STRENGTHS AND WEAKNESSES OF NOTICE AND CONSENT REQUIREMENTS UNDER THE GDPR, THE CCPA/CPRA, AND THE FCC BROADBAND PRIVACY ORDER♦

SCOTT JORDAN*

ABSTRACT

We compare the notice and consent requirements of the three recent privacy regulations that are most likely to serve as the starting points for the creation of a comprehensive consumer privacy bill in the United States: the European General Data Protection Regulation, the California Consumer Privacy Act/California Privacy Rights Act, and the Federal Communications Commission's Broadband Privacy Order. We compare the scope of personal information under each regulation, including the test for identifiability and exclusions for de-identified information, and identify problems with their treatment of de-identified information and of pseudonymous information. We compare notice requirements, including the level of required detail and the resulting ability of consumers to understand the use and flow of their personal information, and identify deficiencies with consumers' ability to track the flow of their personal information. Finally, we compare consumer choices under each regulation, including when a consumer must agree to the use of their personal information in order to utilize a service or application, and find that none of the regulations take full advantage of the range of options, and thereby fail to disincentive tracking.

*Professor, Donald Bren School of Information and Computer Science, Samueli School of Engineering, University of California, Irvine. This material is based upon work supported by the Herman P. & Sophia Taubman Foundation and by the National Science Foundation under Grant No. 1956393.

1. INTRODUCTION

It is likely that the United States Congress will in the next few years pass a comprehensive consumer privacy bill. Several bills have been proposed during the last few years, and the California Consumer Privacy Act has added pressure for Congress to create a nationwide law.

There are three likely starting points for such a bill. The most comprehensive is the 2016 European General Data Protection Regulation (GDPR),[1] which sets a new standard for comprehensive consumer privacy protections. The United States Federal Communications Commission (FCC) followed soon after with its Broadband Privacy Order ("FCC Order"),[2] which focusses on consumer privacy for broadband Internet service. In 2018, California passed the California Consumer Privacy Act (CCPA),[3] which adopts some elements from both the GDPR and the FCC Order, but places the emphasis on the sale of personal information. In 2020, California passed the California Privacy Rights Act (CPRA),[4] which modifies some of the provisions of the CCPA.

Some researchers and some stakeholders have criticized the notice-and-consent approach to consumer privacy regulation, pointing out the difficulty that consumers have reading privacy notices and the powerful position that businesses have in constructing consent mechanisms. However, whether or not alternatives to notice-and-consent are incorporated into a future U.S. comprehensive privacy law, it is exceedingly likely that notice-and-consent will remain a critical part of any such law.

Our goal in this paper is to analyze and compare the notice and consent requirements of the GDPR, the FCC Order, and the CCPA/CPRA, and to discuss their strengths and weakness. We hope that such a comparison can be used by policymakers in the formulation of future privacy bills.

There are academic papers that separately analyze the GDPR, the FCC Order, and the CCPA, but comparisons between them are rare.

An overview of the GDPR's roots and goals can be found in Hoofnagle, van der Sloot, and Borgesios.[5] They explain the history of

[1] 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), OJ 2016 L 119/1 [hereinafter *GDPR*].

[2] Protecting the Privacy of Customers of Broadband and Other Telecommunications, 47 C.F.R. 64 (2016) [hereinafter *FCC Order*]. The Order was repealed by the United States Congress in 2017.

[3] California Consumer Privacy Act of 2018, CAL. CIV. CODE § 1798.100 (West 2018) (amended 2020) [hereinafter *CCPA*].

[4] California Privacy Rights Act of 2020, CAL. CIV. CODE § 1798.100 (West 2020) [hereinafter *CPRA*].

[5] Chris Jay Hoofnagle, Bart van der Sloot & Frederik Zuiderveen Borgesius, *The European Union*

European data protection and privacy laws prior to the GDPR;[6] the GDPR's scope;[7] Fair Information Practices;[8] the legal basis for processing personal data;[9] special requirements for sensitive personal data;[10] data transfers;[11] and enforcement.[12] They also broadly discuss the responsibilities of controllers and processors[13] and the rights of consumers.[14] However, they do not give detailed analyses of notice and consent requirements.

A summary of the GDPR's notice requirements, along with advice on how a business may comply with them, can be found in Hintze.[15] He briefly discusses the types of organizations subject to the GDPR[16] and then discusses in detail the required elements of privacy notices. His focus is broader than that of our paper, including not only notices regarding processing of personal data, but also notices regarding the identity of the controller;[17] the legal basis for processing personal data;[18] user rights to access, correct, and delete personal data;[19] the user right to data portability;[20] the user right to complain;[21] data transfers;[22] and data retention.[23]

A summary of the FCC Order can be found in Howell.[24] He briefly summarizes the Order's notice and consent requirements.[25] He also summarizes other provisions in the Order, including the FCC's statutory authority,[26] and data security.[27] However, most of the paper is focused on a comparison of the FCC Order with the approach taken by the Federal Trade Commission.

General Data Protection Regulation: What It is and What It Means, 28 INFO. COMMC'N TECH. L. 65 (2019).
6 *Id.* at 69–72.
7 *Id.* at 72–76.
8 *Id.* at 76–78.
9 *Id.* at 79–82.
10 *Id.* at 82–83.
11 *Id.* at 83–85.
12 *Id.* at 92–97.
13 *Id.* at 85–88.
14 *Id.* at 88–92.
15 Mike Hintze, *Privacy Statements under the GDPR*, 42 SEATTLE UNIV. L. REV. 1129 (2019).
16 *Id.* at 1131.
17 *Id.* at 1132–34.
18 *Id.* at 1138–39.
19 *Id.* at 1140–42.
20 *Id.* at 1142–43.
21 *Id.* at 1144.
22 *Id.* at 1144–47.
23 *Id.* at 1147–48.
24 Sean Howell, *Broadband Privacy*, 58 SANTA CLARA L. REV. 59 (2018).
25 *Id.* at 70–72.
26 *Id.* at 67–69.
27 *Id.* at 72.

A summary of the CCPA can be found in Pardau.[28] He briefly summarizes the CCPA's notice and consent requirements.[29] He also summarizes other provisions in the CCPA, including its scope[30] and user rights to access and delete personal information.[31]

There are a few academic papers that compare various aspects of the GDPR and the CCPA. Buresh compares the European and American principles and definitions of privacy, and discusses some of the relevant case law.[32] He then compares user rights under the GDPR and the CCPA. Blanke focuses on the treatment under the GDPR and the CCPA of inferences drawn from personal information.[33] However, neither paper goes into much detail on the similarities and differences in the notice and consent requirements of the GDPR and the CCPA.[34]

We are interested in our paper in comparing the notice and consent approaches taken in the GDPR, the FCC Order, and the CCPA/CPRA. We restrict our attention to the collection, use, and sharing of personal information, and to user consent over such collection, use, and sharing. We do not consider notices regarding other user rights, such as the right to access, correct, or delete personal information, which are surely worthy of attention, but require a separate analysis.

Below, in discussing provisions that are identical in the CCPA and the CPRA, we simply refer to the CPRA and in citations we use the section numbering of the CPRA. However, when discussing provisions that the CPRA modified from those in the CCPA, we discuss those differences.

We are interested in the scope of personal information under each regulation, including the degree to which information must identify a person in order to qualify as personal information, whether personal information extends to information related to devices, and what constitutes de-identified information. We are particularly interested in the similarities and differences in each regulation's notice requirements, including the detail of required disclosures, how well and how easily a consumer can identify the uses of various types of personal information, and how easily a consumer can track the flow of their personal information through the information ecosystem. We are also particularly

28 Stuart L. Pardau, *The California Consumer Privacy Act: Towards a European-Style Privacy Regime in the United States?*, 23 J. TECH. L. & POL'Y 68 (2018).
29 *Id.* at 96–99.
30 *Id.* at 92–93.
31 *Id.* at 94–96.
32 Donald L. Buresh, *A Comparison Between the European and the American Approaches to Privacy*, 6 INDON. J. INT'L & COMP. L. 253 (2019).
33 Jordan M. Blanke, *Protection for 'Inferences Drawn': A Comparison Between the General Data Protection Regulation and the California Consumer Privacy Act*, 1 GLOB. PRIV. L. REV. 81 (2020).
34 In addition, we disagree here with some of the comparisons drawn in Buresh. *See* Buresh, *supra* note 32.

interested in which choices each regulation affords to consumers, including when each regulation deems a take-it-or-leave-it choice appropriate, how each regulation draws the line between when opt-in and opt-out choices are appropriate, how each regulation handles sensitive personal information, and how each regulates financial incentives to give up privacy.

In Section 2, we analyze the scope of personal information under each regulation, including exclusions for de-identified information. Although some stakeholders have argued for a narrow definition of personal information, we find that both the GDPR and the CPRA have broad definitions of personal information that include household identifiers, non-unique identifiers, temporary identifiers, device identifiers, and information not paired with an identifier. However, we find that the GDPR's treatment of de-identified information is inadequate to protect it. We also find that both the GDPR's and the CPRA's treatment of pseudonymous information is inadequate to incentivize pseudonymization.

In Section 3, we briefly discuss how each regulation handles the common situation in which a business outsources a task to another company and discloses personal information as part of outsourcing that task.

In Sections 4 through 6, we compare and contrast the notice requirements of each regulation. In Section 4, we consider notices regarding collection. We find that although both the GDPR and the CPRA require notice of categories of personal information collected and the categories of sources from which it originates, these notices are insufficient to inform consumers of the sources and methods by which personal information is collected.

In Section 5, we consider notices regarding use. We find that although both the GDPR and the CPRA require notice about the purposes for collecting personal information, these notices are insufficient to inform consumers about the purpose for collecting specific categories of personal information.

In Section 6, we consider notices regarding sharing. We find that although both the GDPR and the CPRA require notice about the categories of recipients with whom personal information is shared, these notices are insufficient to inform consumers about the purposes for doing so or of the recipients of their personal information.

In Section 7, we briefly discuss requirements on accessibility, clarity, and format of required disclosures. The regulations differ on whether notices should be provided at the time of purchase of a service and/or at the time that personal information is collected or used.

In Section 8, we compare and contrast consent requirements, including take-it-or-leave-it, opt-out, and opt-in approaches. We find that the GDPR and the CPRA only agree on one thing: that functional use of non-sensitive information can be mandated through terms and conditions. The CPRA also allows terms and conditions to mandate functional use of sensitive personal information and non-functional use of sensitive personal information, while the GDPR allows neither. The CPRA requires opt-out consent for all other uses and all sharing, while the only type of consent the GDPR recognizes for such uses and sharing is opt-in. We find that neither the GDPR nor the CPRA take full advantage of take-it-or-leave-it, opt-out, and opt-in approaches, and neither properly disincentives tracking.

Finally, we conclude in Section 9 with a summary of these comparisons.

2. PERSONAL INFORMATION

The scope of the GDPR, the CPRA, and the FCC Order all critically depend on each regulation's definition of the personal information subject to their rules. Each regulation's definition of personal information in turn relies on two concepts: (1) personal identity and (2) information relating to a personal identity.

A. *Personal Identifiers*

The GDPR, the CPRA, and the FCC Order all rely on some notion of personal identity.

Under the GDPR and the CPRA, personal information is information that pertains to people, not to businesses, institutions, or other such entities.[35] The GDPR and the CPRA both use the term *natural person* to mean such a person.[36]

A common method of establishing identity is use of a *personal identifier*. However, there are many complexities and issues of debate as to what constitutes a personal identifier and how identifiers can be used to establish identity.

There is a small set of personal identifiers that almost all stakeholders agree should qualify as a personal identifier, including a person's name, personal telephone number, personal email address, and

[35] European Union Agency for Fundamental Rights and Council of Europe, *Handbook on European Data Protection Law*, at 85 (2018) [hereinafter *EU Handbook*], https://www.echr.coe.int/Documents/Handbook_data_protection_ENG.pdf [https://perma.cc/RT3Y-B9SD]; *CPRA*, *supra* note 4, § 1798.140(i).

[36] *GDPR, supra* note 1, art. 4(1); *CPRA, supra* note 4, § 1798.140(i).

government issued individual identifiers (e.g., driver's license number, social security number, or passport number).[37]

However, there have been repeated policy arguments over whether many other identifiers should qualify as personal identifiers.

One such disagreement is whether an identifier that belongs to a group of natural persons should qualify as a personal identifier. A common example is an identifier connected to a household (e.g., home postal address or home telephone number). Some stakeholders have argued that personal identifiers should be restricted to a single natural person, and thus that household identifiers should be excluded.[38] However, most stakeholders have argued that household identifiers should qualify as personal identifiers,[39] and the GDPR, the CPRA, and the FCC Order have all agreed.[40]

Similarly, stakeholders have also disagreed on whether a non-household identifier that is not unique to a single natural person (e.g., date of birth) should qualify as a personal identifier. Here, different regulations have taken various tacks. The CPRA defines a *probabilistic identifier* as an identifier that identifies a natural person "to a degree of certainty of more probable than not,"[41] and classifies such probabilistic identifiers as personal identifiers.[42] The GDPR classifies an identifier that belongs to a group of natural persons as a personal identifier *if and only if* the identifier is "reasonably likely to be used," either alone or in combination with other information, to identify a natural person, taking into account "the available technology at the time of the processing and technological developments."[43] For example, the European Union ("EU") suggests that "[d]ate and place of birth are often used" together to identify a natural person, and thus that date of birth may be considered to be a personal identifier.[44] Therefore, under the GDPR, it remains somewhat unclear how large the group may be to whom a personal identifier corresponds. However, we expect that the GDPR test for a personal identifier is largely similar to the CPRA test. The FCC Order uses a similar test to the GDPR: whether the identifier is "reasonably linkable" to an individual. The FCC Order explains that an identifier is reasonably linkable if it "can reasonably be used on its own . . . or in combination to identify an individual . . . or to logically associate with

37 *CPRA*, *supra* note 4, § 1798.140(v)(1)(A); *FCC Order*, *supra* note 2, ¶ 93.
38 *FCC Order*, *supra* note 2, ¶ 44.
39 *FCC Order*, *supra* note 2, ¶ 93.
40 *GDPR*, *supra* note 1, at Recital 18; *CPRA*, § 1798.140(v)(1); *FCC Order*, *supra* note 2, ¶ 44.
41 *CPRA*, *supra* note 4, § 1798.140(x).
42 *Id.* § 1798.140(ai).
43 *GDPR*, *supra* note 1, at Recital 26.
44 *EU Handbook*, *supra* note 35, at 90.

other information about a specific individual . . . ."[45] As examples, the FCC includes a person's date of birth or mother's maiden name.[46]

Another disagreement is whether an identifier that can be used to establish identity for only a limited period of time should qualify as a personal identifier. For example, there has been a spirited debate over whether an IP address assigned to a household should qualify as a personal identifier. One common argument made by those opposed to classifying a household's IP address as a personal identifier is that IP addresses are often assigned to a household for only a limited period of time.[47] However, the CPRA and the FCC Order both agree that temporary identifiers qualify as personal identifiers if they are persistent.[48] The CPRA explicitly incorporates this into its definition of *unique identifier*, which is defined in part as "a persistent identifier that can be used to recognize a consumer [or] a family . . . over time . . .," and the CPRA explicitly includes IP addresses.[49] The GDPR takes a slightly different tack, classifying a temporary identifier as a personal identifier *if* it can be reasonably used to identify an individual or household,[50] and European Commission ("EC") guidance states that an IP address temporarily assigned to a household qualifies.[51]

Yet another disagreement is whether a device identifier (e.g., a MAC address, IMEI, or advertising identifier) should qualify as a personal identifier. Some stakeholders have argued that device identifiers only identify a device, and that, without additional information about the natural person who is using that device, such a device identifier should not be classified as a personal identifier.[52] The FCC Order explicitly rejects that argument. The FCC Order explains that device identifiers are "easily linkable to an individual," and thus classifies device identifiers as personal identifiers.[53] The GDPR and the CPRA appear to take a narrower approach. The GDPR only classifies a device identifier as a personal identifier if it can be reasonably used to identify an individual or household.[54] EU guidance states that a "device . . . linked to an identification number" qualifies,[55] and EC guidance classifies advertising identifiers as personal identifiers.[56] The CCPA included device identifiers

45 *FCC Order*, *supra* note 2, ¶ 89.
46 *Id.* ¶ 93.
47 *Id.* ¶ 71.
48 *CPRA*, *supra* note 4, § 1798.140(ai); *FCC Order*, *supra* note 2, ¶ 93.
49 *CPRA*, *supra* note 4, § 1798.140(ai).
50 *GDPR*, *supra* note 1, at Recital 26.
51 *What Is Personal Data?*, EUR. COMM'N https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_en [https://perma.cc/HD9G-G5YD] [hereinafter *EC Personal Data*].
52 *See, e.g.*, *FCC Order, supra* note 2, ¶ 91.
53 *Id.* ¶ 91.
54 *GDPR*, *supra* note 1, at Recital 26.
55 *EU Handbook*, *supra* note 35, at 92.
56 *EC Personal Data, supra* note 51.

in its definition of *unique identifier*, but the CPRA modified that definition, restricting the inclusion to devices that are "linked to a consumer or family."[57]

As a result, we think that while the GDPR, the CPRA, and the FCC Order agree on most identifiers that they classify as personal identifiers, the GDPR and the CPRA may be slightly narrower than the FCC Order. The GDPR and the CPRA may classify only device identifiers that can be reasonably used to identify an individual or household as personal identifiers, while the FCC Order presumes that device identifiers can likely be used to identify individuals and thus always treats device identifiers as personal identifiers. It remains to be seen how much consequence this difference will have.

B. *Personal Information*

The GDPR, the CPRA, and the FCC Order each define the scope of information that falls within their rules. However, because they use different terms for similar concepts, in this paper we use the term *personal information* when we refer to the generic concept, and we use the regulatory specific terms when referring to each regulation's specific definition.

Stakeholders have argued vociferously over the scope of personal information subject to privacy regulations, with businesses often arguing for a narrow scope and privacy advocates often arguing for a broad scope.

The argument often starts with a disagreement over what makes information personal. Businesses often argue that information should be classified as personal information only if the information is paired with a personal identifier. As discussed above, businesses also often argue for recognition of a narrow set of personal identifiers, such as a person's name or personal telephone number. Thus such stakeholders are likely to view the information "Joan Smith visited the website www.webmd.com" as personal information, but do not view the information "a user with IP address 70.181.1.1 visited the website www.webmd.com" as personal information. Similarly, such stakeholders are unlikely to view the information "a person at location 38.89° N and -77.01° E visited the website www.webmd.com" as personal information. In contrast, privacy advocates often argue that information should be classified as personal information if the person to whom the information relates could be identified, using that information and/or using other information.

The GDPR adopts a definition of *personal data* (its version of personal information) closer to that proposed by privacy advocates than to that proposed by many businesses. The GDPR defines *personal data*

[57] *CCPA*, *supra* note 3, § 1798.140(x); *CPRA*, *supra* note 4, § 1798.140(aj).

as "any information relating to an identified or identifiable natural person."[58] There are two components to this definition that we must analyze: (1) "relating to" and (2) "identified or identifiable natural person."

Regarding the phrase "identified or identifiable natural person," the GDPR defines an *identifiable natural person* as a person "who can be identified, directly or indirectly . . . ."[59] It gives a list of examples of how a person may be identified, which we separate into two subsets.

First, the GDPR specifies that a natural person may be identified "by reference to an identifier such as a name, an identification number, . . . [or] an online identifier."[60] This method is common. Often, a data record will contain both a personal identifier and additional information relating to a person who is identifiable using the personal identifier. If the personal identifier is a person's name, the identification is direct. If the personal identifier is a personal telephone number, personal email address, or government issued individual identifier, the potential identification is indirect. Nevertheless, the GDPR considers the associated information to be *personal data,* because the personal identifier can be reasonably used to identify an individual or household "by the use of additional information" (e.g., a telephone directory).[61] Thus, any pairing of information relating to a person with a personal identifier results in that information being classified under the GDPR as *personal data*.

Second, the GDPR specifies that a natural person may be identified "by reference to . . . location data . . . or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person."[62] The EU clarifies that "it is possible to categorise [a] person on the basis of socio-economic, psychological, philosophical or other criteria and attribute certain decisions to him or her."[63] Thus, data records that contain no personal identifiers are also classified under the GDPR as personal data *if* the information in those records is "reasonably likely to be used," potentially in combination with other available information, "to identify the natural person" to whom the information relates.[64]

The arguments between stakeholders often continues with a disagreement over the types of information that should be considered to

[58] *GDPR*, *supra* note 1, art. 4(1).
[59] *Id.*
[60] *Id.*
[61] *Id.* at Recital 26; *see also EU Handbook, supra* note 35, at 89.
[62] *GDPR*, *supra* note 1, art. 4(1).
[63] *EU Handbook, supra* note 35, at 89 (quoting an opinion issued by the Article 29 Data Protection Working Party).
[64] *GDPR*, *supra* note 1, at Recital 26.

be personal. Businesses often argue that only certain categories of information (e.g., medical and financial information) should be classified as personal information. In contrast, privacy advocates often argue that any information relating to a person should be classified as personal information, whether or not that information is private, and whether or not that information is sensitive.

The GDPR adopts in its definition of *personal data* language that proposed by some privacy advocates, using the "relating to" phrase. The EU further clarifies that "relating to" means "information about a person" and that it includes not only "information pertaining to the private life of a person" but also "professional activities, as well as information about his or her public life."[65] As examples, the GDPR lists a "natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements."[66] The GDPR thus addresses a broad scope of information.

The FCC Order takes an approach similar to, but somewhat broader than, the GDPR's approach. The FCC Order defines *customer proprietary information* (its version of personal information) to include three overlapping types of information: (1) *personally identifiable information*, (2) *individually identifiable customer proprietary network information*, and (3) *content of communications*.

The first type, *personally identifiable information*, is roughly akin to the GDPR's *personal data*, and is defined as "any information that is linked or reasonably linkable to an individual or device."[67] Similar to the GDPR, the FCC Order explains that information is "reasonably linkable to an individual or device" if it "can reasonably be used . . . to logically associate with other information about a specific individual or device."[68] On this basis, the FCC Order classifies as *personally identifiable information* any information that is paired with a personal identifier.[69] This already makes the FCC Order's approach broader than the GDPR's approach, since the FCC Order classifies a broader range of device identifiers as personal identifiers than does the GDPR.

The second type of information that the FCC Order classifies as personal information is *individually identifiable customer proprietary network information*. The FCC built its Broadband Privacy Order on top of an existing statute, which requires confidentiality of a type of personal information called *customer proprietary network information* ("CPNI"). The statute defines CPNI to include "information that relates to the

65 *EU Handbook, supra* note 35, at 83, 86.
66 *GDPR*, *supra* note 1, art. 4(4).
67 *FCC Order*, *supra* note 2, app. A, § 64.2002(m).
68 *Id.* ¶ 89.
69 *Id.* ¶¶ 93–95.

quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service."[70] The FCC Order states that CPNI includes many elements of information that may be collected by a provider of broadband service, including: the geo-location of a person or device;[71] the domain names and IP addresses of the websites with which a person communicates;[72] traffic statistics;[73] application usage;[74] and information about a user's devices.[75] The FCC Order includes in its definition of personal information any CPNI that is "individually identifiable."[76] It further clarifies that such information is individually identifiable if "it can reasonably be used on its own, in context, or in combination to identify an individual or device."[77] Thus, under the FCC Order, a person's precise geo-location, web browsing history, and application usage is classified as personal information, even if it is *not* paired with a personal identifier.[78] In comparison, the GDPR classifies these types of information as *personal data* if and only if they can be used to identify a natural person.

The third type of information that the FCC Order classifies as personal information is *content of communications*, which it defines as "any part of the substance, purport, or meaning of a communication or any other part of a communication that is highly suggestive of the substance, purpose, or meaning of a communication."[79] The Order includes in *content of communications* many pieces of communications, including "the body of a webpage, the text of an email or instant message, the video served by a streaming service, the audiovisual stream in a video chat, [] the maps served by a ride-sharing app," "source and destination email addresses or website URLs, . . . contents of emails; communications on social media; search terms; web site comments; items in shopping carts; inputs on web-based forms; and consumers' documents, photos, videos, books read, [and] movies watched."[80] Noting that "[c]ontent is highly individualistic, private, and sensitive", the FCC Order classifies *content of communications* as personal information.[81] In comparison, the GDPR classifies these types of information as *personal data* if and only if they can be used to identify a natural person.

[70] *Id.* ¶ 47.
[71] *Id.* ¶ 65.
[72] *Id.* ¶¶ 68–69, 72.
[73] *Id.* ¶ 74.
[74] *Id.* ¶¶ 76–79.
[75] *Id.* ¶¶ 80–81.
[76] *Id.* at app. A, § 64.2002(f).
[77] *Id.* ¶ 111.
[78] *Id.* ¶ 177.
[79] *Id.* ¶ 102.
[80] *Id.* ¶¶ 103–04.
[81] *Id.* ¶ 101.

The CPRA also takes an approach similar to, but somewhat broader than, the GDPR's approach. The CPRA defines *personal information* as "information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household."[82] The phrase "relates to" is identical to that used in the GDPR's definition of *personal data*, and the phrase "could reasonably be linked, directly or indirectly, with" is similar to that used in the FCC Order's definition of *personally identifiable information*. It is unclear whether the CPRA's addition of the phrase "describes" broadens its definition, since it is unclear whether there is any information that "describes," but does not "relate to," a particular consumer or household.

The inclusion of the phrase "identifies" may be more consequential. "Information that identifies . . . a particular consumer of household" is simply a personal identifier. However, a personal identifier itself may or may not be considered to be private. Some personal identifiers are often public (e.g., a person's name, home postal address, or home telephone number). Other personal identifiers are not public but are shared with others with whom one communicates (e.g., a personal telephone number, personal email address, or household IP address). Yet other personal identifiers are typically private (e.g., government issued individual identifiers). The GDPR, the CPRA, and the FCC Order all exempt certain types of publicly available information from certain rules; we discuss this in Section 2.C. The CPRA and the FCC Order both treat private personal identifiers as personal information. In contrast, the GDPR treats a private personal identifier as *personal data* if and only if it is construed as "information about a person."

Finally, there is one other manner in which the CPRA's definition of *personal information* is broader than the GDPR's definition of *personal data*. The CPRA uses the phrase "a particular consumer or household," whereas the GDPR uses the phrase "identified or identifiable natural person," and the FCC Order uses the phrase "an individual or device." Recalling our discussion above about personal identifiers, because the CPRA's definition of *unique identifier* is broader than the GDPR's treatment of an "identifiable natural person," we correspondingly conclude that the CPRA's definition of *personal information* is broader than the GDPR's definition of *personal data*.

[82] *CPRA*, *supra* note 4, § 1798.140(v)(1).

C. *Exclusions from Personal Information*

The GDPR, the CPRA, and the FCC Order each exclude certain types of information from their definitions of personal information and/or place specific restrictions on their use.

i. Public Information

Some stakeholders have argued that *only* information that a person keeps secret should be classified as personal information.[83] If a regulation agrees to exclude from its definition of personal information any information that is not kept secret, the policy question is how wide a distribution of information renders it as information that is not kept secret. Some stakeholders have argued that any information that is widely distributed should be classified as public information. Other stakeholders have argued for an even broader definition of public information that includes any information that is commercially available. Yet other stakeholders have argued for a much narrower definition of public information that include only information that is publicly available from government sources.

The CCPA excluded only a narrow category of publicly available information from its definition of *personal information*, namely only "information that is lawfully made available from federal, state, or local government records."[84] As a result, information made available from government records is exempt from the CCPA's rules about the treatment of personal information. The CPRA substantially expanded the definition of *publicly available* information to also include information about a consumer that a consumer themself made publicly available, information about a consumer that the consumer disclosed to a third party "if the consumer has not restricted the information to a specific audience," and information about a consumer that was made publicly available by "widely distributed media."[85] The CPRA also excludes "lawfully obtained, truthful information that is a matter of public concern," even if that information is not publicly available.[86] The GDPR does not provide any similar exclusion from *personal data* for any type of publicly available information. Indeed, the GDPR's right-of-access requires disclosure of whether *personal data* came from a publicly accessible source.[87] However, the GDPR does exempt, from a prohibition on the use

[83] *See, e.g.*, *FCC Order*, *supra* note 2, ¶ 86.
[84] *CCPA*, *supra* note 3, § 1798.140(o)(2).
[85] *CPRA*, *supra* note 4, § 1798.140(v)(2).
[86] *Id.*
[87] *GDPR*, *supra* note 1, art. 14(2)(f).

of certain types of sensitive personal information, any "personal data which are manifestly made public by the data subject."[88]

ii. Aggregate Information

It is widely recognized that there are some forms of aggregate information whose collection, use, and sharing offer substantial benefit with minimal privacy risk. However, the contours of this aggregate information are widely debated. Some stakeholders have argued for a broad definition of aggregate information, including a dataset of multiple data records wherein each data record corresponds to a pseudonymous individual. Other stakeholders have argued for a narrow definition, including only summary statistics, but not including a dataset of multiple pseudonymized individual data records.

The FCC inherited a statute that defines *aggregate customer information* as "collective data that relates to a group or category of services or customers, from which individual customer identities and characteristics have been removed."[89] Some stakeholders focused on the latter part of the definition, and argued that the definition should be interpreted to include a dataset of multiple individual data records, *if* each data record has been anonymized in some manner that removes individual customer identities and characteristics. Other stakeholders focused on the earlier part of the definition and argued that the definition should be interpreted to include only summary statistics, namely collective data that relates to a group of customers. The FCC declined to settle this argument, instead incorporating *aggregate customer information* into a new definition of *de-identified information*, which we discuss below.

The GDPR, in contrast, does not explicitly define aggregate information. In a single place, it mentions that personal data processed for statistical purposes produces "aggregate data," and that such aggregate data no longer fits the definition of *personal data*, i.e., the aggregate data does not relate to an identified or identifiable natural person.[90] The GDPR thus applies its rules to the collection of the personal data used to create "statistical results" but not to the resulting aggregate data.[91] The GDPR also requires member States to further regulate the processing of personal data for statistical purposes, calling upon them to "determine statistical content, control of access, specifications for the processing of personal data for statistical purposes and appropriate

88 *Id.* at art. 9(2)(e).
89 *FCC Order*, *supra* note 2, ¶ 110, n.294.
90 *GDPR*, *supra* note 1, at Recital 162.
91 *Id.* at Recital 162.

measures to safeguard the rights and freedoms of the data subject and for ensuring statistical confidentiality."[92]

The CPRA creates a definition of *aggregate customer information* as "information that relates to a group or category of consumers, from which individual consumer identities have been removed, that is not linked or reasonably linkable to any consumer or household, including via a device."[93] As with the definition used in the FCC Order, this requires that aggregate customer information must relate to a group or category of individuals, and that individual identities be removed. In addition, it requires that aggregate customer information not be linked or reasonably linkable to any consumer. This is similar to the FCC Order's requirement that individual characteristics be removed, since the presence of such individual characteristics would otherwise render the information as *personal information* under the CPRA's definition. Furthermore, whereas neither the GDPR nor the FCC Order clarify whether aggregate information is restricted to summary statistics or includes a dataset of multiple anonymized individual data records, the CPRA explicitly states that *aggregate consumer information* does not include "one or more individual consumer records that have been de-identified."[94]

iii. Anonymous or De-Identified Information

The regulatory treatment of anonymized information is one of the most hotly debated elements of the GDPR, the CPRA, and the FCC Order. Some stakeholders argue that the use and sharing of datasets containing multiple pseudonymized individual data records is essential, and that pseudonymization techniques are mature enough to minimize privacy risks, and consequently that such datasets should be excluded from the definition of personal information. Other stakeholders argue that pseudonymization techniques are insufficient to protect the privacy of individuals whose data is included in such datasets, and consequently that such datasets should not be excluded from the definition of personal information. Yet other stakeholders argue that there are substantial benefits from the use and sharing of such datasets, but that privacy risks are significant, and consequently that specialized protections should be applied to the use and sharing of such datasets.

The GDPR contemplates multiple forms of anonymized or pseudonymized information. If the information collected "does not relate to an identified or identifiable natural person," namely if the information

92 *Id.*
93 *CPRA*, *supra* note 4, § 1798.140(b).
94 *Id.*

was anonymous starting from the point of collection, then it is not *personal data* (and it never was).[95]

More commonly, however, the information collected does relate to an identifiable natural person, and it is later anonymized or pseudonymized. If the anonymization technique creates a dataset containing only "personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable," then the resulting anonymized dataset is considered to no longer be *personal data*.[96] The GDPR does not, in general, apply specialized protections to anonymized datasets that are no longer considered to be *personal data*. This is confusing, since (as mentioned above) it does require member States to create specialized protections for the creation, use, and sharing of statistical datasets (which it considers to be one form of information anonymized so that it is no longer *personal data*).

In contrast, if the resulting pseudonymized dataset "could be attributed to a natural person by the use of additional information," then it remains *personal data*.[97] The GDPR encourages pseudonymization and encourages that any "additional information for attributing the personal data to a specific data subject" be "kept separately."[98]

The FCC Order takes a different approach and applies specialized protections. If information is "linked or reasonably linkable to an individual or device" then it qualifies as *personally identifiable information* and, thus, as personal information.[99] If a carrier creates a dataset of multiple anonymized individual data records, then such a dataset may qualify under the FCC Order as *de-identified information*, which is excluded from the definition of *customer proprietary information*.[100] The FCC Order does not define the term *de-identified information*, but it does lay out a set of requirements for information to qualify. First, the business that creates the anonymized dataset must itself "determine[] that the [anonymized] information is not reasonably linkable to an individual or device."[101] However, since the FCC believes that such a determination by the business is not sufficient protection,[102] the FCC Order also creates specialized protections that must be applied to the use and sharing of such datasets. Regarding use, the business must "publicly commit[] to maintain and use the data in a non-individually

95 *GDPR*, *supra* note 1, at Recital 26.
96 *Id.*
97 *Id.*
98 *Id.* at Recital 29.
99 *FCC Order*, *supra* note 2, app. A, § 64.2002(m).
100 *Id.* ¶ 106.
101 *Id.*
102 *Id.*

identifiable fashion and to not attempt to re-identify the data."[103] Regarding sharing, the business must "contractually prohibit[] any entity to which it discloses or permits access to the de-identified data from attempting to re-identify the data."[104]

The CPRA takes a similar approach to the FCC Order, also applying specialized protections. If a business creates a dataset of multiple anonymized individual data records, then such a dataset may qualify under the CPRA as *de-identified information*, which is excluded from the definition of *personal information*.[105] The definition of *de-identified information* starts as "information that cannot reasonably be used to infer information about, or otherwise be linked to, a particular consumer," which mimics the FCC Order's requirement that a business determine that de-identified information be not reasonably linkable to an individual or device.[106] It then adds "infer"[107] which appears in CPRA's expanded list of qualifiers in the definition of *personal information*.[108] The definition of *de-identified information* also incorporates the FCC Order's specialized protections. Regarding use, the business must "publicly commit[] to maintain and use the information in deidentified form and not to attempt to reidentify the information."[109] Regarding sharing, the business must implement "contractually obligate[] any recipients of the information to comply with all provisions."[110] These protections closely track those provided in the FCC Order.

3. Businesses and Service Providers

Both the GDPR and the CPRA apply to a wide range of businesses. The GDPR defines a *controller* as an entity that "alone or jointly with others, determines the purposes and means of the processing of personal data."[111] The CPRA similarly defines a *business* as an entity that "collects consumers' personal information, or on the behalf of which such information is collected and that alone, or jointly with others, determines

103 *Id.*
104 *Id*.
105 *CPRA*, *supra* note 4, § 1798.140(v)(3).
106 *Id.* § 1798.140(m). The CPRA modifies the CCPA's definition of *de-identified information*, which instead began with the phase "identify, relate to, describe, be capable of being associated with, or be linked, directly or indirectly, to a particular consumer." *See CCPA, supra* note 3, at § 1798.140(h).
107 *CPRA*, *supra* note 4, § 1798.140(m).
108 *Id.* § 1798.140(v)(1)(K).
109 *Id.* § 1798.140(m)(2). This requirement replaced the CCPA's requirement that a business implement "technical safeguards that prohibit reidentification of the consumer to whom the information may pertain" and make "no attempt to reidentify the information." *See CCPA*, *supra* note 3, §§ 1798.140(h)(1), (h)(4).
110 *CPRA, supra* note 4, § 1798.140(m)(3). This requirement replaced the CCPA's requirement that a business must implement "business processes that specifically prohibit reidentification of the information." *See CCPA*, *supra* note 3, §1798.140(h)(2).
111 *GDPR*, *supra* note 1, art. 4(7).

the purposes and means of the processing of consumers' personal information."[112] Below, we use the term *business* to refer to such an entity.

The CPRA exempts non-profit businesses and small businesses[113] from its rules. The GDPR does not exempt small businesses from any of its notice and consent rules, and it exempts non-profit businesses only from a prohibition on the use of certain types of sensitive personal information.[114]

Both the GDPR and the CPRA recognize that personal information is often shared by a business with other entities, sometimes creating large ecosystems based on personal information. The policy question is how to differentiate, if at all, between a business that collects personal information directly from consumers and the entities with which it shares this information. Sometimes a business shares personal information with another entity when it outsources a business task to such entity (e.g., when a business hires a company to process payments). Other times a business shares personal information with another entity when it seeks ad revenue (e.g., when a business hires an ad broker to place an ad on the business's website).

Both the GDPR and the CPRA may differentiate between these two different use cases. If the entity to whom personal information is disclosed may *only* use the shared information for purposes specified by the business sharing the personal information, then the entity is treated differently from the business that collected and shared the personal information. The GDPR refers to such an entity as a *processor*,[115] and the CPRA refers to such as entity as a *service provider* or *contractor*.[116] Below, we use the term *service provider* to refer to such an entity. When a business hires a company to process payments, it often limits the processor to using the personal information that the business provides to the processor for the purposes of processing the payment. In this situation, the payment processor is likely to qualify as a service provider.

In contrast, if the entity to whom personal information is disclosed may use the shared information in a manner in which that entity determines the purposes and means of any further processing of consumers' personal information, then this entity is considered to be a *controller* (under the GDPR) and a *business* (under the CPRA). When a business hires an ad broker to place an ad on the business's website, it

112 *CPRA*, *supra* note 4, § 1798.140(d).
113 Small businesses are those that collect personal information on fewer than 100,000 consumers, have annual gross revenues less than twenty-five million dollars, and derive less than fifty percent of these revenues from selling or sharing personal information. *See id.*.
114 *GDPR*, *supra* note 1, art. 9(2)(d).
115 *Id.* at art. 4(8).
116 *CPRA*, *supra* note 4, §§ 1798.140(j)(1), (ag)(1).

may or may not limit the ad broker to using the personal information that the business provides to the ad broker for the purposes of placing ads on that business's website. If so, the ad broker may qualify as a service provider. But commonly, a business hires an ad broker and allows the ad broker to use the shared personal information for the ad broker's own purposes, including building user profiles that the ad broker may use to sell other businesses personalized advertising. In this latter case, the ad broker is classified as a business, not as a service provider.

Given the importance of the distinction between a business and a service provider, it is critical to place proper limits on a service provider's use of personal information. The GDPR limits a processor's handling of personal information to that "governed by a contract . . . that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, [and] the type of personal data and categories of data subjects."[117] The CPRA similarly limits a service provider's handling of personal information to that "for a business purpose pursuant to a written contract [which] prohibits the [service provider] from [s]elling or sharing the personal information" and from "[r]etaining, using, or disclosing the personal information for any purpose other than for the business purposes specified in the contract."[118]

4. NOTICES REGARDING COLLECTION

The GDPR, the FCC Order, and the CPRA each have transparency requirements regarding the *collection*, *use*, and *disclosure* of personal information; and regarding *user choices* over the collection, use, and disclosure of personal information. We consider notices regarding *collection* in this Section, and notices regarding *use* and *disclosure* in the following two Sections. We consider notices regarding *consent* in Section 8.

The first policy question is how broadly to define *collection*. The GDPR does not formally define *collection* of personal information. However, it does define *processing* of personal information—which includes *collection*, *use,* and *disclosure* of personal information—as "any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction."[119] The GDPR requires a controller to

117 *GDPR*, *supra* note 1, art. 28(3).
118 *CPRA*, *supra* note 4, § 1798.140(ag)(1); *see also CPRA*, *supra* note 4, § 1798.140(j)(1).
119 *GDPR*, *supra* note 1, art. 4(2).

provide disclosures to individuals about its collection, use, and disclosure of personal data.[120]

The next policy question is when and where to require a business to disclose information about its collection of personal information. The GDPR, the FCC Order, and the CPRA have made different decisions about the locations and timing of such disclosures. As detailed below, some of the required GDPR disclosures must occur at the time the personal data is collected, some must occur within a reasonable period after the personal data is collected, and some only occur if and when an individual requests the information.

The FCC Order similarly requires a telecommunications carrier to provide disclosures about its collection, use, and sharing of *customer proprietary information*.[121] However, these disclosures must be made in a publicly available privacy policy, whereas disclosures mandated by the GDPR may occur at multiple times and places.

The CPRA similarly requires a *business* to provide disclosures about its collection, use, and disclosure of *personal information*.[122] As detailed below, some of these disclosures must occur at or before the point the personal information is collected, and some only occur if and when an individual requests the information.

A. *Categories of Personal Information*

The next policy question is what disclosures about collection of personal information to require a business to provide. Although almost all stakeholders agree that disclosures should contain some information about the types of personal information that business collects, they disagree over the level of detail that should be required, as well as the timing and placement of these disclosures.

Regarding the level of detail, the GDPR, the FCC Order, and the CPRA all require (at a minimum) that a business disclose the categories of personal information that it collects. However, they disagree about the timing and placement.

The GDPR's requirements differ depending on how the personal information was obtained. If the personal data was not obtained directly from the individual whom the personal data concerns, but instead from an intermediary, then the GDPR requires a controller to disclose, "within a reasonable period after obtaining the personal data, but at the latest within one month"[123] after the personal data was collected, "the

120 *Id.* at art. 12(1).
121 *FCC Order*, *supra* note 2, app. A, § 64.2003(a)–(b).
122 *CPRA*, *supra* note 4, § 1798.130.
123 *GDPR*, *supra* note 1, art. 14(3)(a).

categories of personal data"[124] the controller has collected. We expected that GDPR would include a similar disclosure requirement for a controller that collects personal data directly from individual people, and perhaps that such disclosures be provided at or before the time the personal data was collected; strangely, however, it is unclear whether the GDPR requires a controller who collects personal data directly from individual people to publicly disclose the categories of personal data collected.[125] Regardless of whether a controller collects personal information directly from individual people or from an intermediary, the GDPR also requires a controller to disclose, *upon request by the individual*, "the categories of personal data" that it has collected *about that individual*.[126]

The FCC Order similarly requires telecommunications carriers to "[s]pecify and describe the types of customer proprietary information that the telecommunications carrier collects."[127] The Order explains that "[i]n order to make informed decisions about their privacy, customers must first know *what types* of their information their provider collects through the customers' use of the service."[128] However, unlike the GDPR, the FCC Order requires that this disclosure be made both in the carrier's privacy policy and at the point of sale, rather than only upon request.

The CPRA takes a hybrid approach. A business must, in its privacy policy, disclose "the categories of personal information it *has collected* about consumers in the preceding 12 months."[129] A business must also disclose, at or before the point of collection,"[t]he categories of personal information *to be collected*."[130] Finally, upon request by the individual, a business must also disclose "[t]he categories of personal information it has collected *about that consumer*."[131]

Disclosure of the categories of personal information that a business collects informs consumers about the types of personal information collected, but it does not inform consumers about the *specific pieces* of personal information that a business has collected *about them*. Neither the GDPR nor the FCC Order includes a requirement for a business to disclose the specific pieces of personal information that a business has collected about an individual.[132] In contrast, the CPRA requires a

124 *Id.* at art. 14(1)(d).
125 Note the omission of such a requirement in the GDPR's Article 13, as compared to its inclusion in Article 14(1)(d). *GDPR*, *supra* note 1, art. 13, 14(1)(d).
126 *Id.* at art. 15(1)(b).
127 *FCC Order*, *supra* note 2, app. A, § 64.2003(b)(1).
128 *Id.* ¶ 127 (emphasis in original).
129 *CPRA*, *supra* note 4, § 1798.130(a)(5)(B) (emphasis added).
130 *Id.* § 1798.100(a)(1) (emphasis added).
131 *Id.* § 1798.110(a)(1) (emphasis added).
132 Note the omission of such a requirement in the GDPR's Article 13, as compared to the inclusion of the requirement to disclose categories of personal data in Article 15(b). *GDPR*, *supra* note 1, art.

business to disclose to a consumer, upon request, the "specific pieces of personal information the business has collected about that consumer."[133] This more detailed information can substantially increase the insight that a consumer has about a business's collection of personal information, since many consumers may learn more by seeing a specific list of personal information relating to them than by seeing a generic list of categories of personal information.

B. *Sources of Personal Information*

The next policy question is whether to require a business to disclose the method and/or source by which it collects personal information.

Unfortunately, neither the GDPR nor the CPRA requires a business that collects personal information directly from a consumer to disclose the *methods* by which it collects this personal information. This lack of disclosure about methods of collection is often used by businesses to obscure details about what personal information is collected. For example, a business may simply disclose that it collects information about which websites a consumer visits but fail to disclose whether it collects this information by examining packet headers or by collecting DNS queries. The latter information about the method used could have informed a consumer about whether adopting a different DNS provider would change the collection of personal information.

The approach of these privacy regulations towards disclosure of the *source* of personal information is better, but still not strong.

Under the GDPR, if a controller collects personal data from an intermediary, then the controller must also disclose "from which source the personal data originate, and if applicable, whether it came from publicly accessible sources."[134] This language seems to clearly articulate a requirement to disclose each source. However, the GDPR muddies the water in two other seemingly conflicting statements. First, upon request by the individual, a controller need only disclose "any *available* information as to their source."[135] Second, a GDPR recital comments that "[w]here the origin of the personal data cannot be provided to the data subject because various sources have been used, general information should be provided," which seems to weaken the requirement.[136]

Under the CPRA, a business must disclose, in its privacy policy, "[t]he categories of sources from which the personal information is

13, 15(b).
133 *CPRA*, *supra* note 4, § 1798.110(a)(5).
134 *GDPR*, *supra* note 1, art. 14(2)(f).
135 *Id.* at art. 15(1)(g) (emphasis added).
136 *Id.* at Recital 61.

collected."[137] CCPA regulations define *categories of sources* as "types or groupings of persons or entities from which a business collects personal information about consumers, described with enough particularity to provide consumers with a meaningful understanding of the type of person or entity."[138] The regulations give as examples of categories of sources: "the consumer directly, advertising networks, internet service providers, data analytics providers, government entities, operating systems and platforms, social networks, and data brokers."[139] Unlike the GDPR, however, the CPRA does not require the disclosure of the specific sources.

C. *Sources of Each Category of Personal Information*

It is unclear whether the GDPR or the CPRA requires a business to disclose, *for each category* of personal information collected, the source or category of sources of that category of personal information.

For example, consider a business that discloses that it collects both your address and your browsing history, and that separately discloses that it collects personal information both directly from you and from your Internet Service Provider ("ISP"). These separate disclosures fail to indicate whether the business collects your browsing history from your ISP.

The California Attorney General has gone back and forth on the interpretation of this part of the CCPA, at one point requiring the disclosure in a business's privacy policy of "*[f]or each category* of personal information collected, . . . the categories of sources from which that information was collected" and later only requiring separate unconnected disclosures of categories of personal information and of categories of sources.[140]

D. *Collection of Personal Information by Service Providers*

If the GDPR or the CPRA is interpreted *not* to require disclosures *for each category* of personal information collected of the source or category of sources of that category of personal information, then it becomes more difficult for a person to track down who collected which of their personal information. This challenge differs, however, based on

137 *CPRA*, *supra* note 4, § 1798.110(c)(2).
138 California Consumer Privacy Act Regulations, 11 CAL. CODE REGS. §§ 999.300, 999.301(d)(b)(1) (2020), https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/oal-sub-final-text-of-regs.pdf [hereinafter *CCPA Regulations*].
139 *Id.*
140 *Compare* First Proposed Text of California Consumer Privacy Act Regulations, 11 CAL. CODE REGS. §999.300, §999.308(b)(1)(d)(2) (2019), *available at* https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-proposed-regs.pdf [hereinafter *CCPA Regulations v1*] (emphasis added), *with CCPA Regulations*, *supra* note 138, § 999.308(c)(1)(d)–(e).

whether the recipient of the personal information is a service provider or another business.

We consider the case of a service provider here, and we defer the case of another business until Section 6. Under both the GDPR and the CPRA, a business that employs service providers remains responsible for disclosures regarding collection of personal information by each service provider on behalf of the business.[141] Thus, to determine which of their personal information is collected, a consumer need not examine the disclosures of each service provider that a business employs. Correspondingly, a business need not disclose the list of service providers that it employs.[142]

5. NOTICES REGARDING USE

In addition to the transparency requirements regarding *collection* of personal information (discussed in the previous section), the GDPR, the FCC Order, and the CPRA each have transparency requirements regarding the *use* of personal information.

A. *Purposes for Collecting Personal Information*

Many privacy policies have historically been quite vague about the uses of personal information by a business.

In the GDPR, the purposes for which personal data is collected play a prominent role in the regulations. Disclosures are mandated to include "the purposes of the processing for which the personal data are intended."[143] If the controller collects personal data directly from an individual, then this disclosure must be made at the time the personal data is collected.[144] If the controller collects personal data from an intermediary, then this disclosure must be made within a reasonable period after collection, but within one month.[145]

The FCC Order similarly requires the disclosure of how a telecommunications carrier uses customer proprietary information.[146] The FCC Order explains that "customers have a right to know *how* their information is being used" and that "[n]otices that omit these explanations fail to provide the context that customers need to exercise

141 *GDPR*, *supra* note 1, art. 28(3)(e).
142 The CPRA does however require a business to disclose in its privacy policy a "list of the categories of personal information it has disclosed about consumers for a business purpose in the preceding 12 months." *See CPRA*, *supra* note 4, § 1798.130(a)(5)(C)(ii). Such business purposes include "the use of personal information . . . for a service provider or contractor's operational purposes." *See CCPA*, *supra* note 3, §1798.140(e).
143 *GDPR*, *supra* note 1, arts. 13(1)(c), 14(1)(c).
144 *Id.* at art. 13(1).
145 *Id.* at art. 14(3)(a).
146 *FCC Order*, *supra* note 2, app. A, § 64.2003(b)(1).

their choices."[147] This information must be made both in the carrier's privacy policy and at the point of sale.

The CPRA similarly requires a business to disclose "the purposes for which the categories of personal information are collected or used."[148] However, unlike the GDPR, the CPRA requires this disclosure to be made both at or before the point of collection *and* in the business's privacy policy, regardless of whether the business collects the personal information directly from a consumer.

These disclosures inform consumers as to the use of their personal information. However, they do not inform users of the potential consequences. The GDPR requires special disclosures of the use of personal data for *profiling*, which it defines as "any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements."[149] Controllers are specifically required to disclose "the existence of automated decision-making, including profiling."[150] If a decision is based solely on automated processing, then a controller must also disclose "meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject."[151] Neither the FCC Order nor the CPRA have similar provisions specific to profiling.

B. *Purposes for Collecting Each Category of Personal Information*

It is unclear whether the GDPR, the FCC Order, or the CPRA requires a business to separately disclose, *for each category* of personal information collected, the purpose for collecting that category of personal information.

For example, consider a business that discloses that it collects both your address and the IP addresses of the websites you visit, and separately discloses that it collects personal information both to route your Internet traffic to the intended destination and for advertising. These separate disclosures fail to indicate whether the business uses the IP addresses of the websites that you visited for advertising (i.e., behavioral advertising), or whether the business uses your address for advertising (i.e., location-based advertising). These two possibilities have very different consequences.

147 *Id.* ¶ 128.
148 *CPRA*, *supra* note 4, §§1798.100(a)(1), 1798.110(c)(3).
149 *GDPR*, *supra* note 1, art. 4(4).
150 *Id.* arts. 13(2)(f), 14(2)(g), 15(1)(h).
151 *Id.* arts. 13(2)(f), 14(2)(g), 15(1)(h).

The California Attorney General has gone back and forth on the interpretation of this part of the CCPA, at one point requiring the disclosure in a business's privacy policy "*each category* of personal information collected [and], . . . the business or commercial purpose(s) for which the information was collected" and later only requiring separate unconnected disclosures of categories of personal information and of purposes.[152]

If the GDPR or the CPRA is interpreted *not* to require disclosures, *for each category* of personal information collected, of the purpose for collecting that category of personal information, then it becomes more difficult for you to exercise any rights to consent. We discuss this challenge in Section 8.

6. NOTICES REGARDING DISCLOSURE

In addition to the transparency requirements regarding *collection* and *use* of personal information discussed in the previous sections, the GDPR, the FCC Order, and the CPRA each have transparency requirements regarding the *disclosure* of personal information.

A. *Recipients of Personal Information*

It is well known that personal information is widely shared amongst a large number of businesses that comprise an advertising and tracking ecosystem.[153] One of the most fundamental issues in privacy regulation is how to address this widespread sharing.[154] To attempt to solve this problem, regulations often include both notice and consent provisions.[155] In this section, we discuss notice requirements, and in Section 8 we discuss consent requirements.

Privacy advocates often argue that a business should be required to disclose a list of the entities with which it shares personal information.[156] Many businesses, on the other hand, often argue that these relationships between a business and other entities are confidential.[157]

The GDPR requires controllers to disclose "the recipients or categories of recipients" to whom the personal data have been or will be disclosed.[158] The GDPR defines a *recipient* as "a natural or legal person, public authority, agency or another body, to which the personal data are

---

[152] *Compare CCPA Regulations v1*, *supra* note 140, § 999.308(b)(1)(d)(2) (emphasis added), *with CCPA Regulations*, *supra* note 138, §§ 999.308(c)(1)(d), (c)(1)(f).
[153] Scott Jordan, *A Proposal for Notice and Choice Requirements of a New Consumer Privacy Law*, 74 FED. COMM. L.J. 251, 269–70 (2022) [hereinafter *Jordan Proposed Statute*].
[154] *Id.* at 272–73.
[155] *Id.* at 254–61.
[156] *Id.* at 284–85.
[157] *Id.*
[158] *GDPR*, *supra* note 1, arts. 13(1)(e), 14(1)(e), 15(1)(c).

disclosed, whether a third party or not," and defines a *third party* as "a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data."[159] As with similar disclosures discussed above, the GDPR requires these disclosures be made at the time personal data is collected if it is collected directly from an individual, and within a reasonable period after collection, but within one month, if it is collected from an intermediary. In addition, the GDPR requires disclosure upon request by a consumer.

The FCC Order similarly requires telecommunications carriers to "[s]pecify and describe the categories of entities to which the carrier discloses or permits access to customer proprietary information . . . ."[160] As with similar disclosures discussed above, the FCC Order requires these disclosures be made both in the carrier's privacy policy and at the point of sale.

Another question that arises in the creation of privacy regulations is whether to treat service providers differently than businesses. In particular, the question arises of whether a consumer should be expected to be aware of the identity of service providers.

Unlike the GDPR, the CPRA distinguishes between disclosing personal information to a *service provider* and sharing personal information with a *third party*. The CPRA defines a *third party* as any entity other than a *business* or a *service provider*.[161] The CPRA uses the terms *share* and *sell* almost always in conjunction. They are defined as "sharing," "selling," "renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's personal information by the business to a third party . . . ."[162] The difference between the two terms is that selling is "for monetary or other valuable consideration,"[163] whereas sharing is "for cross-context behavioral advertising, whether or not for monetary or other valuable consideration, including transactions between a business and a third party for cross-context behavioral advertising for the benefit of a business in which no money is exchanged." [164] A business is not considered to be selling or sharing personal information when it discloses it to a service provider, because a service provider is not considered to be a *third party*.

159 *Id.* arts. 4(9)–(10).
160 *See FCC Order*, *supra* note 2, app. A, § 64.2003(b)(3).
161 *CPRA*, *supra* note 4, §§ 1798.140(ai)(2)–(3).
162 *Id.* §§ 1798.140(ad)(1), (ah)(1).
163 *Id.* § 1798.140(ad)(1).
164 *Id.* § 1798.140(ah)(1).

Recall from the discussion in Section 4 that, under both the GDPR and the CPRA, a business that employs service providers remains responsible for disclosures of collection of personal information by each service provider on behalf of the business.[165] Correspondingly, the CPRA does not require the disclosure of the service providers to whom it discloses personal information, or even of the categories of such service providers.

In the CPRA, disclosures of, and user choice over, the selling of personal information play a prominent role. The CPRA treats sharing of personal information with a third party quite differently than it does disclosure to a service provider. The CPRA requires a business to disclose the categories of third parties with whom the business shares personal information. CCPA regulations define *categories of third parties* as "types or groupings of third parties with whom the business shares personal information, described with enough particularity to provide consumers with a meaningful understanding of the type of third party," and give as examples "advertising networks, internet service providers, data analytics providers, government entities, operating systems and platforms, social networks, and data brokers."[166] A business must disclose in its privacy policy the "categories of third parties to whom [personal] information was disclosed or sold,"[167] and, upon request by a consumer, it must also disclose the "categories of third parties to whom the [customer's] personal information was sold or shared" or "disclosed for a business purpose."[168]

B. *Tracking Sources and Recipients of Personal Information*

If a consumer wishes to track the path of their personal information through the advertising and tracking ecosystem, it would be useful to know both the recipients of their personal information from a particular business and also the source of their personal information from a downstream business.

Regarding recipients of personal information, although the GDPR, the FCC Order, and the CPRA all require disclosure of *categories of recipients*, none require disclosure of *a list of recipients* to whom a business discloses personal information. The FCC Order explains that while it considered doing so, it rejected this approach, explaining that requiring disclosure of only categories of recipients "ensures that consumers understand what third parties that receive their information do

165 *GDPR*, *supra* note 1, art. 28(3)(e); *see supra* Part IV.
166 *CCPA Regulations*, *supra* note 138, § 999.301(e).
167 *Id.* § 999.308(c)(1)(g)(2).
168 *CPRA*, *supra* note 4, §§ 1798.115(a)(2)–(3). *See also CCPA Regulations*, *supra* note 138, §§ 999.313(c)(10)(d)–(f).

as a general matter" and "balances customers' rights to meaningful transparency with the reality of changing circumstances and the need to avoid overlong or over-frequent notifications."[169]

Regarding sources of personal information, recall from the discussion in Section 4 that the GDPR requires a business to disclose the sources of the personal information collected from an intermediary, but that the CPRA only requires a business to disclose the categories of such sources.

This combination of required disclosures about recipients and sources makes it very difficult for a consumer to track the flow of their personal information through the personal information ecosystem. A consumer has direct interaction with the businesses from whom the consumer directly obtains services. If privacy policies and other disclosures are accurate, concise, and readable, then a consumer might understand what personal information such businesses collect and how this personal information is used. However, because businesses are not required to disclose a list of recipients, a consumer cannot easily track the downstream flow of their personal information.

One may contemplate whether a consumer could instead track the flow of their personal information back to its original source. However, the CPRA does not make this possible, since it does not require disclosure of even the immediate source of personal information collected from an intermediary. Even under the GDPR, identifying the original source is likely to be infeasible. First, a customer would have to identify all of the businesses that might have collected the customer's personal information via intermediaries; that list is very long, and most of the businesses on it are unknown to consumers. Second, even if a consumer identifies such a third party and verifies that it is indeed collecting the consumer's personal information, the disclosure of the source of that personal information is likely to identify another intermediary rather than the original source. Thus, the consumer would have to repeat the process a number of times, until the original source is finally identified.

C. *Purposes for Disclosing Personal Information*

Notices about disclosure of personal information are of limited use unless a consumer also understands why a business is sharing their personal information.

In addition to requiring a telecommunications carrier to disclose the purposes for which it collects personal information and the categories of entities with whom it shares personal information, the FCC Order recognizes that "[a] critical part of deciding whether to approve of the

[169] *FCC Order*, *supra* note 2, ¶ 131.

sharing of information is knowing *who* is receiving that information and for what purposes."[170] For this reason, the Order also requires a telecommunications carrier to "[s]pecify and describe . . . the purposes for which the customer proprietary information will be used *by each category of entities*" to which it discloses or permits access to customer proprietary information.[171]

The CPRA similarly requires a business to disclose in its privacy policy "the business or commercial purpose for . . . selling personal information,"[172] and to disclose upon consumer request "[t]he business or commercial purpose for which it . . . sold the [customer's] personal information."[173]

However, the usefulness of these mandated notices is determined in part by the amount of detail. For example, consider a business that discloses that it shares both your address and your browsing history, and that separately discloses that it shares personal information both for advertising and to improve insurance rate-setting. These separate disclosures fail to indicate whether the business shares your browsing history for advertising (i.e., behavioral advertising) or for insurance rate-setting (e.g., risk estimation). These two possibilities have very different consequences.

The FCC Order requires a business to separately disclose, *for each category* of personal information collected, the purpose for sharing that category of personal information.[174] It is unclear whether the CPRA has a similar requirement for separate disclosures. The California Attorney General has gone back and forth on the interpretation of this part of the CCPA, at one point requiring the disclosure upon consumer request of "*each category* of personal information collected [and] the business or commercial purpose(s) for which it sold or disclosed the category of personal information" and later only requiring separate unconnected disclosures of categories of personal information and of purposes.[175]

The GDPR has a similar requirement for a controller to disclose the purposes for which it discloses personal information, but it is buried in the text. The GDPR requires a controller to disclose "the purposes of the processing for which the personal data are intended," and it defines *processing* to include disclosure to third parties.[176] It follows that the GDPR requires a controller to disclose the purposes for disclosure of

170 *Id.* ¶ 130 (emphasis in original).
171 *Id.* app. A, § 64.2003(b)(3) (emphasis added).
172 *CCPA Regulations*, *supra* note 138, § 999.308(c)(1)(f).
173 *See id.* § 999.313(c)(10)(c).
174 *FCC Order*, *supra* note 2, app. A, § 64.2003(b)(3).
175 *Compare CCPA Regulations v1*, *supra* note 140, § 999.313(c)(10)(d) (emphasis added), *with CCPA Regulations*, *supra* note 138, § 999.313(c)(10)(c).
176 *GDPR*, *supra* note 1, arts. 13(1)(c), 14(1)(c), 4(2).

personal information to third parties. However, as with the CPRA, it remains unclear whether the GDPR requires a controller to separately disclose the purposes for which personal information will be used by each category of recipients.

D. *Categories of Personal Information Disclosed*

Clearly, another critical part of a consumer decision about whether to allow sharing of one's personal information is knowledge of which of their personal information would be shared. For this reason, the FCC Order also requires a telecommunications carrier to "[s]pecify and describe under what circumstances the telecommunications carrier discloses or permits access *to each type* of customer proprietary information that it collects."[177]

As the sale or sharing of personal information features prominently in the CPRA, its rules about the categories of personal information that are shared are even more explicit. The CPRA requires a business to disclose in its privacy policy a "list of the categories of personal information it has sold or shared about consumers in the preceding 12 months. . . ."[178] CCPA regulations interpret the CCPA as also requiring the disclosure in privacy policies of the "third parties to whom [each category of personal information] was . . . sold."[179] Furthermore, upon consumer request, a business must disclose the "categories of personal information that the business sold or shared *about the consumer* . . . for each category of third parties to whom the personal information was sold or shared."[180] Even though the CPRA does not require disclosure of even the categories of service providers, it does require a business to disclose in its privacy policy a "list of the categories of personal information it has disclosed about consumers for a business purpose in the preceding 12 months."[181]

Surprisingly, it is unclear whether the GDPR has a similar requirement that a controller disclose the categories of personal data disclosed to third parties. The problem stems from the GDPR's exposition of required disclosures. First, as mentioned above, the disclosure requirements when a controller shares personal data with third parties are buried in the requirement to disclose "the purposes of the processing for which the personal data are intended." So, we must examine whether the required disclosure of these purposes includes disclosure of the purposes *for a particular category* of personal data.

177 *FCC Order*, *supra* note 2, app. A, § 64.2003(b)(2) (emphasis added).
178 *CPRA*, *supra* note 4, § 1798.130(a)(5)(C)(i).
179 *CCPA Regulations*, *supra* note 138, §§ 999.308(c)(1)(g)(1)–(2).
180 *CPRA*, *supra* note 4, § 1798.115(a)(2) (emphasis added).
181 *Id.* § 1798.130(a)(5)(C)(ii).

Unfortunately, as discussed in Section 4.C, it is unclear whether the GDPR requires a business to separately disclose, *for each category* of personal information collected, the purpose for collecting that category of personal information. It follows that it is also unclear whether the GDPR requires disclosure of the categories of personal data shared.

7. ACCESSIBILITY, CLARITY, AND FORMAT OF NOTICES

Research has long shown that it is necessary but not sufficient that privacy policies contain particular information about collection, use, and disclosure of personal information.[182] In order for users to meaningfully exercise choices, it is also necessary that privacy policies be accessible and clear, tests that many privacy policies have long failed.[183]

A. *Accessibility*

The accessibility of privacy policies varies widely. Sometimes, privacy policies are linked from a website or app's home page or screen. Often, however, they are not, and finding them requires perseverance. The timing and placement of privacy notices are other fundamental challenges of privacy regulations.[184]

The GDPR chose to associate the timing of privacy notices with the time at which personal information is collected or processed. Some of the disclosures required by the GDPR must occur at the time the personal data is collected, some must occur within a reasonable period after the personal data is collected, and some only occur if and when an individual requests the information. The GDPR requires that notices be in an "easily accessible form."[185] The EU advises that "it should be immediately apparent to [consumers] where and how this information can be accessed, for example by providing it directly to them, by linking them to it, by clearly signposting it or as an answer to a natural language question."[186]

The FCC Order took a different approach, focusing on notices at the time that a consumer purchases a service. The FCC Order requires that notices be "made available to prospective customers at the point of sale,"[187] explaining that "requiring notices at the point of sale ensures that notices are relevant in the context in which they are given, since this is a

182 *See* Joel R. Reidenberg, Travis Breaux, Lorrie Faith Cranor, Brian French, Amanda Grannis, James T. Graves, Fei Liu, Aleecia McDonald, Thomas B. Norton, Rohan Ramanath, N. Cameron Russell, Norman Sadeh & Florian Schaub, *Disagreeable Privacy Policies: Mismatches between Meaning and User' Understanding*, 30 BERKELEY TECH. L.J. 39 (2014) [hereinafter *Reidenberg*].
183 *Id.*
184 *FCC Order*, *supra* note 2, ¶¶ 137–55.
185 *GDPR*, *supra* note 1, art. 12(1).
186 Article 29 Data Protection Working Party, *Guidelines on Transparency Under Regulation 2016 /679*, ¶ 11 (Apr. 11, 2018).
187 *FCC Order*, *supra* note 2, app. A, § 64.2003(c)(1).

time when a customer can still decide whether or not to acquire or commit to paying for service."[188] The FCC Order also requires that notices be made "persistently available through a clear and conspicuous link on the [telecommunications] carrier's homepage, [and] through the provider's application,"[189] explaining that "customers must be able to review the notice and understand the carrier's privacy practices at any time since they may wish to reevaluate their privacy choices as their use of services change, as their personal circumstances change, or as they evaluate and learn about the programs offered by the provider."[190]

Blending the GDPR and FCC requirements, the CPRA requires a privacy policy, another notice at or before the point the personal data is collected, and yet another notice if and when an individual requests the information. Each of these three notices has specified elements, as discussed earlier in this paper. The CPRA requires that all notices be "in a form that is reasonably accessible to consumers."[191] Going beyond the GDPR's requirements (but similar to the FCC Order's), the CPRA requires that the privacy policy be linked from the business's website homepage using the word 'privacy.'[192]

B. *Clarity*

Privacy policies are often long, vague, and difficult to understand.[193] Another fundamental challenge that privacy regulations face is determining how to encourage, or require, privacy policies that are both informative and easy to understand.

The GDPR requires that notices be "in a concise, transparent, [and] intelligible . . . form, using clear and plain language."[194] Regarding conciseness, the EU advises that privacy notices should be separate from terms and conditions of the service, and that "controllers should present the information/ communication efficiently and succinctly in order to avoid information fatigue" (e.g., using a layered format).[195] Regarding intelligibility, the EU advises that privacy notices "should be understood by an average member of the intended audience" and that a controller should calibrate the language to the intended audience.[196] Regarding clean and plain language, the EU advises that "information should be provided in as simple a manner as possible, avoiding complex sentence

188 *Id.* ¶ 138.
189 *Id.* ¶ 140.
190 *Id.*
191 *CPRA*, *supra* note 4, § 1798.130(a).
192 *CCPA Regulations* , *supra* note 138, at § 999.308(b).
193 *Reidenberg*, *supra* note 182.
194 *GDPR*, *supra* note 1, art. 12(1).
195 Article 29 Data Protection Working Party, *supra* note 186, at 7.
196 *Id.*

and language structures" and that "[t]he information should be concrete and definitive" and "should not be phrased in abstract or ambivalent terms or leave room for different interpretations."[197]

In comparison, the FCC Order requires that notice "be presented in a way that is clear and conspicuous, in language that is comprehensible and not misleading.[198] Regarding conciseness and clarity, the Order explains that privacy policies are "frequently too long and unclear" and that "overlong notices are often inherently less comprehensible."[199] It explains that "providers must balance conveying the required information in a comprehensive and comprehensible manner" and suggests layered notices may achieve "these parallel objectives."[200]

Finally, the CCPA delegates to the California Attorney General the responsibility to develop regulations "necessary to ensure that the notices and information that businesses are required to provide . . . are provided in a manner that may be easily understood by the average consumer."[201] Correspondingly, the CCPA regulations requires businesses to provide notices that "[u]se plain, straightforward language and avoid technical or legal jargon."[202] Notices regarding collection and sharing "shall be written in a manner that provides consumers a meaningful understanding of the information being collected" and of "why the information is collected or sold."[203]

It remains to be seen how future enforcement of these requirements affects the resulting clarity of privacy policies and other privacy notices.

C. *Format*

Some papers propose privacy labels to standardize the presentation of information regarding the collection, use, and sharing of personal information.[204]

Neither the GDPR, the FCC Order, nor the CPRA require a standardized format for privacy notices.[205] However, both the GDPR and the CPRA contemplate voluntary use of standardized icons that may represent a business's privacy practices and/or user choices.

197 *Id.* at 8–9.
198 *FCC Order*, *supra* note 2, ¶ 125.
199 *Id.* ¶ 149.
200 *Id.*
201 *CCPA*, *supra* note 3, § 1798.185(a)(6).
202 *CCPA Regulations*, *supra* note 138, §§ 999.305(a)(2)(a), 999.306(a)(2)(a), 999.307(a)(2)(a), 999.308(a)(2)(a).
203 *Id.* §§ 999.305(b)(1), 999.308(c)(1)(f).
204 *See, e.g.*, Patrick Gage Kelley, Joanna Bresee, Lorrie Faith Cranor & Robert W. Reeder, *A "Nutrition Label" for Privacy*, 4 CARNEGIE MELLON UNIV., SCH. COMPUT. SCI. 1 (2009), https://dl.acm.org/doi/10.1145/1572532.1572538 [https://perma.cc/7GNL-YFF3].
205 *FCC Order*, *supra* note 2, ¶¶ 144–55.

The GDPR states that notices about processing "may be provided in combination with standardised icons in order to give in an easily visible, intelligible and clearly legible manner a meaningful overview of the intended processing," and delegates to the European Commission the power to "determin[e] the information to be presented by the icons and the procedures for providing standardised icons."[206] It is not yet known what types of information would be represented by such icons.

In comparison, the CCPA delegates to the California Attorney General the responsibility to develop regulations "[f]or the development and use of a recognizable and uniform opt-out logo or button . . . to opt-out of the sale of personal information."[207] The logo or button has not yet been designed, and its exact functionality remains unknown.

Another issue is whether certain elements of privacy notices should not only be standardized but also be machine-readable. The goal of making notices machine-readable is to allow the development of third-party apps that crawl through a large number of notices and then present useful comparisons to consumers. The GDPR states that "[w]here [standardized] icons are presented electronically they should be machine-readable."[208] The CCPA delegates to the California Attorney General the responsibility to develop regulations "to facilitate . . . the consumer's authorized agent's ability to . . . obtain information."[209] However, no requirement that information be machine-readable has yet been issued.

8. CONSENT REQUIREMENTS

User consent is a primary driver for both the GDPR and the CPRA.[210] However, they approach the issue of user consent very differently, and consequently, afford consumers substantially different choices.

A. *Take It or Leave It*

Historically, the terms and conditions of many services specified that use of the service is conditioned on a user agreeing to the collection, use, and sharing of personal information.[211] While some terms and conditions limited the mandated collection and use to that personal information that is technically required to offer the service's core functionality, other terms and conditions often mandated collection, use,

206 *GDPR*, *supra* note 1, art. 12(7)–(8).
207 *CCPA*, *supra* note 3, § 1798.185(a)(4)(C).
208 *GDPR*, *supra* note 1, art. 12(7).
209 *CCPA*, *supra* note 3, § 1798.185(a)(7).
210 *Jordan Proposed Statute*, *supra* note 153.
211 *Id.* at 271.

and sharing of personal information that a user would often view as unrelated to the service.[212]

It is common that the core functionality of a business's service or application is technically dependent on the collection and use of a minimal set of personal information.[213] For example, services and applications that can only be used when a user is logged in are dependent upon personal information used to establish login credentials.[214] Services and applications that transmit content (e.g., email) require access to the content to be transmitted.[215] Services and applications whose core functionality revolves around user personalization require personal information upon which the personalization is based.[216]

A key question is when and for which purposes a privacy regulation allows a service's terms and conditions to mandate the collection and use of personal information.

i. The GDPR

The GDPR requires a lawful basis for any type of processing, which includes collection, use, and disclosure of personal information.[217] Two of the lawful bases for the processing of non-sensitive personal information are contracts and user consent.[218] EU guidance explains that contracts and user consent are different concepts, and that when a consumer agrees to a contract this is not to be construed as user consent.[219] Terms and conditions are a form of a contract. We consider contracts in this subsection and we consider user consent in Section 8.B.

The GDPR does not attempt to determine when personal information is necessary for core functionality of a service, for elective functionality, or for unrelated purposes. Instead, it examines the contract between a business and a consumer to determine what processing is necessary to implement the service to which they have agreed. Specifically, under the GDPR, processing of non-sensitive personal information is lawful if the processing is "necessary for the performance of a contract" between the natural person and the controller.[220] EU guidance explains that "what is 'necessary for the performance of a

212 *Id.* at 267–70.
213 *Id.* at 267–68.
214 *Id.*
215 *Id.*
216 *Id.*
217 *GDPR*, *supra* note 1, art. 6(1).
218 *Id.*
219 *European Data Protection Board on Guidelines 2/2019 on the Processing of Personal Data Under Article 6(1)(b) GDPR in the Context of the Provision of Online Services to Data Subjects*, ¶ 20 (Oct. 8, 2019) [hereinafter *EU Contracts*], https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines-art_6-1-b-adopted_after_public_consultation_en.pdf [https://perma.cc/D2R5-H67T].
220 *GDPR*, *supra* note 1, art. 6(1)(b).

contract' is not simply an assessment of what is permitted by or written into the terms of a contract."[221] It further explains that the *necessity* clause limits processing authorized by terms and conditions to that which "cannot, as a matter of fact, be performed if the specific processing of the *personal data in question* does not occur."[222] The contract is thus *not* a lawful basis for any processing of personal data that is *not* required to provision the service. One such example of processing not required to provision a service is the processing of personal information for the purposes of improving a service.[223] Furthermore, although a controller may bundle several separate services into one contract, the processing authorized under a contract is limited to that required to implement only those services the consumer is actually using.[224]

Many businesses that offer advertising-supported services or apps have argued that behavioral advertising provides a principal source of revenue for the service, and consequently that a business should be able to require the collection, use, and sharing of personal information for purposes of behavioral advertising in the terms and conditions of its service. EU guidance states that a contract cannot be used as a lawful basis for such processing.[225]

Many businesses that offer personalized services or apps have similarly argued that they should be able to require the collection, use, and sharing of personal information for purposes of personalization in the terms and conditions of their services. EU guidance states that "personalisation of content . . . may be regarded as necessary for the performance of the contract" if it is "an intrinsic aspect" of the service.[226]

ii. FCC Order

Like the GDPR, the FCC Order looks to the contract between a business and a consumer to determine what processing is necessary to implement the service to which they have agreed. However, since the FCC Order is focused on telecommunications services, it limits the collection and use of personal information mandated in terms and conditions to that required to offer the telecommunications service. Specifically, the FCC Order accepts a contract between a user and a telecommunications carrier as a lawful basis to collect and use customer proprietary information "to provide the telecommunications service from which it was derived, and services necessary to, or used in the

221 *EU Contracts*, *supra* note 219, ¶ 23.
222 *Id.* ¶ 30 (emphasis in original).
223 *Id.* ¶¶ 48–49.
224 *Id.* ¶¶ 36–37.
225 *Id.* ¶¶ 51–56.
226 *Id.* ¶ 57.

telecommunications service."[227] The Order explains that "[c]onsent to use customer [proprietary information] for the provision of service is implied in the service relationship."[228] However, it clarifies that this basis does not include the use of personal information collected to provision the service *for another unrelated purpose*.[229]

Comparing the ability of a business to mandate collection and use of personal information under the GDPR versus under the FCC Order, we find that the FCC Order has a wider scope of the use of personal information for the provision of a service than does the GDPR. First, whereas the GDPR limits the processing of personal information justified under a contract to *non-sensitive* personal information, the FCC Order allows the processing of both non-sensitive and sensitive personal information for the provision of a service.[230] Second, whereas the GDPR does not allow the processing of personal information for the purposes of improving a service to be mandated in terms and conditions, the FCC Order explicitly includes the use of personal information "for the purpose of conducting research to improve and protect networks or telecommunications."[231] Finally, whereas the GDPR does not allow the processing of personal information for the purposes of marketing to be mandated in terms and conditions, the FCC Order includes the use of non-sensitive personal information for first-party marketing of "other communications services commonly marketed with the telecommunications service to which the customer already subscribes."[232]

iii. The CPRA

The CCPA did not require user consent for *collection* and *use* of personal information. The CPRA requires user consent for the use of sensitive personal information for any purposes other than those "necessary to perform the services . . . reasonably expected by an average consumer" or for certain specified business purposes[233]; we discuss this further in Section 8.B.iv. Thus, a business may mandate in the terms and conditions of a service the collection and use of any non-sensitive personal information it desires. This is a fundamental limitation on the consent requirements of the CPRA. The CPRA treats *disclosure* of personal information very differently from *collection* and *use* of personal information. Like the GDPR and the FCC Order, it allows some types of

227 *FCC Order*, *supra* note 2, ¶ 203.
228 *Id.*
229 *Id.*
230 *Compare GDPR*, *supra* note 1, art. 6(1)(b), *with FCC Order*, *supra* note 2, ¶ 203.
231 *FCC Order*, *supra* note 2, ¶ 209.
232 *Id.* ¶ 205.
233 *CPRA*, *supra* note 4, § 1798.121(a)

disclosure to be mandated by the terms and conditions of a service. However, whereas the GDPR looks to the contract between a business and a consumer to determine what processing is necessary to implement the service to which they have agreed, the CPRA severely limits the disclosure of personal information that can be mandated by terms and conditions.

The CPRA limits such disclosures of personal information in two ways. First, it limits the disclosure of personal information that may be mandated by terms and conditions of a service to those disclosures made to *service providers*. Sharing of personal information by a business with an entity other than a service provider requires user consent, as discussed in Section 8.B. As discussed in Section 3, disclosure of personal information to a service provider requires a written contract between the business and the service provider. Furthermore, the contract must "prohibit[] the [service provider] from [s]elling or sharing the personal information" and from "[r]etaining, using, or disclosing the personal information for any purpose other than for the business purposes specified in the contract."[234] Thus, while the GDPR looks to the contract between the business and a *consumer*, the CPRA looks to the contract between the business and a *service provider*. The result, however, is similar in that the GDPR's requirement that processing be necessary for the performance of a contract would naturally restrict disclosure to processors and not allow sharing with third parties.

Second, the CPRA limits the disclosure of personal information that may be mandated by terms and conditions of a service to those required for a *business purpose*,[235] which it defines as the "use of personal information for the business's operational purposes . . . provided that the use of personal information shall be reasonably necessary and proportionate to achieve the purpose."[236] As with the GDPR, the use under this exception must be related to the functionality of the service. As with the GDPR, the CPRA does not allow sharing of personal information for behavioral advertising without user consent.[237]

Comparing the ability of a business to mandate collection and use of personal information under the GDPR versus under the CPRA, we find that the CPRA is in some respects narrower than the GDPR, and in some respects broader than the GDPR. First, whereas the GDPR only allows processing to be mandated in terms and conditions if the contract with the consumer *cannot be performed* without the personal information in question, the CPRA allows processing to be mandated in terms and

234 *Id.* § 1798.140(ag)(1); *see also id.* § 1798.140(j)(1).
235 *Id.* § 1798.135(f).
236 *Id.* § 1798.140(e).
237 *Id.* § 1798.140(e)(4); *see also id.* § 1798.135(f).

conditions if the processing is *reasonably necessary and proportionate* to achieve an operational purpose.[238] Second, whereas the GDPR does not allow a business to mandate in its terms and conditions the processing of personal information for the purposes of improving a service, the CPRA does.[239] Third, whereas the GDPR does not allow a business to mandate in its terms and conditions processing for bundled services, the CPRA allows a business to mandate in its terms and conditions the disclosure of personal information to a service provider for "another purpose that is compatible with the context in which the personal information was collected."[240] However, whereas the GDPR in some cases allows personalization of content without user consent,[241] the CPRA restricts such personalization to "[s]hort-term, transient use" and excludes "build[ing] a profile about the consumer. . . ."[242] In addition, while the GDPR allows any processing that is necessary for the performance of a contract to be mandated in terms and conditions,[243] the CPRA only allows disclosure to service providers of personal information for business purposes; furthermore, the CPRA details a specified and exhaustive list of categories of such business purposes.[244]

B. *Opt-in and Opt-out*

User consent plays a critical role in the GDPR, the FCC Order, and the CPRA. Under the GDPR, processing of personal information is lawful if the user has "given consent to the processing of his or her personal data for one or more specific purposes."[245] Under the FCC Order, use and disclosure of customer proprietary information for other than providing the telecommunications service requires user consent.[246] Under the CPRA, use of sensitive personal information for other than providing the service requires user consent, and sharing or sale of personal information requires user consent.[247]

i. User choice

One question that each privacy regulation faces is what constitutes user consent.

The GDPR defines *consent* as "any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or

238 *See* Section 8.A.i.
239 *CPRA*, *supra* note 4, § 1798.140(e)(7).
240 *Id.* § 1798.140(e).
241 *See* Section 8.A.i.
242 *CPRA*, *supra* note 4, § 1798.140(e)(4).
243 *See* Section 8.A.i.
244 *CPRA*, *supra* note 4, § 1798.140(e)(1)–(8).
245 *GDPR*, *supra* note 1, arts. 6(1)(a), 9(2)(a).
246 *See* Section 8.B.ii.
247 *See* Section 8.B.ii.

she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her."[248] EU guidance clarifies that the "freely given" requirement precludes "consent [that] is bundled up as a non-negotiable part of terms and conditions . . . ."[249] As discussed in Section 8.A, a contract may be used as a lawful basis *only* for processing non-sensitive personal data necessary for the performance of a contract. One common question is whether a controller can require user consent for *other* purposes of processing as a prerequisite for using the service. EU guidance states that since users would not be able to use the service without consenting to such purposes, this "consent cannot be considered as being freely given."[250] In particular, a controller may not require user consent for the collection and sharing of personal information for behavioral advertising, even if such advertising provides a principal source of revenue for the service.[251]

Both the FCC Order and the CPRA similarly distinguish user consent from take-it-or-leave-it offers. The FCC Order explicitly states that it "prohibit[s] [broadband Internet access service] providers from conditioning the provision of broadband service on a customer surrendering his or her privacy rights," explaining that "such 'take-it-or-leave-it' practices offer no choice to consumers."[252] Under the CPRA, a business cannot require user consent for selling personal data to third parties as a prerequisite for using the service.[253] In addition, the CPRA adopted a definition of opt-in user consent that mirrors the GDPR's definition: "any freely given, specific, informed and unambiguous indication of the consumer's wishes by which he or she, . . . by a statement or by a clear affirmative action, signifies agreement to the processing of personal information relating to [the consumer] for a narrowly defined particular purpose."[254]

ii. Opt-in vs. Opt-out

A large area of debate in the development of privacy regulations exists as to when user consent should be opt-in versus opt-out. Research shows that consumers usually do not change the default setting of most privacy choices they are given. The GDPR and the CPRA differ regarding when user consent is opt-in or opt-out.

248 *GDPR*, *supra* note 1, *id.* art. 4(11).
249 *Eur. Data Prot. Bd. on its Guidelines 05/2020 on Consent Under Regulation 2016/679*, ¶ 13 (2020) [hereinafter *EU Consent*].
250 *Id.* ¶ 15.
251 *See, e.g.*, *id.* ¶¶ 40–41.
252 *FCC Order*, *supra* note 2, ¶ 295.
253 *CPRA*, *supra* note 4, §§ 1798.120, 1798.125(a)(1)(A).
254 *Id.* § 1798.140(h).

The GDPR requires that consent be "by a statement or by a clear affirmative action."[255] The GDPR explains that "clear affirmative action . . . could include ticking a box . . . [or] choosing technical settings," but does not include "[s]ilence [or] pre-ticked boxes."[256] The GDPR's consent requirement is thus often described as *opt-in*.

The FCC Order requires opt-in consent in some situations and allows opt-out consent in others. It defines *opt-in approval* as "[a] method for obtaining customer consent . . . [that] requires that the carrier obtain from the customer *affirmative, express consent* allowing the requested usage, disclosure, or access to the customer proprietary information . . . ."[257] It defines *opt-out approval* as "[a] method for obtaining customer consent . . . [under which] a customer is deemed to have consented to the use, disclosure, or access to the customer's proprietary information *if the customer has failed to object* thereto after the customer is provided appropriate notification of the carrier's request for consent . . . ."[258] The FCC Order differentiates between situations that require opt-in approval and those for which opt-out approval is appropriate based on the sensitivity of the personal information involved. The FCC Order requires opt-in approval for a telecommunications carrier to "use, disclose, or permit access to any of the customer's *sensitive* customer proprietary information," and requires opt-out approval (at a minimum) for a telecommunications carrier to "use, disclose, or permit access to any of the customer's *non-sensitive* customer proprietary information."[259] We discuss the Order's definition of *sensitive* below.

The CPRA similarly defines *opt-in consent* as an affirmative authorization[260] and a *right to opt-out* as direction from a consumer.[261] Although the CCPA did not differentiate between these on the basis of the sensitivity of the personal information involved, the CPRA does.[262] We discuss the CPRA's definition of *sensitive* below. The CPRA also differentiates based on the age of the consumer: it requires opt-in consent for the sale of personal information of consumers less than 16 years of age and applies the right to opt-out to the sale of personal information of consumers at least 13 years of age.[263]

255 *GDPR*, *supra* note 1, art. 4(11).
256 *Id.* at recital 32.
257 *FCC Order*, *supra* note 2, app. A, § 64.2002(j)) (emphasis added).
258 *Id.* § 64.2002(k) (emphasis added).
259 *Id.* §§ 64.2004(b), (c) (emphasis added).
260 *CPRA*, *supra* note 4, § 1798.140(h).
261 *Id.* § 1798.120(a).
262 *See* Section 8.B.iv.
263 *CPRA*, *supra* note 4, § 1798.120(c).

iii. Multiple Purposes

A separate debate exists with respect to the granularity of users' choices. Privacy advocates often argue that higher granularity results in greater consumer choice. However, many businesses often argue that higher granularity may also result in consumer confusion and decision overload. The three privacy regulations differ in the required granularity of user choices.

The GDPR requires high granularity. It requires that consent be "specific."[264] EU guidance clarifies that if a controller uses personal data for more than one purpose, the consumer must have "a choice in relation to each of them."[265]

In contrast, the FCC Order allows businesses to determine whether user choices are of high or low granularity. Specifically, the FCC Order does not mandate that a telecommunications carrier offer consumers separate choices over which purposes to allow the use and disclosure of their personal information. The Order states that "[a] carrier is free to give the customer the ability to pick and choose among which marketing channels the customer will opt out of," and also free "to give the customer the ability to opt out of all marketing with a single click . . . ."[266]

The CPRA requires a low-granularity option, but also allows businesses to simultaneously offer high-granularity choices. The statute only describes the right of consumers to opt-out of the *aggregate* sale of their personal information by a business. CCPA regulations state that a business may, at its discretion, offer "the choice to opt-out of sales for *certain* uses of personal information . . . ."[267] However, the regulations also require that "a business . . . present[s] . . . a *global* option to opt-out of the sale of *all* personal information," and this global option must be "more prominently presented than the other choices."[268]

iv. Sensitive Personal Information

The GDPR, the FCC Order, and the CPRA all have special requirements for what they consider to be *sensitive* personal information. However, the definition of *sensitive* personal information is always a matter of great debate and lobbying.

The GDPR's definition of *sensitive* personal data includes specific types of information relating to a person's physical characteristics: "racial and ethnic origin" and "genetic data, biometric data [processed] for the purpose of uniquely identifying a natural person, [and] data concerning

264 *GDPR*, *supra* note 1, art. 4(11).
265 *EU Consent*, *supra* note 249, ¶¶ 55, 60.
266 *FCC Order*, *supra* note 2, ¶ 227.
267 *CCPA Regulations*, *supra* note 138, § 999.315(e) (emphasis added).
268 *Id.* (emphasis added).

health . . . ."[269] The GDPR's definition also includes specific types of information relating to a person's behavior or beliefs: "personal data revealing . . . political opinions, religious or philosophical beliefs, or trade union membership" and "data concerning a natural person's sex life or sexual orientation . . . ."[270]

The FCC Order's definition of *sensitive* customer proprietary information similarly includes some information relating to a person's physical characteristics, particularly health information.[271] The Order also specifically includes one identifier: Social Security numbers.[272] However, it focuses much more on information relating to a person's behavior or beliefs.[273] For some types of such information, including financial and pertaining to children, there was widespread support for designating them as sensitive, and the Order does so.[274] The Order also classifies "precise geo-location information" as sensitive, explaining that "[r]eal-time and historical tracking of precise geo-location . . . can expose 'a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations.'"[275]

Given the FCC Order's focus on telecommunications, a particularly spirited debate occurred over the treatment of personal information relating to a customer's Internet activity and application usage.[276] There was widespread support for classifying the "content of communications" as sensitive, and the Order does so, explaining that "Congress recognized communications as being so critical that their content, information about them, and even the fact that they have occurred, are all worthy of privacy protections."[277]

However, there was much greater debate over whether the websites that a consumer visits on the Internet and the applications that a customer uses should be classified as sensitive personal information.[278] Some stakeholders argued that only a customer's visits to *sensitive websites* should be classified as sensitive personal information.[279] However, the Order rejects this proposal, explaining that "the lines between [which websites are] and [are] not considered sensitive information can be

269 *GDPR*, *supra* note 1, art. 9(1).
270 *Id.*
271 *FCC Order*, *supra* note 2, ¶ 178.
272 *Id.*
273 *Id.* ¶¶ 178, 183
274 *Id.* ¶ 178
275 *Id.* ¶ 179 (quoting United States v. Jones, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring)).
276 *Id.* ¶¶ 181–90.
277 *Id.* ¶ 180.
278 *Id.* ¶¶ 181–90.
279 *Id.*

difficult to determine."[280] Instead, the Order classifies all "'Web browsing history'" as sensitive customer proprietary information, explaining that:

> a user's browsing history can provide a record of her reading habits, . . . her video viewing habits, . . . who she communicates with, . . . when and with what entities she maintains financial or medical accounts, her political beliefs, . . . attributes like gender, age, race, income range, and employment status, . . . familial status, . . . religion, political leanings, . . . and location.[281]

The FCC Order similarly classifies "application usage history" as sensitive customer proprietary information, explaining that:

> the user's newsreader application will give indications of what he is reading, when, and how; an online video player's use will transmit information about the videos he is watching in addition to the video contents themselves; an email, video chat, or over-the-top voice application will transmit and receive not only the messages themselves, but the names and contact information of his various friends, family, colleagues, and others; a banking or insurance company application will convey information about his health or finances; even the mere existence of those applications will indicate who he does business with. A customer using ride-hailing applications, dating applications, and even games will reveal information about his personal life merely through the fact that he uses those apps, even before the information they contain (his location, his profile, his lifestyle) is viewed.[282]

The CCPA treated non-sensitive and sensitive personal information identically, and thus lacked a definition of sensitive personal information. The CPRA adds special treatment for sensitive personal information. Its definition of *sensitive personal information* incorporates many of the elements of the GDPR's definition, including genetic data, biometric information, health information, racial or ethnic origin, religious or philosophical beliefs, and sex life or sexual orientation.[283] It also incorporates many of the elements of the FCC Order's definition, including social security number, precise geolocation, and the content of communications.[284] However, unlike the FCC Order, the CPRA does not classify web browsing history or application usage history as sensitive

[280] *Id.* ¶ 188.
[281] *Id.* ¶ 183.
[282] *Id.* ¶¶ 184–85.
[283] *CPRA*, *supra* note 4, § 1798.140(ae).
[284] *Id.*

personal information.[285] The CPRA also requires notices regarding collection, use, and sharing of sensitive personal information.[286]

Having defined a category of sensitive personal information, the next question is what protections to apply to the processing of such information.

The GDPR has heightened requirements for the processing of sensitive personal data. First, it does not accept contracts between a controller and a consumer as a lawful basis for processing sensitive personal data.[287] Second, if user consent is used as a lawful basis for processing sensitive personal data, it requires a higher level of opt-in consent, described as "explicit consent."[288] EU guidance clarifies that "explicit consent" means that the person "must give an express statement of consent," e.g., "by filling in an electronic form, by sending an email, by uploading a scanned document carrying the signature of the data subject, . . . by using an electronic signature," or "by offering an explicit consent screen that contains Yes and No check boxes, provided that the text clearly indicates the consent, for instance 'I, hereby, consent to the processing of my data . . . .'"[289]

The FCC Order also has heightened requirements for the use and disclosure of sensitive personal information. For *non-sensitive* personal information, the Order requires, at a minimum, *opt-out approval* for the use of any personal information other than that required to offer the telecommunications service. For *sensitive* personal information, the FCC raises the bar, requiring *opt-in approval* for both use and disclosure. The Order's definition of opt-in approval already requires *express* consent but does not specify methods by which express consent is obtained.[290]

The CPRA has heightened requirements for the use of sensitive personal information. For non-sensitive personal information, recall from our discussion above that the CPRA does *not* require user consent for the use of non-sensitive personal information.[291] While the CCPA did not require user consent, the CPRA gives consumers a right to opt-out of the use of sensitive personal information for any purposes other than "to perform the services . . . reasonably expected by an average consumer who requests [the] . . . services," for certain specified business purposes, or as otherwise authorized by regulation.[292] Both of these provisions are weaker than those provided in the FCC Order, which required opt-out

285 *Compare FCC Order*, *supra* note 2, ¶ 181, *with CPRA*, *supra* note 4, § 1798.140(ae).
286 *CPRA*, *supra* note 4, § 1798.100(a)(2).
287 *GDPR*, *supra* note 1, art. 9(2).
288 *Id.*, art. 9(2)(a).
289 *EU Consent*, *supra* note 216, ¶¶ 93–96.
290 *FCC Order*, *supra* note 2, §§ 64.2004(b), (c).
291 *See* Section 8.A.iii.
292 *CPRA*, *supra* note 4, § 1798.121(a).

approval for the use of non-sensitive personal information for purposes other than to offer the service, and required opt-in approval for the use of sensitive personal information for purposes other than to offer the service.[293] However, the CPRA does *not* have heightened requirements for the disclosure of sensitive personal information; a consumer has the right to opt-out of the sharing or sale of both non-sensitive and sensitive personal information.

v. Profiling

Personal information is often used to create profiles of consumers.[294] All three privacy regulations lend some transparency to the use of personal information for profiling through their notice requirements, and all give consumers some choices. However, as discussed in Section 5.A, only the GDPR goes beyond these notice-and-consent requirements and requires additional notices regarding the use of personal data for automated decision-making or profiling that give consumers information about the logic involved in any decision that is based solely on automated processing.

In addition to heightened transparency, the GDPR also has heightened thresholds for automated decision-making and profiling. Automated processing (including profiling) that results in "legal effects" or that "significantly affects" a consumer is subject to a higher standard for user consent.[295] If user consent is used as the lawful basis for such automated processing, then it must be "explicit consent," namely, the same higher opt-in standard used for processing of sensitive personal data.[296] However, unlike in the processing of sensitive personal data, contracts between a controller and a consumer can be used as a lawful basis for automated processing of *non-sensitive* personal data.[297] In addition, the GDPR prohibits processing of personal data for direct marking purposes (including profiling) if a consumer expresses an objection to this use of their data.[298]

vi. Financial Incentives

Another lively argument concerns whether a business should be allowed to provide financial incentives for customers to consent to the processing of personal information for particular purposes. Some businesses argue that the offering of financial incentives (e.g., discounts)

293 *See* Section 8.A.ii.
294 *CPRA*, *supra* note 4, § 2(H)(i).
295 *GDPR*, *supra* note 1, art. 22(1).
296 *Id.* art. 22(2)(c).
297 *Id.* arts. 22(2)(a), (c).
298 *Id.* arts. 21(2), (3).

can benefit consumers, e.g., by subsidizing low-income consumers.[299] Privacy advocates, however, often argue that financial incentives can be harmful if used in a coercive manner, e.g., if the incentive is large.[300]

The GDPR allows some financial incentives. However, if user consent is used as the lawful basis for processing, then the requirement that consent be "freely given" precludes some types of financial incentives.[301] EU guidance states that "the onus would be on the controller to demonstrate that consent was still freely given in all the circumstances," for instance, by allowing "the possibility to withdraw consent without any negative consequences[,] e.g.[,] without the performance of the service being downgraded to the detriment of the user . . . ."[302] For example, a business may offer personalized discounts to customers who consent to the collection of personal data on shopping preferences.[303] However, the size and nature of allowed incentives remains unclear.

The FCC Order takes a somewhat different approach. Because it requires *opt-out* consent (at a minimum) for some uses of personal information, it found that it could apply heightened requirements to financial incentive programs by making participation in them *opt-in*.[304] In addition, the FCC had similar concerns to those expressed in the GDPR about financial incentives that are large enough to make user consent meaningless. The Order stated that the FCC "will closely monitor the development of financial incentive practices, particularly if allegations arise that service prices are inflated such that customers are essentially compelled to choose between protecting their personal information and very high prices."[305] However, while the GDPR prohibits a financial incentive if it results in user consent not being 'freely given,' the FCC Order prohibits financial incentives that are "unjust, unreasonable, [or] unreasonably discriminatory . . . ."[306] These tests are inherited from the Order's underlying statute.[307]

The CPRA also allows some financial incentives. As with the GDPR and the FCC Order, it requires that participation in financial incentive programs be opt-in.[308] In line with the GDPR, the CPRA prohibits financial incentive practices that are "coercive."[309] As with the FCC

299 *See, e.g.*, *FCC Order*, *supra* note 2, ¶ 299.
300 *See, e.g., id.* ¶ 300.
301 *GDPR*, *supra* note 1, art. 4(11).
302 *EU Consent*, *supra* note 216, ¶ 48.
303 *Id.* ¶ 50.
304 *FCC Order*, *supra* note 2, ¶ 302.
305 *Id.* ¶ 303.
306 *Id.*
307 *Id.*
308 *CPRA*, *supra* note 4, § 1798.125(b)(3).
309 *Id.* § 1798.125(b)(4).

Order, the CPRA prohibits financial incentive practices that are "unjust, unreasonable," or unreasonably discriminatory.[310] However, the CPRA also introduces a value test, specifically stating that a business may "charg[e] a consumer a different price or rate, or [may] provid[e] a different level or quality of goods or services to the consumer, *if* that difference is *reasonably related to the value* provided to the business by the consumer's data."[311]

It remains to be seen, through future enforcement actions, what type and size of financial incentives are allowed.

vii. Notice Re-user Consent

In addition to notices regarding collection, use, and disclosure (discussed in Sections 4-6), the GDPR, FCC Order, and CPRA all require notices that inform consumers of the choices they are afforded. We first discuss the required content of such notices, and then any requirements about their placement or form.

The GDPR requires that consent be "informed."[312] EU guidance explains that "[p]roviding information to data subjects prior to obtaining their consent is essential in order to enable them to make informed decisions, understand what they are agreeing to, and for example exercise their right to withdraw their consent."[313] The GDPR explains that consumers "should be aware at least of the identity of the controller and the purposes of the processing for which the personal data are intended."[314] EU guidance adds to this list "what (type of) data will be collected and used" and "information about the use of the data for automated decision-making . . . ."[315] Notice must also be given of "the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal."[316] Because the GDPR requires opt-in consent whenever user consent is the lawful basis for processing, it does not need specific requirements for notices to consumers of the right to opt-in, only of the right to *withdraw* consent.

In contrast, because the FCC Order requires opt-out consent (at a minimum) for certain uses of customer proprietary information, it specifically requires that a telecommunications carrier's privacy policy "[s]pecify and describe customers' opt-in approval and/or opt-out

310 *Id.* §§ 1798.125(a)(1)(B), (b)(4).
311 *Id.* § 1798.125(a)(2) (emphasis added).
312 *GDPR*, *supra* note 1, art. 4(11).
313 *EU Consent, supra* note 249, ¶ 62.
314 *GDPR*, *supra* note 1, at Recital 42.
315 *EU Consent*, *supra* note 216, ¶ 64.
316 *GDPR*, *supra* note 1, arts. 13(2)(c), 14(2)(d).

approval rights . . . ."[317] Unlike the GDPR, the Order also requires this notice to be placed in the same privacy policy as specific information about the use, collection, and disclosure of customer proprietary information. The Order explains that "[r]equiring providers to describe in a single place how information is collected, used, and shared, as well as what the consumers' rights are to control that collection, use, and sharing, enhances the opportunity for customers to make informed decisions."[318] Similar to the GDPR, it requires that the notice include "the types of customer [proprietary information] that the carrier is seeking to use, disclose, or permit access to; how those types of customer [proprietary information] will be used or shared; and the categories of entities with which that information is shared."[319] Similar to the GDPR, it also requires that notice be given of a customer's right to withhold or withdraw consent, specifically "[t]hat a customer's denial or withdrawal of approval . . . will not affect the provision of any telecommunications services of which he or she is a customer."[320]

Because the CPRA also requires opt-out consent (at a minimum) for the sale of personal information, it follows the FCC model. The CPRA requires that a business that sells personal information include in its privacy policy a description of a consumer's right to opt-out.[321]

The GDPR does not prescribe the placement of a notice regarding user consent. Perhaps the omission of a placement requirement is due to the presumption that a controller will be motivated by the opt-in requirement to place the notice in a conspicuous location. The GDPR also does not prescribe the form of a notice regarding user consent, beyond the same clarity requirements it applies to other notices. It does, however, state that consent can be "given in the context of a written declaration which also concerns other matters" (e.g., terms and conditions of the service), but if so, "the request for consent shall be presented in a manner which is clearly distinguishable from the other matters . . . ."[322]

Because the FCC requires that a notice regarding user consent be placed in the same privacy policy as other notices, it also applies the same accessibility and clarity requirements.[323]

In contrast, because the CPRA has a strong focus on the sale of personal information, it has specific requirements about the placement and format of a notice regarding a consumer's rights to opt-out. The CPRA gives a business three options: First, a business can provide two

317 *FCC Order*, *supra* note 2, app. A, § 64.2003(b)(4).
318 *Id.* ¶ 133.
319 *Id.* ¶ 226.
320 *Id.* at app. A, § 64.2003(b)(4)(i).
321 *CPRA*, *supra* note 4, § 1798.135(c)(2).
322 *GDPR*, *supra* note 1, art. 7(2); *see also EU Handbook*, *supra* note 35, at 112.
323 *FCC Order*, *supra* note 2, §§ 137–43.

"clear and conspicuous link[s] on the business's internet homepages," one titled "'Do Not Sell or Share My Personal Information'" and a second titled "'Limit the Use of My Sensitive Personal Information.'"[324] Second, a business can provide "a single, clearly labeled link . . . [that] easily allows a consumer to opt-out of the sale or sharing of the consumer's personal information and to limit the use or disclosure of the consumer's sensitive personal information."[325] Finally, a business can develop a standardized "*opt-out preference signal* [that could be] sent by a platform, technology, or mechanism."[326] Such a preference signal is in some respects similar in concept to the *Do Not Track* web browser setting. However, while the *Do Not Track* setting signals a request that a web application disable its tracking of an individual user, the *opt-out preference signal* would instead "indicate a consumer's intent to opt-out of the sale or sharing of the consumer's personal information and[/or] to limit the use or disclosure of the consumer's sensitive personal information."[327] The opt-out preference signal may be either a single signal for opting out of both or two separate signals (one for each opt-out).[328] It is also unclear what the relationship is, if any, between the opt-out preference signal and the "uniform opt-out logo or button . . . to opt-out of the sale of personal information."[329] The task of defining requirements and technical specifications for an opt-out preference signal is delegated to the California Attorney General or to a new California Privacy Protection Agency.[330] The third option (instead of providing links to opt-out webpages) is for a business to simply comply with such an opt-out preference signal.[331] The CPRA also envisions that a user might request a global opt-out using an opt-out preference signal, but wish to opt-in for specific businesses. If a business chooses this third option, it "may [also] provide a link to a web page that enables the consumer to consent to the business ignoring the opt-out preference signal."[332]

If a business chooses either of the first two options, the CPRA requires that links to the same webpages be provided in the business's privacy policy.[333] If a business chooses the third option, the CPRA requires that the business's privacy policy include "a statement that the business responds to and abides by opt-out preference signals."[334]

---

[324] *CPRA*, *supra* note 4, §§ 1798.135(a)(1), (2).
[325] *Id.* § 1798.135(a)(3).
[326] *Id.* § 1798.185(a)(19)(A) (emphasis added).
[327] *Id.*
[328] *Id.* § 1798.185(a)(19)(A)(vi).
[329] *CCPA*, *supra* note 3, § 1798.185(a)(4)(C).
[330] *CPRA*, *supra* note 4, §§ 1798.185(a)(19)(A), 1798.185(d).
[331] *Id.* § 1798.135(b)(1).
[332] *Id.* § 1798.135(b)(2).
[333] *Id.* § 1798.135(c)(2).
[334] *Id.*

9. COMPARISONS

In this concluding section, we summarize the similarities and differences between the GDPR and the CPRA.

A. *Personal Information*

Both the GDPR and the CPRA fundamentally rely on a definition of *personal information*. In both cases, that definition in turn relies on the concept of a *personal identifier*.

Almost everyone agrees that personal identifiers should include a person's name, telephone number, email address, and government-issued individual identifiers. However, almost all other identifiers have been the subject of debate and lobbying.

Some stakeholders have argued that household identifiers (e.g., home postal address, home telephone number) should not be considered to be personal identifiers, but both the GDPR and the CPRA have rejected these arguments.

Similarly, some stakeholders have argued that a non-household identifier that is not unique to a single natural person (e.g., date of birth) should not be classified as a personal identifier, but the GDPR and the CPRA have also rejected these arguments. The GDPR classifies such an identifier as a personal identifier if the identifier is "reasonably likely to be used," either alone or in combination with other information, to identify a natural person. The CPRA similarly classifies such an identifier as a personal identifier if it identifies a natural person "to a degree of certainty of more probable than not." Under either approach, when one identifier (e.g., date of birth) is combined with another identifier (e.g., place of birth), the result is likely to be that the combination becomes a personal identifier.

Some stakeholders have argued that an identifier that can be used to establish identity for only a limited period of time (e.g., a household IP address) should not be classified as a personal identifier. Both the GDPR and the CPRA have rejected this argument as overly broad, classifying a temporary identifier as a personal identifier if it can be reasonably used to identify an individual or household. As such, both agree that an IP address temporarily assigned to a household qualifies as a personal identifier.

Some stakeholders have argued that a device identifier (e.g., a MAC address, IMEI, or advertising identifier) should not be classified as a personal identifier. Again, both the GDPR and the CPRA have rejected this argument. The FCC Order explicitly classifies a device identifier as a personal identifier, while the GDPR and the CPRA take a slightly

narrower approach, classifying a device identifier as a personal identifier *if* it can be reasonably used to identify an individual or household.

Table 1: Definition of Personal Information (● = included; ◐ = included with qualifications; ? = not sure; ○ = not included)

		GDPR	CPRA
Personal identifiers	Personal identifiers (e.g., name, personal telephone number, email address)	●	●
	Household identifiers (e.g., home address, home telephone number)	●	●
	Non-unique identifiers (e.g., date and place of birth)	●	●
	Temporary identifiers (e.g., household IP address)	●	●
	Device identifiers (e.g., IMEI, advertising identifier)	◐	◐
Personal information	Information paired with a personal identifier (e.g., personal characteristic paired with email address)	◐	●
	Information not paired with a personal identifier, but which relates to a person (e.g., location, behavioral characteristics)	◐	◐
	Personal identifier (e.g., email address)	◐	●
	Aggregate or de-identified information	?	○

Both the GDPR and the CPRA then turn to the challenge of defining the scope of *personal information*. The GDPR uses a test of whether the information relates to an identified or identifiable natural person, whereas the CPRA uses a broader test of whether the information identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household. However, the differences between the GDPR's definition and the CPRA's definition are more limited than they may seem.

Some stakeholders have argued that information should be classified as personal information *only if* the information is paired with a person's name, personal telephone number, personal email address, or government issued individual identifier. Both the GDPR and the CPRA

have rejected this argument. Given that both the GDPR and the CPRA also classify household identifiers, device identifiers, some non-unique identifiers, and some temporary identifiers as personal identifiers, they correspondingly classify as personal information any information that is paired with any of these types of personal identifiers.

Some stakeholders have argued that information that relates to a person, but which is *not* paired with a personal identifier, should not be classified as personal information. One common example is location data. Another common example is a set of economic and/or behavioral characteristics. Both the GDPR and the CPRA have rejected this argument, since such information is often reasonably likely to be used to identify a person, device, or household.

Some stakeholders have argued that a personal identifier *itself* should *not* be classified as personal information. Here, the GDPR and the CPRA take slightly different tacks. The CPRA classifies private personal identifiers as personal information, whereas the GDPR only does so if the personal identifier is construed as "information about a person."

One of the most vigorous debates between stakeholders has been over the scope of an exclusion for aggregate and/or de-identified information. Some stakeholders have made broad arguments about the effectiveness of anonymization techniques and have correspondingly argued for broad exclusions for de-identified information. The GDPR is less than clear about the proper treatment of aggregate and/or de-identified information. It appears to exclude both aggregate and de-identified information from the scope of personal data. The GDPR encourages Member States to apply specialized protections to some forms of aggregate information, but very strangely the GDPR does not apply specialized protections to de-identified information, despite the risk that such data can be re-associated with an individual. The CPRA is clearer: it excludes both aggregate information and de-identified information from the scope of personal information, and applies specialized protections to de-identified information, but not to aggregate information.

When personal information is neither aggregate nor de-identified, the GDPR also explicitly encourages pseudonymization, and encourages that processors keep the pseudonymized information separate from the additional information that could be used to identify the consumer. The CPRA does not explicitly address pseudonymization that falls short of de-identification.

B. *Notices*

Both the GDPR and the CPRA require notices regarding the collection, use, and disclosure of personal information. However, there are significant differences between the disclosures required.

Both the GDPR and the CPRA require disclosure of the *categories of personal information* collected. The CPRA (but not the GDPR) also requires a business to disclose, upon request, the *specific pieces* of personal information that a business has collected about a person, which may result in substantially better insight by a consumer into a business's collection practices.

Neither the GDPR nor the CPRA require disclosure of the *methods* by which a business collects personal information. Such a disclosure, if it existed, would provide more insight into the nature of the categories of personal information that are collected.

Table 2: Required Notices (● = required; ? = not sure; ○ = not required)

		GDPR	CPRA
Personal information collected	Categories of personal information collected (e.g., device identifiers, location, user interests)	●	●
	List of specific pieces of personal information collected (e.g., IMEI, GPS coordinates, websites visited)	○	●
How personal information is collected	Methods by which personal information is collected (e.g., deep packet inspection, web beacon)	○	○
	Categories of sources from which personal information originates	●	●
	List of sources from which personal information originates	●	○
	List of sources from which a particular category of personal information originates	?	○
Uses of personal information	Purpose for collecting personal information	●	●
	Purpose for collecting a particular category of personal information	?	?
Sharing of personal	Categories of recipients of personal information	●	●

information	List of recipients of personal information	○	○
	Purpose for sharing a particular category of personal information	?	?
	Categories of personal information shared	?	●

The GDPR requires the disclosure of the sources from which personal information originates, whereas the CPRA only requires disclosure of categories of sources. The GDPR, but not the CPRA, thus allows a consumer to potentially trace back from whom their personal information was originally collected, and potentially cut off the source, *if* he or she can identify the downstream businesses that are harvesting this personal information. However, it is unclear whether the GDPR requires the disclosure of the source for each category of personal information collected. If not, tracing the upstream source of multiple categories of personal information is much more difficult.

Both the GDPR and the CPRA also require disclosure of the uses of personal information. However, it is unclear whether they require the disclosure of the purpose for collecting each category of personal information. If not, decisions over consent are more difficult.

Both the GDPR and the CPRA also require some transparency over disclosure of personal information. Both require disclosure of the categories of recipients, but neither requires disclosure of a list of recipients. This lack of transparency over the list of recipients makes it quite difficult for a consumer to identify the downstream harvesters of his or her personal information.

Both the GDPR and the CPRA have other potential problems with transparency over disclosure. It is unclear whether either framework requires a business to separately disclose, for each category of personal information collected, the purpose for sharing that category of personal information. If not, consumers face a difficult decision whether to allow such sharing. The FCC Order demonstrates how to close this potential loophole. In addition, although the CPRA clearly requires a business to disclose the categories of personal data disclosed to third parties, it is unclear whether the GDPR has a similar requirement.

C. *Consent*

User consent is often categorized into three approaches: take-it-or-leave-it, opt-out, and opt-in. Any privacy regulation must decide which approach is most appropriate for which types and uses of personal information.

Both the GDPR and the CPRA allow a business to mandate the collection and use of certain personal information through the service's terms and conditions. With respect to non-sensitive information, the GDPR allows a business to require a user to agree, through a contract, to the processing of non-sensitive personal information that is necessary for the performance of the contract. The CPRA allows a business to require a user agree to the collection and use of non-sensitive information, regardless of whether it is functionally necessary to offer the service. With respect to sensitive personal information, the GDPR does not allow a business to require a user to agree to processing of sensitive personal information. In contrast, the CPRA does allow a business to do so, providing that the use of the sensitive personal information is limited to that functionally required to offer the service. This is one of the largest differences between the GDPR and the CPRA. The GDPR limits the take-it-or-leave-it collection and use of personal information to personal information that is both non-sensitive and necessary for the performance of the contract. The CPRA limits the take-it-or-leave-it collection and use of personal information only to personal information that is both sensitive and functionally necessary to offer the service.

Additionally, both the GDPR and the CPRA allow a business to mandate the sharing of certain personal information through the service's terms and conditions. However, both regulations limit such sharing mandated by terms and conditions to the disclosure of personal information to a service provider. The CPRA is explicit about such limits. It both prohibits take-it-or-leave-it mandates of sharing to third parties, and limits the personal information disclosed to service providers to that used for a specified list of business purposes. The GDPR's restriction is less explicit. It limits take-it-or-leave-it mandates of sharing to that necessary to implement the service to which the business and user have agreed. However, this implicitly implies that any such disclosure of personal information by the business must be under a contract that limits the recipient's use to those agreed purposes, and hence the recipient must be a service provider.

Thus, both the GDPR and the CPRA hold a business responsible for the use of personal information by a service provider. However, there are some differences between the GDPR and the CPRA. The CPRA allows a business to require in the terms and conditions of its service the disclosure to a service provider of both sensitive and non-sensitive personal information, whereas the GDPR only allows for the disclosure to a service provider of non-sensitive personal information. The CPRA (but not the GDPR) allows disclosure to a service provider of personal information for the purposes of improving a service. The CPRA more severely limits the disclosure of personal information for purposes of

personalization. Furthermore, the CPRA restricts the uses authorized by such contracts to specified business purposes.

Table 3: Consent (● = valid consent; ◐ = valid consent with qualifications; ? = not sure; ○ = not valid consent)

		GDPR	CPRA
Take-it-or-leave-it	Collection and use of non-sensitive personal information necessary for the service	●	●
	Collection and use of non-sensitive personal information not necessary for the service	○	●
	Collection and use of sensitive personal information necessary for the service	○	●
	Collection and use of sensitive personal information not necessary for the service	○	○
	Disclosure of non-sensitive personal information to a service provider for specified business purposes	●	●
	Disclosure of non-sensitive personal information to a service provider for other service-related purposes	●	○
	Disclosure of sensitive personal information to a service provider for specified business purposes	○	●
	Disclosure of sensitive personal information to a service provider for other service-related purposes	○	○
	Sharing of personal information with another business	○	○
Opt-in or opt-out of collection	Opt-out of collection and use of non-sensitive personal information	○	●

and use	Opt-out of collection and use of sensitive personal information	○	●
	Opt-in to collection and use of non-sensitive personal information	●	●
	Explicit opt-in to collection and use of sensitive personal information	●	●
	Single opt-in or opt-out to the collection and use of multiple categories of personal information	○	●
Opt-in or opt-out of sharing	Opt-out of sharing of non-sensitive personal information	○	●
	Opt-out of sharing of sensitive personal information	○	●
	Opt-in to sharing of non-sensitive personal information	●	●
	Explicit opt-in to sharing of sensitive personal information	●	●
	Single opt-in or opt-out for the sharing of multiple categories of personal information	○	●
	Financial incentive for opt-in or opt-out of the collection, use, or sharing of personal information	◐	◐

When take-it-or-leave-it is not appropriate, the GDPR and the CPRA have drawn different lines between which collection, use, and sharing of personal information should be subject to opt-out consent versus opt-in consent.

The GDPR and the CPRA have made fundamentally different decisions about the appropriate level of protection. Under the GDPR, when user consent is the lawful basis for processing, the consent must be opt-in. Furthermore, when the personal information is sensitive, the consent must be explicit. Comparatively, under the CPRA, user consent is not required for the collection and use of non-sensitive personal information, but opt-out must be offered (at a minimum) for any sharing of personal information with another business. A middle ground can be found in the FCC Order, which requires opt-out consent (at a minimum) for processing of non-sensitive personal information and opt-in consent for processing of sensitive personal information. Any future privacy regulation will surely revisit this fundamental decision.

Future regulations will also surely revisit the question of the appropriate granularity of consumer choices. The GDPR requires that consumers have separate choices over each use of personal information.

In contrast, the CPRA not only has no such requirement, but rather requires businesses that offer separate choices to also offer a global choice. The impact on consumers of separate versus combined choices merits further study.

Future regulations will also surely revisit the question of whether they should rely on the concept of *sensitive personal information*, and if so how to delineate it. The GDPR's definition focusses primarily on physical characteristics and information relating to a person's behavior or beliefs. The FCC Order's definition focusses much more on online activity such as web browsing and application usage. The CCPA chose not to differentiate between sensitive and non-sensitive personal information, but the CPRA did. Although the GDPR and the FCC Order found the distinction useful in order to draw lines between opt-out and opt-in consent, or between non-explicit and explicit consent, it remains difficult to delineate the scope of sensitive personal information.

Finally, future regulations will also surely revisit the question of financial incentives. The issue of financial incentives plays a significant role in almost every debate over privacy. Some stakeholders suggest drawing clear lines: either that regulations should prohibit all financial incentives or that regulations should not limit financial incentives at all. Both the GDPR and the CPRA attempt to find a middle-ground, allowing reasonable financial incentives but prohibiting those that are unjust, unreasonable, unreasonably discriminatory, or coercive. However, they leave to enforcement authorities the determination of what size or type of financial incentive meets these limits, and there is not yet a sufficient track record on enforcement actions to judge the result of this approach.