A Once and Future Federal Privacy Law?

Maureen K. Ohlhausen, Matthew R. Baker & Jonathon J. Duzak-Forestier

Although some say that the United States does not have a federal privacy law, that is—at best—a half-truth. Almost all companies have some existing federal privacy and data security obligations under the Federal Trade Commission Act and other sectoral-specific federal statutes. Outside of federal law, companies may be subject to the far-reaching EU General Data Protection Regulation (GDPR),[1] and to a growing number of state laws, most notably the California Consumer Privacy Act (CCPA). As the collection, use, and sharing of personal data grows in amount and complexity, and consumers and businesses increasingly navigate a variety of privacy and security regulations, there has been a clamor for Congress to enact comprehensive federal privacy legislation that will provide consumers more rights, businesses more uniform obligations, and the FTC increased regulatory and enforcement powers.

To do so, Congress must resolve several controversial issues. Chief among them is how federal privacy obligations would interact with current and emerging state laws in a borderless online marketplace. At the same time, there is wide agreement on some goals for any federal privacy legislation. One is to provide consumers clarity and visibility into data collection, use, and sharing practices, as well as empower consumers with choices and rights regarding these practices. Another is to provide a national, uniform set of protections and consumer rights throughout the digital economy. A final goal is to strengthen the FTC's enforcement powers, including the ability to impose large fines on companies that violate the new federal privacy obligations.

However, hard choices remain beyond these areas of convergence. Will all entities ultimately be subject to the same obligations or will common carriers and nonprofits, to the extent they currently escape FTC oversight, have different rules? Will the new detailed federal legislation broadly preempt state privacy laws or will states continue to forge their own paths when they do not directly conflict with the federal law? Who will enforce the law—the FTC alone or with the aid of state attorneys general? Will private rights of action be permitted?

This article will discuss current federal privacy law and survey the current three major federal privacy proposals. While it is difficult to predict whether a comprehensive privacy bill will pass, any assessment of what a future privacy bill may contain and its chance of success requires a firm understanding of current law, the points of convergence in the proposals, and the important areas of divergence that Congress will ultimately need to reconcile.

■

Maureen K. Ohlhausen *is chair of the antitrust group at Baker Botts LLP and former acting chairman and commissioner of the Federal Trade Commission from 2012 to 2018.* ***Matthew R. Baker*** *is a partner in the Baker Botts LLP San Francisco office.* ***Jonathon J. Duzak-Forestier*** *is a staff attorney in the Baker Botts LLP San Francisco office.*

[1] The GDPR is a data protection and privacy law in the European Union (EU) and the European Economic Area (EEA). It contains requirements relating to the processing of personal data of individuals and addresses the transfer of personal data outside the EU and EEA. The GDPR aims primarily to give individuals more control over their personal data and to simplify the regulatory environment for international businesses by unifying the regulation within the EU. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) 1.

Current U.S. Consumer Privacy Framework

There are several federal statutes that address privacy concerns. For example, the FTC Act's prohibition on unfair and deceptive acts or practices[2] protects individual consumer privacy on a general level and has served as the primary basis for enforcement against privacy and security violations online and offline for decades. The FTC also enforces the Children's Online Privacy Protection Act of 1998 (COPPA)[3] and related regulations,[4] which restricts collection and use of "personal data" pertaining to children under 13 by certain "covered operators" of websites and other online services without prior and "verifiable parental consent."[5]

Likewise, the Financial Services Modernization Act of 1999[6] (Gramm-Leach-Bliley or GLB) regulates the use and dissemination of consumers' "nonpublic personal [financial] information" (NPI)[7] by broadly-defined "financial institutions."[8] Under GLB, the FTC has issued regulations regarding the protection of NPI and has enforcement authority except where it is specifically assigned to other regulators.[9] Although not enforced by the FTC, the Health Insurance Portability and Accountability Act of 1996 (HIPAA) regulates the use of "Protected Health Information" held by "covered entities" and certain business associates. The Department of Health and Human Service has civil enforcement powers and the Department of Justice can impose criminal sanctions for some violations. Though these examples cover different subject matter, they all share the same basic purpose: to regulate the collection, use, and security of certain types of personal information.

In addition to various federal privacy laws, every state has some form of breach notification law, and, at the time of this writing, approximately 35 have data disposal laws, 30 have statutes that address data security vis-à-vis the government, 25 have similar laws concerning private actors, and 26 have data privacy laws that have been enacted, passed, or are pending.

The most comprehensive state data privacy and security law is the CCPA, which became effective January 1, 2020.[10] The first of its kind for the United States, the CCPA is designed to enhance California consumers' privacy and control over how companies use their personal data by providing the rights of transparency, access, deletion, and to opt-out from the sale of personal information. To enforce these rights and associated compliance requirements, the CCPA creates two enforcement mechanisms: (1) the California Attorney General can enforce compliance and obtain injunctive relief and civil penalties, and (2) a private right of action for security breaches, which allows impacted California consumers to recover statutory or actual damages for a breach that results from a business's failure to implement proper information security procedures and mechanisms.

---

[2] 15 U.S.C. § 45.

[3] 15 U.S.C. §§ 6501 et seq.

[4] 16 C.F.R. § pt. 312 (2013).

[5] *Id.* § 312.5(a)(1).

[6] 15 U.S.C. § 6801 et seq.

[7] *Id.* § 6809(4) ("The term 'nonpublic personal information' means personally identifiable financial information—(i) provided by a consumer to a financial institution; (ii) resulting from any transaction with the consumer or any service performed for the consumer; or (iii) otherwise obtained by the financial institution.").

[8] *Id.* § 6809(3)(A) ("[A]ny institution the business of which is engaging in financial activities as described in section 1843(k) of title 12.").

[9] *See id.* §§ 6801–09, §§ 6821–6827.

[10] Cal. Civ. Code § 1798.100 et seq.

2019: The Year of Federal Privacy Proposals

Rapidly evolving privacy legislation and regulation, such as the CCPA and GDPR, have forced companies to consider how they collect, process, use, and share personal data from consumers. The CCPA, though limited by its terms to California residents, may have a wide impact outside the state's borders as Californians engage in online commerce. Other state bills under consideration, such as those in Illinois,[11] New York,[12] and Washington,[13] could have similar effects. The emergence of state privacy laws, existing federal laws that protect sectoral-specific privacy interests, the patchwork of data breach notification statutes, and foreign data privacy collection and transfer restrictions, have created a widespread belief that a comprehensive U.S. federal consumer privacy bill is overdue.

The emergence of state privacy laws, existing federal laws that protect sectoral-specific privacy interests, the patchwork of data breach notification statutes, and foreign data privacy collection and transfer restrictions, have created a widespread belief that a comprehensive U.S. federal consumer privacy bill is overdue.

Hard on the heels of GDPR, the CCPA has nudged federal lawmakers into action, prompting them to propose a variety of federal bills. While several earlier bills were introduced,[14] three federal privacy laws proposed in late 2019 have garnered the most attention. Two of these bills were introduced by members of the U.S. Senate Committee on Commerce, Science, and Transportation. The Consumer Online Privacy Rights Act (COPRA) was introduced by Senator Cantwell (D-WA), Ranking Member of the Commerce Committee, on November 26, 2019.[15] Shortly thereafter, the U.S. Consumer Data Privacy Act of 2019 (CDPA) was introduced by Commerce Committee Chairman Senator Wicker (R-MS) on November 29, 2019.[16] Finally, the House released an untitled bipartisan privacy bill drafted by the House Energy and Commerce Committee (E&C Draft) on December 18, 2019.[17]

These bills share a focus on transparency, limits on data use, and individual consumer rights, but differ in their approach on numerous key areas, such as enforcement mechanisms and the hotly contested issue of federal preemption. For example, COPRA would coexist with state privacy laws to the extent that they do not directly conflict with any of its provisions,[18] while CDPA would replace all state data privacy laws.[19] We discuss below how each of the key areas are dealt with in the three legislative proposals.

---

[11] Data Transparency and Privacy Act, S.B. 2330, IL 101st Gen. Assemb. Reg. Sess. 2019–2020 (2020).

[12] New York Privacy Act, S.B. 5642, N.Y. Legis. Assemb. Reg. Sess. 2019–2020 (resubmitted 2020).

[13] Washington Privacy Act, S.B. 6281, WA 66th Leg. Assemb. Re. Sess. 2020 (2020).

[14] *See, e.g.*, Online Privacy Act of 2019, H.R. 4978, 116th Cong. (1st Sess. 2019) (includes individual privacy rights, requires comprehensive privacy and security requirements, and proposed a new federal agency—the United States Digital Privacy Agency—to enforce the Act); Designing Accounting Safeguards to Help Broaden Oversight and Regulations on Data Act, S. 1951, 116th Cong. (1st Sess. 2019) (requires data harvesters, like social medial platforms, to inform consumers and financial regulators of the data they collect and if the data is being leveraged by the platform for profit); American Data Dissemination Act of 2019, S. 142, 116th Cong. (1st Sess. 2019) (proposes a national consumer data privacy law that protects both consumers and the innovative capabilities of Internet economies and places much of the regulatory burden on the FTC).

[15] Consumer Online Privacy Rights Act, S. 2968, 116th Cong. (1st Sess. 2019) (Discussion draft) [hereinafter COPRA], https://www.congress.gov/116/bills/s2968/BILLS-116s2968is.pdf (last visited Feb. 10, 2020).

[16] U.S. Consumer Data Privacy Act of 2019, 116th Cong. (1st Sess. 2019) (Discussion draft) [hereinafter CDPA].

[17] H.R. 116th Cong. (1st sess. 2019) (Discussion draft).

[18] In other words, COPRA would set minimum standards upon which states could build—a concept that is sometimes referred to as "floor preemption."

[19] That is, CDPA expressly preempts any and all state laws seeking to regulate the same area.

Principal Federal Privacy Proposals

All three proposals enumerate: (1) the covered organizations to which the requirements and provisions apply; (2) the specific types of personal data covered; (3) the protected individuals and the rights they have with respect to the covered data; and (4) enforcement powers and rulemaking.

Covered Entity. COPRA applies to any entity or person that (1) is subject to the FTC Act and (2) processes or transfers covered data.[20] The E&C Draft's definition of "covered entity" extends the definition out slightly to include common carriers[21] and nonprofit organizations,[22] which are otherwise exempt from FTC jurisdiction. CDPA goes further still and extends coverage to "any person who operates in or affects interstate or foreign commerce."[23] The breadth of CDPA means that, in addition to common carriers (carrying out common carriage activities) and nonprofits, entities like Internet Service Providers, which are not currently considered common carriers, would be included alongside social media and search engines that collect similar types of personal data. COPRA's limitation to entities subject to the FTC Act is notable given efforts by the Obama-era Federal Communications Commission to reclassify broadband as a common carriage service.[24]

All three bills contain special provisions intended to reduce the burden on small businesses. While the definitions of "small business" are similar under the three proposals, each one treats them differently. Under COPRA and CDPA, a "small business" is any covered entity that did not, in the preceding three calendar years, (1) exceed $25 million in annual revenue; (2) annually process covered data of 100,000 or more individuals, households (COPRA only),[25] or devices; or (3) derive 50 percent or more of its annual revenue from transferring covered data.[26] The E&C Draft's definition is narrower in that a covered entity may not have processed the personal data of 50,000 or more individuals to qualify, and, like CDPA, does not include households.[27]

COPRA excludes small businesses from its requirements entirely,[28] whereas CDPA only excludes a small business from individual control and data minimization requirements,[29] which are discussed below under "Consumer Rights" and "Data Minimization," respectively. In an interesting provision that seems to reflect some aspects of COPPA, the E&C Draft provides that small businesses would be able to apply to the FTC for approval of self-regulatory guidelines rather than granting flat exclusions like those in COPRA and CDPA.[30] A small business in compliance with such FTC-approved guidelines would be deemed in compliance with the law,[31] although approval may be withdrawn under certain circumstances.[32]

---

[20] COPRA § 2(9).

[21] Common carriers in telecommunications are entities that provide wired and wireless communication services to the general public for a fee.

[22] The E&C Draft § 17(7).

[23] CDPA § 2(8).

[24] The FCC's effort at reclassification, which was upheld by the D.C. Circuit, was rescinded by the current FCC. *See* U.S. Telecom Ass'n v. FCC, 359 F.3d 554 (D.C. Cir. 2016).

[25] CDPA does not include "households." *See* CDPA § 108(d).

[26] COPRA §§ 2(9)(C), 23; CDPA § 108(d).

[27] The E&C Draft § 13(a)(1).

[28] COPRA § 2(9)(C).

[29] CDPA § 108(d).

[30] The E&C Draft § 13(a)(1).

[31] *Id.* § 13(a)(5).

[32] *Id.* § 13(a)(3)(C).

Finally, CDPA and the E&C Draft each require data brokers[33] to register annually with the FTC.[34] The former mirrors the provisions of the CCPA[35] and requires data brokers to provide their name, physical address, email, and website.[36] It also requires them to pay a $100 registration fee and imposes penalties for non-compliance.[37] The E&C Draft requires the FTC to create a centralized web-based registry of data brokers[38] "that process covered information [of more than 5,000 individuals per year]."[39] It must be accessible to the general public to allow consumers to identify the companies that hold their data and how they can exercise their rights to access, correct, and delete data held by brokers.[40] Data brokers must place a "clear and conspicuous notice" to consumers on their website identifying themselves as such.[41] It also requires them to provide more detailed information to the FTC than that required by CDPA, which will be included in the registry.[42] The E&C Draft calls for a $15,000 annual registration fee but is silent on penalties for non-compliance.[43]

Covered Data. Under COPRA, "covered data" encompasses information that "identifies, or is linked or reasonably linkable to an individual or consumer device, including derived data,"[44] which is covered data created based on assumptions about an individual, household, or device.[45] For example, a company may employ machine learning algorithms to draw inferences about an individual from collected data, such as preferences, intelligence, or a psychological profile. Notably, de-identified data,[46] employee data, and public records are excluded from covered data.[47] However, by including derived data linkable to a household, COPRA is broader than the typical federal definition of personal data and, in that way, similar to the broader sweep of the

---

[33] CDPA defines a data broker as "a covered entity that knowingly collects or processes on behalf of, or transfers to, third parties the covered data of an individual with whom the entity does not have a direct relationship." CDPA § 2(9). The E&C Draft, on the other hand, has somewhat broader terms: "(A) a covered entity that regularly collects, assembles, or maintains covered information and sells or licenses to a third party or is otherwise compensated for disclosing such information for the third party's own purposes; and (B) does not include a commercial entity to the extent that such entity processes information collected by and received from a third party concerning individuals who are current or former customers or employees of the third party to provide benefits to the employees or directly transact business with the customers." The E&C Draft § 17(12).

[34] CDPA § 203(a)–(b); the E&C Draft § 10(c)(1).

[35] CAL. CIV. CODE § 1798.99.80(d).

[36] CDPA § 203(b)(2).

[37] *Id.* § 203(c).

[38] The E&C Draft refers to them as "information brokers" except in one instance (Section 3(a)(1)(H)). For purposes of comparison we refer to them as data brokers throughout.

[39] The E&C Draft § 10(c)(1).

[40] *Id.* § 10(c)(2).

[41] *Id.* § 10(a).

[42] *Id.* § 10(c).

[43] *Id.* § 10(d)(2).

[44] COPRA § 2(8)(A).

[45] *Id.* § 2(11).

[46] De-identified data is defined as information that cannot reasonably be used to infer information about, or otherwise be linked to, an individual, a household, or a device used by an individual or household, provided that the entity (A) takes reasonable measures to ensure that the information cannot be reidentified or associated; (B) publicly commits to process and transfer the data in de-identified form and not attempt to reidentify or associate the data; and (C) contractually obligates any person or entity that receives the information to comply with all the requirements. *Id.* § 2(10).

[47] *Id.* § 2(8)(B).

CCPA. Although CDPA uses a similar standard to define covered data ("identifies or is linked or reasonably linkable"), it does not extend the definition to "households" and excludes aggregated data[48] and publicly available information.[49] The E&C Draft defines "covered information" as any information that is "linked or reasonably linkable to a specific individual [or consumer device],"[50] making it similar to CDPA, though it contains exclusions more like those in COPRA.[51]

Notably, all three proposed bills exclude employee data and de-identified data from the definition of covered data, although CDPA also excludes aggregated data.[52] CDPA further excludes publicly available information, which is broader than COPRA's exclusion of public records. This difference is important in connection with the ability to use personal data from social media posts, many of which are publicly available information[53] but would not qualify as public records.[54] The E&C Draft does not exclude public records or publicly available information from the definition of covered data. However, covered data that is in the public record may be exempted under the section addressing individuals' rights with respect to their data.[55]

The bills also separately define "sensitive covered data." While all three proposals include commonly identified sensitive elements similar to those found in the CCPA and GDPR, such as religious, political, or sexual information; health information; biometric information; and financial information,[56] COPRA extends to several other unique elements, including (1) the metadata of private communications; (2) email addresses and phone numbers; and (3) information regarding online activities over time and across third-party websites or online services.[57] All three allow the FTC to designate other covered data as "sensitive" through its rulemaking authority.[58]

Processing or transferring sensitive data requires affirmative express consent under all three bills (though it is referred to as "express, affirmative consent" in the E&C Draft) and each includes a non-exhaustive list of common types of sensitive biometric information.[59] CDPA also enumerates sensitive behavioral qualities from which identity could be established (e.g., sleep or exercise data),[60] whereas COPRA and the E&C Draft only contemplate physical qualities. COPRA, though, provides exclusions with respect to some basic physical characteristics (e.g., height, weight, hair color, and eye color) to the extent that they are not used as biometric information.[61]

---

[48] Aggregated data means "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." CDPA § 2(7)(D).

[49] *Id.* § 2(7).

[50] The E&C Draft § 17(8)(A)(i).

[51] *Id.* § 17(8)(A)(ii).

[52] "'[A]ggregated data' means 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." CDPA § 2(7)(D).

[53] The term "publicly available information" is defined to be inclusive of public records, and, generally, any information that is "widely available to the general public," such as on a website or otherwise through the internet. CDPA § 2(7)(G).

[54] COPRA defines public records to mean "information that is lawfully made available from Federal, State, or local government records." COPRA § 2(19).

[55] *See* the E&C Draft § 5 (a)(4).

[56] *See* COPRA §2(20); CDPA §2(20); the E&C Draft § 17(22).

[57] COPRA § 2(20).

[58] *Id.* § 2(20)(N); CDPA § 2(20)(M); the E&C Draft § 17(22)(B).

[59] COPRA §§ 105(c)(1)–(2), 2(3); CDPA § 104; the E&C Draft § 6(d)(2).

[60] CDPA § 2(3).

[61] COPRA § 2(3).

Consumer Rights. Consumers are afforded the rights to access, delete, and correct inaccuracies in their covered data under all three proposals,[62] though CDPA is the only bill that gives the covered entity the option to "delete *or de-identify*."[63] All three proposals also give consumers the right to obtain the identity of any third party to which a covered entity transferred covered data, along with the purpose for such transfer.[64] Under COPRA and CDPA, requests to delete or correct covered data must be transmitted to any third-party recipients.[65] The E&C Draft, however, does not explicitly extend the rights to delete and correct to third parties (although the bill requires companies to respond to requests received from third parties on the consumer's behalf).[66] In addition, COPRA and CDPA provide consumers a right of "portability," meaning consumers may obtain a copy of their covered data from the covered entity.[67]

All three proposals also give consumers the right to obtain the identity of any third party to which a covered entity transferred covered data, along with the purpose for such transfer.

CDPA and the E&C Draft both contain deadlines for companies to respond to consumer requests: 45 days—and, in the case of the E&C Draft—the possibility of an additional 45-day extension.[68] CDPA is the only bill that limits the number of consumer requests to two in a 12-month period.[69] COPRA does not address timing or frequency other than to state that companies must take the applicable action upon receiving a verified request.[70]

COPRA allows consumers the right to opt-out of having their personal data disclosed, released, shared, disseminated, sold, or licensed to other entities,[71] while CDPA more broadly gives them the right to opt-out of processing and transfer of personal data.[72] The E&C Draft allows consumers to opt-out if they do not want a company to process their covered information for first-party marketing purposes.[73] As discussed above, all three proposals require affirmative express consent before processing or transferring sensitive covered data[74] and a covered entity must provide some easy means by which a consumer may withdraw consent.[75]

Uniquely, the E&C Draft entitles an individual to access their consumer profile[76] or consumer score,[77] the source of their consumer score, and how the score will be used to make decisions about them.[78] A consumer score is a numeric value or categorization used to rate, rank, or seg-

---

[62] *Id.* §§ 102(a), 103–104; CDPA § 103(a); the E&C Draft § 5.

[63] CDPA § 103(a)(1)(C).

[64] COPRA § 102(a)(2); CDPA § 103(a)(1)(A); the E&C Draft § 5(a)(2)(C).

[65] COPRA §§ 102(a), 103–104; CDPA §§ 103(a)(1)(B)–(C).

[66] The E&C Draft § 5(c)(1)(C)(i).

[67] COPRA § 105(a); CDPA § 103(1)(D).

[68] *Id.* § 103(a)(1); the E&C Draft § 5(c)(1)(C).

[69] CDPA § 103(a)(2).

[70] COPRA § 102(a).

[71] *Id.* § 105(b).

[72] CDPA § 104(d).

[73] The E&C Draft § 6(c).

[74] COPRA § 105(c)(1)–(2); CDPA § 104; the E&C Draft § 6(d)(2).

[75] COPRA § 105(c)(3); CDPA § 104; the E&C Draft § 6(e)(2).

[76] Defined as "any covered information, including covered information resulting from any form of processing of an individual's covered information" and inferences drawn therefrom, "used to create a profile about the individual reflecting" certain characteristics of the individual. The E&C Draft § (17)(4).

[77] *See id.* § (17)(5).

[78] *Id.* § 5(a)(2)(F).

ment an individual or to predict certain characteristics of the individual. For example, a company might use information from a social media profile to create a numeric value for reliability or trustworthiness, and then use that value to determine whether to provide certain services. This provides access rights that are significantly broader than COPRA or CPDA, as the inferred data contained in such scores or reports often covers individual preferences, pre-dispositions, behaviors, attitudes, intelligence, aptitudes, fitness, abilities, interests, reliability, location, movements, or other such characteristics.[79]

Transparency. The three proposals impose similar transparency requirements on covered entities regarding the content and posting of privacy policies, though with a few notable differences.[80] All three require a covered entity to post a detailed privacy policy easily understood and readily accessible by consumers. COPRA, for example, requires the following information to be posted: (1) how to contact the company regarding privacy issues; (2) the categories of data collected and the purpose for collecting it; (3) whether the company transfers covered data and, if so, each category of service provider and third party to which it transfers the data, the identities of the third parties, and the purposes for the transfer; (4) the length of time the company will retain the covered data; (5) the company's retention, data security, and minimization policies; (6) how individuals can exercise their rights under COPRA; and (7) the effective date of the privacy policy.[81]

Pursuant to COPRA and CDPA, covered entities are prohibited from making changes to the posted policy that would materially weaken the protection of previously-collected covered data or the consumer's ability to exercise applicable rights without first obtaining "affirmative express consent" from affected consumers.[82] COPRA requires a company to include each category of service provider and third party to which it transfers covered data and also requires disclosure of the specific identity of third-party recipients. CDPA requires a company to disclose the identities of affiliates to which it may transfer data but only the categories of third-party recipients.[83] Likewise, the E&C Draft only requires disclosure of the categories of recipients.[84] Furthermore, while the E&C Draft's transparency requirements regarding a covered entity's privacy policy are substantially similar to those in CDPA, it incorporates language regarding consumer scores,[85] as explained above, and requires data brokers and large companies[86] to pay a fee and file more detailed privacy policies with the FTC.[87]

Data Minimization. Similar to principles of data minimization found within GPDR,[88] COPRA limits the collection and processing of covered data to that which is "reasonably necessary, proportionate, and limited" to carry out the specific processing purposes and transfers specified in

---

[79] *Id.* § 17(4), (5).

[80] *See* COPRA § 102(b); *see also* CDPA §§ 102(a)–(b); the E&C Draft § 3(a)(1).

[81] COPRA § 102(b).

[82] *Id.* § 102(d); CDPA § 102(d).

[83] *See* COPRA § 102(b)(3).

[84] *See* the E&C Draft § 3(a)(1)(G).

[85] *Id.* § 3(a)(1)(D)(iv).

[86] *Id.* § 3(a)(2) ("Each covered entity that either has annual revenue in excess of [$250,000,000] in the prior year or that processes covered information of more than [10,000,000] individuals [or consumer devices] in the prior year.").

[87] *Id.* § 3(a)(2), (b).

[88] The principle of data minimization involves limiting data processing to only what is required to fulfill the specific purpose for which the data was originally collected.

the privacy policy or for which the covered entity has obtained affirmative express consent.[89] For example, to fulfill an online product order, data minimization requires a business to collect only the personal information necessary to process the order and deliver the product, such as contact, delivery, and payment information. Collecting personal information wholly unrelated to the order, such as political affiliation, would be improper. CDPA uses similar language, but includes product improvement as an acceptable purpose.[90] Under the E&C Draft, the FTC would be responsible for drafting rules that require companies to retain data for only as long as "reasonably necessary for the purpose for which the data is processed," as well as ensure that covered information is only disclosed to third parties under certain conditions.[91] However, unlike COPRA and CDPA, this proposal does not address data minimization explicitly.

Data Security. COPRA and CDPA directly establish a requirement that a covered entity must maintain reasonable data security practices,[92] whereas the E&C Draft relies on the FTC to issue information security regulations and guidance.[93] Under COPRA, these practices must include, at a minimum, assessing vulnerabilities, taking preventive and corrective actions to mitigate vulnerabilities (which may include implementing administrative, technical, or physical safeguards), disposing of data when required, and training employees with access to covered data on safe data handling practices.[94] CDPA requires similar practices, but appears to limit the requirement to sensitive covered data.[95]

Duty of Loyalty. Under COPRA, organizations would be bound by a duty of loyalty, which prohibits covered entities from engaging in deceptive or harmful data handling practices.[96] Although not explicitly referenced as a "duty of loyalty," CDPA also prohibits covered entities from engaging in deceptive and harmful data practices by reference to the FTC Act.[97] The E&C Draft, however, remains silent on any explicit or implicit duty.

Oversight/Civil Rights. To oversee compliance and protection efforts, COPRA requires organizations to appoint a privacy and data security officer responsible for implementing a comprehensive data privacy program and conducting annual data risk assessments.[98] Additionally, companies that use algorithmic decision-making to determine the placement of advertisements for housing, jobs, credit, or educational opportunity based on collected covered data would be required to conduct an annual impact assessment to determine whether the system produces discriminatory results based on protected categories (e.g., race, color, religion, national origin, gender, sexual orientation, disability).[99] Companies would similarly be required to designate privacy

---

[89] COPRA § 106.

[90] *See* CDPA §105(a)(1).

[91] The E&C Draft § 7.

[92] *See* COPRA § 107; *see also* CDPA § 204.

[93] *See* the E&C Draft § 9.

[94] *See* COPRA § 107.

[95] CDPA §204(b).

[96] *See* COPRA § 101.

[97] CDPA § 401(a)(1).

[98] COPRA § 202.

[99] *Id.* § 108.

officers and data security officers to oversee compliance with CDPA.[100] The E&C Draft requires all data breaches to be reported to the FTC with supporting information about the company's security policies.[101]

New Bureau. COPRA directs the FTC to establish a new bureau to assist it with exercising its authority under the act.[102] Similarly, the E&C Draft requires the FTC to create a distinct division (in this case, the "Bureau of Privacy").[103] Its purpose would be to enable the FTC to issue regulations requiring companies to establish privacy programs and implement data security measures that support the size, nature, scope, and complexity of the company's data activities.[104] CDPA is silent on the matter.

Enforcement. All three bills grant enforcement power to the FTC and state attorneys general with similar terms. COPRA, however, is currently the only bill that provides consumers with a private right of action. Enforcement under COPRA would extend to the FTC, the state attorneys general, and consumers.[105] The FTC can initiate or intervene in, and supervise the litigation of, any civil action brought under COPRA.[106] The FTC must "notify the [state] Attorney General of any such action . . . or request that the Attorney General commence, defend, or intervene in any such action" or appeal on the FTC's behalf.[107] The FTC can impose civil penalties to be used for consumer redress.[108] In addition to FTC enforcement, a state can bring a civil action on behalf of its residents to enjoin violations, enforce compliance, and obtain damages, civil penalties, or other compensation.[109] If possible, the state is required to notify the FTC in writing before initiating a civil action and provide a copy of the complaint.[110]

Finally, COPRA would provide consumers a private right of action to enforce their privacy rights under the statute.[111] Courts may award prevailing consumers statutory, actual, or punitive damages,[112] attorneys' fees, and any other relief that the court deems appropriate.[113] Although CDPA and the E&C Draft also provide enforcement authority to the FTC and state attorneys general,[114] they do not provide for a private right of action.

Preemption. The issue of whether a federal privacy law should preempt all state privacy laws is a significant point of contention, which both COPRA and CDPA address directly. COPRA provides for limited preemption of state laws, displacing them only to the extent that they directly con-

---

100 *See* CDPA § 301.

101 The E&C Draft § 9(a)(4).

102 COPRA § 301(a)(1).

103 The E&C Draft § 14.

104 *Id.* § 9.

105 COPRA § 301(a)–(c).

106 *Id.* § 301(a).

107 *Id.*

108 *Id.* § 301(a)(3)(B).

109 *Id.* § 301(b).

110 *Id.* § 301(c)(2).

111 *Id.* § 301(c).

112 *Id.*

113 *Id.*

114 *See* CDPA §§ 401–402; *see also* the E&C Draft § 15.

flict with COPRA or a rule or regulation promulgated under it.[115] This creates potential compliance hurdles for covered entities operating in jurisdictions with conflicting state laws (i.e., state laws that may not conflict with COPRA, but that conflict with each other). CDPA, however, expressly preempts all state laws related to data privacy save for data breach notification laws, creating a more uniform compliance approach to privacy for covered entities.[116] The E&C Draft does not currently address preemption.

Consumers may benefit from a uniform federal privacy law with transparency requirements, robust security provisions, ample rights, and strong limitations on the use of their personal data. In addition, a single set of rules that apply independent of location will provide uniformity and simplicity for consumers.

Though COPRA generally preempts directly-conflicting state laws, it specifically preserves certain categories of state laws, such as data breach notification laws, laws protecting civil liberties, and consumer protection statutes of generally applicability (e.g., those that protect against unfair and deceptive practices).[117] It also prevents preemption of "Federal or State common law rights or remedies, or any statute creating a remedy for civil relief."[118] Conversely, CDPA replaces all state laws "related to the data privacy or security and associated activities of covered entities," other than breach notification laws,[119] effectively deleting the CCPA and all other state privacy laws and rendering any current enforcement actions thereunder moot.

The Elusive Federal Privacy Law

The net benefit to consumers of any privacy law turns on a number of factors: the breadth of the rights, protections, and remedies it provides; the extent to which the law impairs business operations and negatively affects consumer services and market competition; the extent of the FTC's enforcement authority; and, finally, the availability of resources to enforce the law.

Consumers may benefit from a uniform federal privacy law with transparency requirements, robust security provisions, ample rights, and strong limitations on the use of their personal data. In addition, a single set of rules that apply independent of location will provide uniformity and simplicity for consumers. Conversely, a patchwork of state privacy laws may confuse consumers while undermining their confidence and certainty as to how businesses handle their personal data. If consumers are inundated with different mechanisms that vary by applicable state law, exercising informed choices will become even more laborious, causing fatigue and indifference.

Moreover, if compliance is overly burdensome for companies due to multiple or even conflicting state laws, an unfettered private right of action, and an unnecessarily broad federal law, it could ultimately harm consumers. Severe restrictions may slow innovation, create barriers to entry, and even cause competitors to exit the market. Alternatively, companies could simply block users who are in states where the cost of compliance with privacy laws and the risk of liability outweigh the benefit of doing business there. Companies might also pass increased expenses on to consumers by making changes that reduce the quality of their services or moving to a fee-based model. Finally, poorly drawn or conflicting laws could negatively impact research that relies on the use of large sets of personal data. This, in turn, would stifle progress and have a significant long-term negative impact on innovation.

Thus, it will benefit all parties for Congress to create a strong unified nationwide standard for consumer data privacy and security that is flexible enough to accommodate rapidly developing

---

115 COPRA § 302(c).

116 CDPA § 404.

117 *See* COPRA § 302(b).

118 *Id.* § 302(d).

119 CDPA § 404(a)–(b).

technology. To be effective, a new law will need to give the FTC expanded enforcement powers and additional resources. Enabling state officials to enforce the new law along with the FTC would help to mitigate the overtaxing of federal resources.

Difficult choices remain, however, about the extent of federal preemption and private rights of action. Though it is hard to imagine any comprehensive bill forthcoming during an election year, concern about privacy and the threat of conflicting state laws will continue to drive talks in Washington. Unless Congress converges on an approach, a comprehensive federal privacy law will always remain in the future and achieving the goal of improved consumer protections paired with greater certainty for business will remain elusive.

Postscript

There is no doubt that the COVID-19 pandemic has affected the public debate on privacy regulation and that these events will influence Congressional efforts to enact a federal privacy law. Perspectives on the benefits and risks of data sharing and the need for a uniform federal approach may change as governments, businesses, and individuals alike focus on stopping the spread of the virus. This article, however, was written prior to the onset of the COVID-19 pandemic and thus does not assess the potential impact that it may have on consumer data privacy. ●