public interest that adheres to all other applicable ethics and privacy laws and is approved, monitored, and governed by an institutional review board or a similar oversight entity that meets standards promulgated by the [commission] pursuant to section 553 of title 5, United States Code."	"… 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 subsection (c), to detect or respond to a security incident, provide a secure environment, or maintain the safety of a product or service. Subject to subsection (c), 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 section 553 of title 5, United States Code."