A Proposal for Notice and Choice Requirements of a New Consumer Privacy Law

Scott Jordan*

TABLE OF CONTENTS

* Scott Jordan is a Professor of Computer Science at the University of California, Irvine. He served as the Chief Technologist of the Federal Communications Commission during 2014-2016. This material is based upon work supported by the National Science Foundation under Grant No. 1956393.

I. INTRODUCTION

The United States Congress has been devoting substantial attention to crafting a comprehensive consumer privacy law in the last few years. Any bill that attracts a majority vote is almost certain to include specific requirements for notices (e.g., elements of privacy policies) and for user choices (e.g., opt-out and/or opt-in). The formulation of these notice and choice provisions is the focus of this article.

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

In addition to notice and choice provisions, a comprehensive consumer privacy law may include requirements relating to a lawful basis other than user consent; data minimization; duties of care, loyalty, and confidentiality; readability of privacy policies; consumer rights to access, correct, and delete their personal information; methods for consumers to exercise these rights; methods for exercising choice; data portability; financial incentives; profiling; automated decision-making; research purposes; data security; data breaches; and enforcement. These issues are important but are outside the scope of this article.

The two common starting points for a comprehensive consumer privacy law are the 2016 European General Data Protection Regulation (GDPR)[1] and the 2018 California Consumer Privacy Act (CCPA).[2] In the GDPR and in the CCPA, notice requirements and user choices play a central role. However, the GDPR and the CCPA often do not agree on the specific requirements for notice and for user choice.[3] Thus, the GDPR and the CCPA often present two different policy options for notice and for choice.

However, policy options should not be limited to those offered by the GDPR and the CCPA. The notice requirements in these two options have proven to be insufficient to provide consumers the information necessary to make informed choices about their use of services and applications. Privacy policies often use non-standardized definitions of personal information that do not align with those in the GDPR or the CCPA or even with each other, leaving consumers confused about what constitutes personal information. Privacy policies often include assertions about the anonymity of personal information that exceed both the technical abilities and legal definitions of

1. Commission Regulation 2016/679, 2016 O.J. (L 119/1) [hereinafter GDPR].
2. CAL. CIV. CODE § 1798 (Deering, LEXIS through Ch. 11 of 2022 Reg. Sess.).
3. *See generally* Scott Jordan, *Strengths and Weaknesses of Notice and Consent Requirements Under the GDPR, the CCPA/CPRA, and the FCC Broadband Privacy Order*, CARDOZO ARTS & ENT. L.J., (2021), https://papers.ssrn.com/abstract=3894553.

anonymization and of de-identification. Privacy policies often lack specificity over what personal information is collected and how, leaving consumers uncertain about the related privacy risks. Additionally, privacy policies often lack transparency about which personal information is required to provide functionality of the service or app, and which personal information is used for non-functional purposes such as advertising, frustrating consumers' attempts to balance functionality and privacy. Privacy policies often fail to disclose sufficient information about sharing of personal information, impeding consumers' ability to understand the degree of identifiability of their shared information, to determine the associated privacy risks, or to follow the dissemination of their personal information through the data ecosystem. A comprehensive consumer privacy law should remedy these shortcomings of the GDPR and the CCPA.

Turning to the opt-in and opt-out choices currently offered to consumers, there are also failings that need to be addressed. When privacy policies give choices to consumers, the choices are often limited. Privacy policies often give consumers little choice over what personal information is collected. Privacy policies generally do not provide consumers choices about the use of their personal information that provide a tradeoff between functionality of the service or application and the consumer's privacy. Privacy policies also often fail to give consumers much control over which of their personal information is shared, with whom, and for what purposes. Ultimately, privacy policies generally give consumers little control over the dissemination of their personal information through the data ecosystem. The choice requirements mandated by the GDPR (often described as opt-in) and by the CCPA (often described as opt-out) present two different policy options. However, there are policy options that apply opt-in and opt-out requirements to different types of personal information, that may be superior to either the GDPR's or the CCPA's approaches, and that may remedy these shortcomings.

The academic literature includes several articles that analyze the GDPR and/or the CCPA. Hoofnagle, van der Sloot, and Borgesios provide an overview of the GDPR's roots and goals.[4] They explain the history of European data protection and privacy laws prior to the GDPR,[5] the GDPR's scope,[6] Fair Information Practices,[7] the legal basis for processing personal data,[8] special requirements for sensitive personal data,[9] data transfers,[10] and enforcement.[11] They also broadly discuss the responsibilities of businesses and processors[12] and the rights of consumers.[13] However, this piece does not give detailed analyses of notice and consent requirements.

4. Chris Jay Hoofnagle et al., *The European Union General Data Protection Regulation: What it is and What it Means*, 28 INFO. & COMMC'NS TECHNOLOGY L. 65 (2019).
5. *Id.* at 69-72.
6. *Id.* at 72-76.
7. *Id.* at 76-78.
8. *Id.* at 79-82.
9. *Id.* at 82-83.
10. *Id.* at 83-85.
11. *Id.* at 92-97.
12. *Id.* at 85-88.
13. *Id.* at 88-92.

Hintze provides a summary of the GDPR's notice requirements, along with advice on how a business may comply with them.[14] He briefly discusses the types of organizations subject to the GDPR,[15] and then discusses in detail the required elements of privacy notices. His article is broader than the focus of this article, including discussion of not only notices regarding the processing of personal data, but also notices regarding the identity of the controller;[16] the legal basis for processing personal data;[17] user rights to access, correct, and delete personal data;[18] the user right to data portability;[19] the user right to complain;[20] data transfers;[21] and data retention.[22] Pardau provides a summary of the unamended original version of the CCPA.[23] He briefly summarizes the CCPA's notice and consent requirements.[24] He also summarizes other provisions in the CCPA, including its scope[25] and user rights to access and delete personal information.[26]

There are a few academic articles 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.[27] He then compares user rights under the GDPR and the unamended original version of the CCPA. Blanke focuses on the protection under the GDPR and the CCPA of personal information that consists of inferences drawn from other personal information.[28] However, neither article goes into much detail on the similarities and differences in the notice and consent requirements of the GDPR and the CCPA.[29] Jordan compares the notice and consent requirements of the GDPR, the unamended original version of the CCPA, and the recently amended version of the CCPA, including definitions of personal information; notices regarding use, collection, and sharing; and choice frameworks.[30]

The academic literature also includes many articles that criticize the GDPR and/or the CCPA, and that propose alternatives to notice and choice

---

14. Mike Hintze, *Privacy Statements Under the GDPR*, 42 SEATTLE UNIV. L. REV. 1129-30 (2019).
15. *Id.* at 1131.
16. *Id.* at 1132-34.
17. *Id.* at 1138-39.
18. *Id.* at 1140-42
19. *Id.* at 1142.
20. *Id.* at 1144.
21. *Id.* at 1144-47.
22. *Id.* at 1147-48.
23. Stuart L. Pardau, *The California Consumer Privacy Act: Towards a European-Style Privacy Regime in the United States?*, 23 J. TECHNOLOGY L. & POL'Y 68, 91-100 (2018).
24. *Id.* at 96-99.
25. *Id.* at 92-93.
26. *Id.* at 94-96.
27. Donald L. Buresh, *A Comparison Between the European and the American Approaches to Privacy*, 6 INDONESIAN J. INT'L & COMPAR. L. 257 (2019).
28. 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).
29. In addition, this article disagrees with some of the comparisons drawn in Buresh, *supra* note 27.
30. *See generally* Jordan, *supra* note 3.

frameworks. Van Eijk *et al.* propose supplementing notice and choice with rules on unfair commercial practices.[31] Rothchild suggests supplementing notice and choice with rules grounded in the doctrines of unfairness and unconscionability.[32] Barrett proposes applying a fiduciary requirement to data collectors.[33] Hartzog and Richards propose a combination of rules regarding the corporate form: duties of discretion, honesty, protection, and loyalty; data minimization, deletion, and obscurity; and mitigating externalities.[34]

However, few academic articles propose specific requirements for notices of collection, use, and sharing. Hintze briefly argues that privacy policies should include increased detail, e.g., more granular detail about collection of personal information, and separate disclosures *for each category* of personal information collected of the purpose for collecting that category of personal information.[35] In contrast, Pardau briefly argues that a business' privacy policy should not be required to disclose the detailed list of disclosures about collection, use, and sharing required by the CCPA, but should only be required to disclose "the nature of its business as it relates to the collection of personal information."[36]

Similarly, there are no academic articles that propose alternative choice frameworks to those in the GDPR and in the CCPA.

The void in the academic literature has been filled by proposals from advocacy groups. Following is a brief summary of the notice and choice provisions in three frameworks that likely span the spectrum.

Privacy for America, an advocacy group composed of advertiser trade associations, proposed statutory text for a comprehensive consumer privacy law.[37] Privacy for America proposes fairly standard definitions of personal information[38] and de-identified information,[39] and a narrow definition of sensitive information that omits web browsing history.[40] With respect to collection and use of personal information, required disclosures are minimal, only including the categories of personal information collected and used.[41] With respect to sharing, required disclosures are heightened, including the categories of third parties and, for each such category, the categories of

31. Nico van Eijk et al., *Unfair Commercial Practices: A Complementary Approach to Privacy Protection*, 3 EUROPEAN DATA PROT. L. REV. 325, 334-37 (2017).

32. John A. Rothchild, *Against Notice and Choice: The Manifest Failure of the Proceduralist Paradigm to Protect Privacy Online (or Anywhere Else)*, 66 CLEVELAND STATE L. REV. 559, 637 (2018).

33. *See generally* Lindsey Barrett, *Confiding in Con Men: U.S. Privacy Law, the GDPR, and Information Fiduciaries*, 42 SEATTLE UNIV. L. REV. 1057 (2019).

34. Woodrow Hartzog & Neil Richards, *Privacy's Constitutional Moment and the Limits of Data Protection*, 61 B.C.L. REV. 1687, 1745-1760 (2020).

35. Mike Hintze, *In Defense of the Long Privacy Statement*, 76 MD. L. REV. 1044, 1083-1084 (2017).

36. Pardau, *supra* note 23, at 112.

37. PRIVACY FOR AMERICA, PRINCIPLES FOR PRIVACY LEGISLATION 13-39 (2019), https://www.privacyforamerica.com/wp-content/uploads/2020/01/Principles-for-Privacy-Legislation.pdf.

38. *Id.* at 16.

39. *Id.* at 14-15.

40. *Id.* at 22-24.

41. *Id.* at 20.

personal information shared and categories of uses.[42] Privacy for America proposes that opt-in consent be required for collection, use, or sharing of sensitive personal information.[43] It proposes no opt-in or opt-out requirements for its broad definition of non-sensitive personal information, other than an opt-out requirement from a narrow subset of data personalization.[44]

The Information Technology & Innovation Foundation (ITIF), an advocacy group funded in large part by the tech and communications industries,[45] proposes elements that it recommends be included in a comprehensive consumer privacy law.[46] ITIF argues for (but does not propose) a narrow definition of personally identifiable information that omits some types of linkable personal information.[47] It argues for (but does not propose) a broad definition of de-identified data that includes not only anonymized and aggregated data but also pseudonymized data.[48] ITIF recommends a narrow definition of sensitive personal data that omits much of web browsing history,[49] and a definition of critical services.[50] It gives few recommendations about notice,[51] but proposes that there should be no required disclosure of the use of personal information.[52] ITIF proposes a novel framework for choice. It proposes that opt-in consent be required for the collection of sensitive personal data for critical services, and that consumers be given an opt-out choice from the collection of non-sensitive personal data for critical services and from the collection of sensitive personal data for non-critical services.[53] It proposes that there should be no opt-in or opt-out requirements for the collection of its broad definition of non-personal data for non-critical services.[54] Finally, although ITIF argues that a law should provide incentives for data sharing, it does not propose any specific provisions regarding sharing.[55]

The Mozilla Foundation, an advocacy group funded primarily by royalties from Firefox web browser search partnerships, proposes a blueprint for a comprehensive consumer privacy law.[56] Mozilla proposes a broad

42. *Id.* at 20.
43. *Id.* at 22-24.
44. *Id.* at 31, 32.
45. ITIF's funders include Amazon, Apple, AT&T, Charter Communications, Comcast, CTIA, Facebook, Google, Microsoft, NCTA, T-Mobile, U.S. Telecom, and Verizon, among others. *Our Supporters*, INFO. TECHNOLOGY & INNOVATION FOUND., https://itif.org/our-supporters [https://perma.cc/7DKG-9BW3].
46. ALAN MCQUINN & DANIEL CASTRO, A GRAND BARGAIN ON DATA PRIVACY LEGISLATION FOR AMERICA (2019), https://itif.org/publications/2019/01/14/grand-bargain-data-privacy-legislation-america [https://perma.cc/SEF9-Y8C7].
47. *Id.* at 16.
48. *Id.* at 18.
49. *Id.* at 16.
50. *Id.*
51. *Id.* at 27.
52. *Id.* at 49.
53. *Id.* at 23.
54. *Id.*
55. *Id.* at 39.
56. MOZILLA, U.S. CONSUMER PRIVACY BILL BLUEPRINT (2019), https://blog.mozilla.org/netpolicy/files/2019/04/Mozilla-U.S.-Consumer-Privacy-Bill-Blueprint-4.4.19-2.pdf [https://perma.cc/4JH2-4RUE].

definition of covered data that includes information that can be reasonably connected to either a person or a device,[57] and argues for (but does not propose) a broad definition of sensitive data.[58] Mozilla makes detailed and expansive recommendations about notice. It proposes that privacy policies should disclose the personal data collected and the sources; the use of personal data, including inferences and decisions based on that data; the categories of personal data shared, with whom, and for what purposes.[59] Mozilla also proposes a novel framework for choice. It proposes that opt-in consent be required for the linking of personal information collected and shared by multiple entities.[60] It proposes that consumers be given an opt-out choice from specific granular uses of their personal information,[61] particularly including marketing.[62] Mozilla does not propose specific consumer choice requirements for collection or sharing, other than for the linking of personal information.

Two of the most discussed bills in the last session of Congress were the Consumer Online Privacy Rights Act (COPRA)[63] sponsored by Sen. Cantwell, and the Setting an American Framework to Ensure Data Access, Transparency, and Accountability Act (SAFE DATA)[64] sponsored by Sen. Wicker.

The COPRA bill includes a definition of *covered data* which includes information that is reasonably linkable to either an individual or a device,[65] a definition of *de-identified data* which includes information that is not reasonably linkable to either an individual or device,[66] and a broad definition of *sensitive covered data* that includes online activities.[67] It requires that privacy policies disclose a moderate amount of detail, including the categories of covered data collected and used and the purposes for collecting and using each category, and a list of third parties with which covered data is shared and the purposes for which it is shared with each.[68] The COPRA bill requires that opt-in consent be obtained for the use or sharing of sensitive data for non-functional purposes,[69] and that consumers be given an opt-out choice from sharing of non-sensitive data for non-functional purposes.[70]

The SAFE DATA bill includes a similar definition of *de-identified data* as does the COPRA bill,[71] but a narrower definition of *covered data* which similarly includes information that is reasonably linkable to an individual, but

57. *Id.* at 2.
58. *Id.*
59. *Id.* at 9.
60. *Id.* at 5.
61. *Id.* at 8.
62. *Id.* at 9.
63. Consumer Online Privacy Rights Act, S. 2968, 116th Cong. (2019) [hereinafter COPRA].
64. SAFE DATA Act, S. 4626, 116th Cong. (2020) [hereinafter SAFE DATA].
65. COPRA, *supra* note 63, at § 2(8).
66. *Id.* § 2(10).
67. *Id.* § 2(20).
68. *Id.* § 102(b)(2-3).
69. *Id.* §§ 105(c)(1-2), 110(c-d).
70. *Id.* §§ 105(b)(1), 110(c-d).
71. SAFE DATA, *supra* note 64, at § 2(10)(E).

only includes information that is reasonably linkable to a device if the device is itself reasonably linkable to an individual, and a narrower definition of *sensitive covered data* that omits many online activities.[72] It requires similar disclosures in privacy policies as does the COPRA bill about the collection and use of covered data,[73] but with respect to sharing it requires less detailed disclosures that only identify the categories of recipients rather than a list of recipients.[74] As with the COPRA bill, it requires that opt-in consent be obtained for the use or sharing of sensitive data for non-functional purposes, but the scope of sensitive data is narrower.[75] It also requires that consumers be given an opt-out choice from collection, use, and sharing of non-sensitive data for non-functional purposes.[76]

The remainder of this article is devoted to identifying failures of the GDPR and the CCPA and to developing alternatives. In Part II, this article reviews the choice frameworks under the GDPR and the CCPA, finding that although both differentiate on the basis of whether personal information is sensitive and on whether it is used solely for functional purposes, neither utilizes both opt-in and opt-out choices. This lack of utilization of both options results in a diffuse application of choice that does not properly differentiate between various degrees of identifiability.

In Part III, the analysis delineates between different types of personal information on the basis of whether the personal information is trackable and/or identifiable. Looking first to the computer science literature to understand the abilities of various types of privacy-preserving algorithms and the spectrum of identifiability that they enable, it is evident that the GDPR's and the CCPA's definitions of personal information are too broad to differentiate between meaningful differences in identifiability within them, and thereby too broad to effectively encourage privacy-preserving treatment. Thus, it would make sense to categorize personal information into three types: reasonably identifiable, pseudonymous, and non-trackable.

Presented in Part IV are examples of collection, use, and sharing of these three types of personal information. The article differentiates between uses of personal information that enable functionality of a service or app versus those that do not. These examples illustrate the need for notices that disclose these differences and the need for choice mechanisms that afford consumers different choices for different types of personal information.

In Part V, a new choice framework is constructed, taking into account both opt-in and opt-out choices, as well as collection, use, and sharing required as part of the terms of a service. Unlike the GDPR (which doesn't use opt-out) and the CCPA (which only uses opt-in for minors and financial incentives), the proposed framework utilizes the full spectrum of user choice options in order to incentive the full spectrum of privacy-preserving techniques. The article differentiates between functional and non-functional

72. *Id.* § 2(30).
73. *Id.* § 102(b)(2-3).
74. *Id.* § 102(b)(4).
75. *Id.* §§ 104(a), 108(a).
76. *Id.* §§ 104(d), 108(a).

use, between non-sensitive and sensitive personal information, and between use and sharing.

Illustrated in Part VI is the effect of this user choice framework on different types of advertising. It shows how the proposed choice framework incentives the use of contextual ads over audience segment ads, and the use of audience segment ads over behavioral ads, and how it disincentivizes tracking.

In Part VII, specific requirements are crafted for disclosures of collection, use, and sharing in privacy policies. These requirements include more detailed disclosures than those required in the GDPR or the CCPA, so that consumers may understand the degree of identifiability of their personal information collected and used, the flow of their personal information through the data ecosystem, and the associated privacy risks.

Finally, Part VIII develops statutory text that implements the proposed choice framework. There are proposed definitions for each of the types of personal information, the goal being to illustrate problems in current privacy policies, and create definitions to address these problems, drawing from the GDPR and the CCPA when helpful. Additionally, the article offers potential legal controls that should accompany each type of personal information.

The proposed statutory text is restated in the Appendix.

II. FAILURES OF THE GDPR AND THE CCPA TO USE BOTH OPT-IN AND OPT-OUT CHOICES

Consent is a primary driver for both the GDPR and the CCPA. However, they approach the issue of consent very differently, and, consequently, afford consumers substantially different choices.

Both the GDPR and the CCPA differentiate on the basis of whether the information is sensitive.[77] This article considers the definition of *sensitive information* in Part VIII. Both the GDPR and the CCPA also differentiate on the basis of whether the information is necessary to offer functionality of the service or application.[78] This article considers the definition of *functional use* in Part VIII.

When *non-sensitive personal information* is only used to provide functionality of the service or application, both the GDPR and the CCPA allow a business to mandate its collection and use in the terms and conditions of the service.[79]

However, when a business wishes to use *sensitive personal information* to provide functionality, the GDPR and the CCPA disagree. The CCPA allows a business to mandate the collection and use of personal information for functional purposes in the terms and conditions of the service.[80] In

77. Jordan, *supra* note 3, at 33-35.
78. *Id.* at 28.
79. GDPR, *supra* note 1, at art. 6(1)(b); Jordan, *supra* note 3, at 28.
80. Jordan, *supra* note 3, at 28.

contrast, the GDPR requires that the business obtain opt-in consent from the consumer, absent another legal basis for the collection and use.[81]

	Terms	Opt-out	Opt-in
Functional use, non-sensitive	X		
Functional use, sensitive	X		
Non-functional use, non-sensitive	X		
Non-functional use, sensitive		X	
Sharing, non-sensitive		X	
Sharing, sensitive		X	

Table 1. User choice under the CCPA.

When *non-sensitive personal information* is used for a purpose other than to provide functionality of the service or application, the GDPR and the CCPA again disagree. The CCPA allows a business to mandate the collection and use of personal information for non-functional purposes in the terms and conditions of the service.[82] In contrast, the GDPR requires that the business obtain opt-in consent from the consumer, absent another legal basis for the collection and use.[83]

	Terms	Opt-out	Opt-in
Functional use, non-sensitive	X		
Functional use, sensitive			X
Non-functional use, non-sensitive			X
Non-functional use, sensitive			X
Sharing, non-sensitive			X
Sharing, sensitive			X

Table 2. User choice under the GDPR.

When a business wishes to use *sensitive personal information* for a purpose other than to provide functionality of the service or application, the GDPR and the CCPA again disagree. The CCPA requires that the consumer be given an opt-out choice,[84] while the GDPR requires opt-in consent absent another legal basis.[85]

Finally, when a business wishes to share either personal information with another business, the GDPR and the CCPA again disagree. The CCPA again requires an opt-out choice,[86] while the GDPR again requires opt-in consent absent another legal basis.[87]

The resulting differences in choice between the GDPR and the CCPA are wide. While the GDPR and the CCPA both allow a business to mandate in the terms and conditions of a service the collection and use of personal information for functional purposes, they do not agree on anything else related to choice.

81. GDPR, *supra* note 1, at art. 9(2)(a).
82. Jordan, *supra* note 3, at 28.
83. GDPR, *supra* note1, at art. 6(1)(a).
84. CAL. CIV. CODE § 1798.121(a) (Deering, LEXIS through Ch. 11 of 2022 Reg. Sess.).
85. GDPR, *supra* note 1, at art. 9(2)(a).
86. CAL. CIV. CODE §§ 1798.120(a), 1798.121(b).
87. GDPR, *supra* note 1, at arts. 6(1)(a), 9(2)(a).

Furthermore, neither the GDPR nor the CCPA utilize all three options: mandating use through terms and conditions, requiring an opt-out choice, and requiring opt-in consent. The CCPA utilizes terms and opt-out, but not opt-in. The GDPR utilizes terms and opt-in, but not opt-out. This underutilization of all three options brings up the question of whether doing so could result in a more effective choice framework.

III. FAILURES OF THE GDPR AND THE CCPA TO ADDRESS THE SPECTRUM OF IDENTIFIABILITY

A. Limited Definitions in the GDPR and in the CCPA

Both the GDPR and the CCPA apply their choice frameworks to information related to an identifiable person, but not to information that is related to an unidentifiable person. The GDPR defines *personal data* (its version of personal information) as "any information relating to an identified or identifiable natural person."[88]

Under the GDPR, *personal data* does not include *anonymous information*, which it defines as "information which does not relate to an identified or identifiable natural person."[89]

Personal data is subject to the GDPR's choice framework, and *anonymous information* is not.

The CCPA 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."[90]

However, the CCPA also recognizes that there may be information that can be linked to a particular consumer or household, but for which the process of linking may be prohibitive due to the difficulty in finding other information with which it can be linked. In 2012, the Federal Trade Commission issued a report containing recommendations for businesses and policymakers.[91] It proposed that information be considered *de-identified information* if it is not reasonably linkable to a particular consumer or device.[92] In a similar vein, the CCPA defines *de-identified information* as "information that cannot reasonably be used to infer information about, or otherwise be linked to, a particular consumer . . . ."[93]

Under the CCPA, *personal information* does not include *de-identified information*. *Personal information* is subject to the CCPA's choice framework, and *de-identified information* is not.

88. *Id.* at art. 4(1).
89. *Id.* at recital 26.
90. CAL. CIV. CODE § 1798.140(v)(1).
91. FTC, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE (2012) [hereinafter *FTC Report*].
92. *Id.* at 21.
93. CAL. CIV. CODE § 1798.140(m).

Both the GDPR and the CCPA thus classify any information relating to a person into one of two mutually exclusive sets (for the GDPR, *personal data* or *anonymous information*; for the CCPA, *personal information* or *de-identified information*) based on whether the person is identifiable.

Unfortunately, while this partition of information into only two sets is simple, it does not reflect the spectrum of identifiability of personal information. Within the category of information that the GDPR classifies as *personal data* and that the CCPA classifies as *personal information*, research has repeatedly shown that there are substantial differences in the degree of identifiability.[94] These differences should be reflected in a choice framework.

B. Lack of Recognition of the Benefits of Pseudonymous Information

In *Shades of Gray: Seeing the Full Spectrum of Practical Data De-identification* Jules Polonetsky presents a spectrum of identifiability of information.[95] To differentiate degrees of identifiability, the article uses the concepts of a *direct identifier* and of an *indirect identifier*.[96] While there is no need to define these terms in a consumer privacy law, the concepts are useful. Simon Garfinkel, in a report by the National Institute of Standards and Technology, defines a *direct identifier* as "data that directly identifies a single individual."[97] Polonetsky somewhat similarly defines a *direct identifier* as "data that can be used to identify a person without additional information or with cross-linking through other information that is in the public domain."[98] Garfinkel then defines an *indirect identifier* as "information that can be used to identify an individual through association with other information."[99]

The most identifiable form of information is that relating to an identified person or household.[100] It contains direct identifiers such as a person's name, personal telephone number, personal email address, driver's license number, or social security number. Polonetsky calls such information *explicitly personal data*,[101] but this article will use the term *reasonably identifiable information*. This type of information is classified as personal information under both the GDPR and the CCPA.[102]

The second most identifiable form of information is information relating to a person or household that is identifiable but has not yet been

94. *See generally* Scott Jordan, *Aligning Legal Definitions of Personal Information with the Computer Science of Identifiability*, RES. CONF. ON COMMUN., INFO., AND INTERNET POL'Y (Sept. 2021), https://ssrn.com/abstract=3893833.

95. Jules Polonetsky et al., *Shades of Gray: Seeing the Full Spectrum of Practical Data De-identification*, 56 SANTA CLARA L. REV. 593 (2016).

96. *Id.*

97. SIMSON L. GARFINKEL, NAT'L INST. OF STANDARDS & TECHNOLOGY, DE-IDENTIFICATION OF PERSONAL INFORMATION 1, 40 (2015).

98. Polonetsky et al., *supra* note 95, at 605.

99. GARFINKEL, *supra* note 97, at 41.

100. Polonetsky et al., *supra* note 95, at 609.

101. *Id.*

102. Jordan, *supra* note 3, at 9-12.

identified, and that is tracked over time.[103] It does not contain direct identifiers, and thus the person or household cannot be identified using a direct identifier.[104] However, this type of information contains indirect identifiers, such as a device identifier or advertising identifier, that can be used to identify the person or household by combining the information with other information containing the same indirect identifiers.[105] The indirect identifiers can also be used to track the person or household over time.[106] Polonetsky calls such information *potentially identifiable*,[107] but this article will use the more common term *pseudonymous information*. This type of information is classified as personal information under both the GDPR and the CCPA, absent legal controls to prevent reidentification.[108]

Neither the GDPR nor the CCPA differentiates between *reasonably identifiable information* and *pseudonymous information* in their choice frameworks.[109] The GDPR requires opt-in consent for the sharing of both types of information.[110] The CCPA requires an opt-out choice from the sharing of either type of information.[111] As a consequence, neither the GDPR nor the CCPA incentivize the use of pseudonyms in their choice frameworks.

C. Lack of Recognition of the Benefits of Non-Trackable Information

A form of information that is less identifiable than *pseudonymous information* is information relating to a person or household that is identifiable but has not yet been identified, and that is *not* tracked over time.[112] It does not contain direct identifiers.[113] It may contain indirect identifiers, but these indirect identifiers cannot be persistent.[114] An example of a non-persistent identifier is a randomized identifier that is only used in a single interaction with a consumer.[115] Apple is beginning to use such one-time identifiers in some of its applications. Polonetsky calls such information *pseudonymous*,[116] but this article will use the term *non-trackable information*. This type of information is classified as personal information under both the GDPR and the CCPA, absent legal controls to prevent reidentification.[117]

103. Polonetsky et al., *supra* note 95, at 609-13.
104. *Id*.
105. *Id.*
106. *Id.*
107. *Id*.
108. Jordan, *supra* note 3, at 9-12.
109. *Id.*
110. *Id.* at 31-32.
111. *Id.*
112. Jordan, *supra* note 94, at 14-17.
113. *Id.*
114. *Id.*
115. Polonetsky et al., *supra* note 95, at 608.
116. *Id.* at 615-17.
117. Jordan, *supra* note 3, at 9-12.

Neither the GDPR nor the CCPA differentiate between *pseudonymous information* and *non-trackable information* in their choice frameworks.[118] The GDPR requires opt-in consent for the sharing of both types of information.[119] The CCPA requires an opt-out choice from the sharing of either type of information.[120] As a consequence, neither the GDPR nor the CCPA incentivize the use of one-time identifiers in their choice frameworks. However, the use of such one-time identifiers could eliminate tracking.

D. Differences in Consumer Views of Reasonably Identifiable Information, Pseudonymous Information, and Non-Trackable Information

The consumer views of reasonably identifiable information, pseudonymous information, and non-trackable information are quite different.

An example of reasonably identifiable information is a person's name paired with personal information about the person.[121] The information can be used for behavioral advertising, since the personal information may provide valuable information about the person's interests. An ad broker can collect reasonably identifiable information and create a profile of the person, resulting in tracking. Furthermore, this profile is associated with the person's name.

An example of pseudonymous information is a device or advertising identifier paired with personal information about the person using the device. As with reasonably identifiable information, the information can be used for behavioral advertising and tracking. However, the profile is associated with the device or advertising identifier, not with the person's name, providing that device or advertising identifier is not associated with a person or household. As a result, the person seeing the advertisements may properly perceive that they are pseudonymous.

An example of non-trackable information is a one-time identifier paired with personal information. As with the other types of information, it can be used for behavioral advertising. However, it cannot be used for tracking. As a result, the person seeing the advertisements may properly perceive that they are pseudonymous and not tracked.

118. *Id.*
119. *Id.* at 14-16.
120. *Id.*
121. *Id.* at 6-8.

	Reasonably identifiable information (I)	Pseudonymous information (P)	Non-trackable information (N)
Example of personal information	Name + personal information	Device or advertising identifier + personal information	One-time identifier + personal information
Example of a user's view of a use of personal information	Behavioral advertising + tracking + associated with my name	Behavioral advertising + tracking + associated with a pseudonym	Behavioral advertising + no tracking + associated with a one-time identifier

Table 3. Examples of the Three Most Identifiable Types of Personal Information

These three types are summarized in Table 3. Although neither the GDPR nor the CCPA choice frameworks differentiate between these three types of personal information, consumers are likely to view their use very differently.

IV. EXAMPLES OF COLLECTION, USE, AND SHARING OF DIFFERENT TYPES OF PERSONAL INFORMATION

Part V will formulate a framework for choices that consumers should be given in a consumer privacy law. To inform the development of this framework, this section gives examples of collection, use, and sharing of the types of personal information discussed in Part III.

Both the GDPR and the CCPA make some attempts to distinguish between uses of personal information that are related to the functionality of the service or app versus uses that are not related. Before examining their approaches to this distinction, this article provides some examples of uses of various types of personal information.

A. Functional Use

Some uses of personal information enable functions or features of a service or app. Table 4 presents some examples.

	Reasonably identifiable information (I)	Pseudonymous information (P)	Non-trackable information (N)
Functional use of non-sensitive personal information	Movie app gives personalized recommendations based on name + non-sensitive audience segment	Movie app gives personalized recommendations based on pseudonym + non-sensitive audience segment	Movie app gives personalized recommendations based on random rapidly resetting identifier + non-sensitive audience segment
Functional use of sensitive personal information	Map app provides turn-by-turn directions based on name + precise geo-location	Map app provides turn-by-turn directions based on pseudonym + precise geo-location	Map app provides turn-by-turn directions based on rapidly resetting identifier + current precise geo-location

Table 4. Examples of Functional Uses of Various Types of Personal Information

Consider a movie app that provides personalized recommendations. In order to determine recommendations, suppose the app observes the title of a

movie that a user has watched, uses the observation to place the user into non-sensitive audience segments (e.g., likes historical dramas), and then immediately discards each movie title. If the app pairs the non-sensitive audience segments with the user's name, then the combination of the user's name and non-sensitive audience segments constitutes non-sensitive reasonably identifiable information. Alternatively, if the app assigns the user a pseudonym, the app pairs the non-sensitive audience segments with the pseudonym, then the combination of the pseudonym and non-sensitive audience segments constitutes non-sensitive pseudonymous information. Finally, if the app assigns the user a random rapidly identifier, then the combination of the random rapidly resetting identifier and non-sensitive audience segment constitutes non-sensitive non-trackable information.

Next, consider a map app that provides turn-by-turn directions. In order to determine directions, suppose the app collects the precise geo-location of the user. If the app pairs the precise geo-location with the user's name, then the combination constitutes sensitive reasonably identifiable information. Alternatively, if the app assigns the user a pseudonym, then the combination of the pseudonym and precise geo-location constitutes sensitive pseudonymous information. Finally, if the app assigns the user a random rapidly resetting identifier and collects only the current geo-location of the user (but not the location history), then the combination of the random rapidly resetting identifier and current precise geo-location constitutes sensitive non-trackable information.

B. Non-Functional Use

Some uses of private person information do not enable functions or features of a service or app, but are used to subsidize the service or app. Table 5 presents some examples.

	Reasonably identifiable information (I)	Pseudonymous information (P)	Non-trackable information (N)
Non-functional use of non-sensitive personal information	Search provider displays ads based on name + non-sensitive audience segment	Search provider displays ads based on device identifier + non-sensitive audience segment	Search provider displays ads based on random rapidly resetting identifier + non-sensitive audience segment
Non-functional use of sensitive personal information	Social network displays ads based on name + liked social network posts	Search provider displays ads based on device identifier + sensitive audience segment	Search provider displays ads based on device identifier + sensitive audience segment

Table 5. Examples of Non-Functional Uses of Various Types of Personal Information

Consider a search provider that displays personalized ads aside search results. In order to determine which ads to display, suppose the search provider uses the search terms to place the user into non-sensitive audience segments (e.g., interested in tennis), and then immediately discards the search terms. If the search provider pairs the non-sensitive audience segments with the user's name, then the combination of the user's name and non-sensitive audience segments constitutes *non-sensitive reasonably identifiable*

information. Alternatively, if the search provider pairs the non-sensitive audience segments with a device identifier, then the combination of the device identifier and non-sensitive audience segments constitutes *non-sensitive pseudonymous information*. Finally, if the search provider assigns the user a random rapidly identifier, then the combination of the random rapidly resetting identifier and non-sensitive audience segment constitutes *non-sensitive non-trackable information*. However, none of these uses are functional; the functional use is limited to displaying the search results, not the ads.

Similarly, consider a social network provider that displays personalized ads aside social network activity. In order to determine which ads to display, suppose the social network provider stores and analyzes a list of social network posts that the user has liked. Because this information constitutes app usage history, it is properly classified as *sensitive personal information*. If the social network provider pairs the list of social network posts that the user has liked with the user's name, then the combination constitutes *sensitive reasonably identifiable information*. This use is non-functional; the functional use is limited to displaying the social network posts, not the ads.

C. Sharing

In addition to using personal information, service or app providers may also share personal information. Table 6 presents some examples.

	Reasonably identifiable information (I)	Pseudonymous information (P)	Non-trackable information (N)
Sharing of non-sensitive personal information	Website shares advertising identifier + non-sensitive audience segments with an ad broker	Website shares pseudonym + non-sensitive audience segments with an ad broker	Website shares one-time identifier + non-sensitive audience segments with an ad broker
Sharing of sensitive personal information	Website shares advertising identifier + user behavior with an ad broker	Website shares pseudonym + user behavior with an ad broker	Website shares one-time identifier + user behavior with an ad broker

Table 6. Examples of Sharing of Various Types of Personal Information

Consider a website that wishes to display ads on one of its webpages. In order to determine which ads to display, suppose the website collects information about user interests, and places the user into non-sensitive audience segments. If the search provider discloses to an ad broker the non-sensitive audience segments paired with a user's advertising identifier, and does not limit how the ad broker uses this information, then the combination of the advertising identifier and non-sensitive audience segments constitutes *non-sensitive reasonably identifiable information*. The information is reasonably identifiable because the user corresponding to the advertising identifier is reasonably identifiable due to the lack of limitations on the ad broker's use of the information.

However, if the website discloses to an ad broker the same information pursuant to a written contract that prohibits the ad broker from identifying the

person to whom the information relates, then the information constitutes *pseudonymous information*.

Finally, consider the case in which the website discloses to an ad broker the non-sensitive audience segments paired with a one-time identifier, pursuant to a contract that ensures that the information remains in a form in which there is no reasonable possibility of logical association with other information relating to the person or household to whom the one-time identifier relates. Then the combination of the one-time identifier and non-sensitive audience segment constitutes *non-trackable information*.

V. PROPOSED CHOICE FRAMEWORK

There are two problems with the policy choices made in the GDPR and the CCPA. First, neither use both opt-in consent and opt-out choice.[122] The GDPR allows functional use of non-sensitive personal data to be mandated as part of the terms and conditions of service, but then jumps all the way up to opt-in consent for all other uses and for sharing.[123] The CCPA requires that users be given an opt-out choice from non-functional use of sensitive personal information and from all sharing, but never requires opt-in consent, even for sharing of sensitive personal information.[124] A superior public policy can be achieved by using opt-out choice for some types of processing and opt-in consent for others.

Second, neither the GDPR nor the CCPA differentiate between *non-trackable information*, *pseudonymous information*, and *reasonably identifiable information*.[125] By failing to differentiate, neither the GDPR nor the CCPA provide much incentive for a business to use less identifiable forms of personal information.

If *pseudonymous information* were differentiated from *reasonably identifiable information*, then there would be an incentive to pair personal information with pseudonyms rather than with names, and hence prevent the person or household relating to the personal information from being identified.

Similarly, if *non-trackable information* were differentiated from *pseudonymous information*, then there may be an incentive to pair personal information with one-time identifiers, and hence prevent tracking. Instead, both the GDPR and the CCPA attempt to reduce profiling in other ways. Both require specific disclosure relating to profiling. However, these disclosures don't translate into the availability of different user choices.

Use of the full range of options would also enable policy to match the full range of user perceptions of the risk associated with different uses of personal information. Sensitive personal information should be accorded higher protections that non-sensitive personal information. More identifiable forms of personal information should be accorded higher protections that less

122. *See supra* Part II.
123. *See supra* Part II.
124. *See supra* Part II.
125. *See supra* Part III.

identifiable forms. In addition, consumers associate a higher risk when their personal information is widely shared among the data ecosystem than when it is held only by the entity with which the consumer is interacting.

This section develops a choice framework. Statutory text to implement this framework is presented in Part VIII.

A. Functional Use

Functional use is a good starting point. Both the GDPR and the CCPA agree that functional use of non-sensitive personal information can be mandated in the terms and conditions of a service. This makes sense. There is a natural tradeoff here. A user must agree to the use of personal information that is technically required to provide the functionality of the service or app. The tradeoff is direct: use of information in exchange for functionality.

However, while the CCPA applies this same logic to functional use of sensitive personal information, the GDPR requires opt-in consent.[126] This makes little sense. If the sensitive personal information is technically required to provide the functionality, the choice remains the same; either agree to use of the personal information or don't use the function. All that requiring opt-in consent does is move the prompt to make the decision from the time at which the service or app is used to the time at which the functionality is used. A business should be allowed to mandate the functional use of both sensitive and non-sensitive personal information in the terms and conditions of a service.

B. Non-Functional Use

Next consider non-functional use (but not sharing) of non-sensitive personal information. Since the use is not functional, it is likely that the purpose of the use is to subsidize the service or app. The CCPA allows non-functional use to be mandated, while the GDPR requires opt-in consent.[127] This is exactly where there should be a distinction based on the level of identifiability. If a consumer privacy law requires that a user be given an opt-out choice for the non-functional use of *reasonably identifiable information*, but not for less identifiable forms, then businesses will be incentivized to prevent the person or household relating to the personal information from being identified.

Next to consider is non-functional use (but not sharing) of sensitive personal information. The CCPA requires that a user be given an opt-out choice, while the GDPR requires opt-in consent.[128] If a consumer privacy law requires opt-in consent for the non-functional use of *sensitive reasonably identifiable information*, but only that users be given an opt-out choice for the non-functional use of *sensitive pseudonymous information*, then businesses will be strongly incentivized to prevent the identification of the person or

126. Jordan, *supra* note 3, at 33-35.
127. *Id.* at 30-32.
128. *Id.* at 33-35.

household to whom sensitive personal information is related. In addition, if a consumer privacy law requires that users be given an opt-out choice for the non-functional use of *sensitive pseudonymous information*, but not for *sensitive non-trackable information*, then businesses will be incentivized to not track people using sensitive personal information.

C. Sharing

Finally, consider the sharing of personal information. The CCPA requires that users be given an opt-out choice, while the GDPR requires opt-in consent.[129] Neither differentiates between non-sensitive and sensitive personal information.[130] Again, there is a superior option in which opt-in consent is required for more identifiable forms of personal information and for more sensitive information. Specifically, opt-in consent should be required for the sharing of both non-sensitive and sensitive *reasonably identifiable information*, and for the sharing of *sensitive pseudonymous information*. In addition, users should be given an opt-out choice from the sharing of all other forms of *reasonably linkable information*.

	Terms	Opt-out	Opt-in
Functional use, non-sensitive	N, P, I		
Functional use, sensitive	N, P, I		
Non-functional use, non-sensitive	N, P	I	
Non-functional use, sensitive	N	P	I
Sharing, non-sensitive	N	P	I
Sharing, sensitive		N	P, I

Table 7. Proposed User Choice in a Market with Effective Competition

The resulting choice framework is summarized in Table 7, where N denotes non-trackable information, P denotes pseudonymous information, and I denotes reasonably identifiable information. Comparing this framework to the GDPR and the CCPA frameworks in Tables 1 and 2, the full range of options are now used. More identifiable forms of personal information are accorded greater protection, thus incentivizing good privacy practices. Non-functional use faces stronger forms of user consent than functional uses and sharing faces yet stronger forms of user consent. Use and sharing of sensitive personal information often requires a stronger form of user consent than does use and sharing of non-sensitive personal information. Finally, in the cases in which GDPR and the CCPA disagree, this proposal often chooses an intermediate option.

There is one last policy issue that should be addressed here. There are some uses of personal information that merit higher thresholds than those proposed in Table 7. First, personal information that takes the form of communications has traditionally been afforded higher privacy protections. Section 705 of the Communications Act prohibits a communications provider from divulging the "existence, contents, substance, purport, effort, or meaning" of communications, except for functional purposes or with

129. *Id.* at 31-32.
130. *Id.* at 33-35.

consent.[131] Second, in situations in which consumers have few choices for a provider of a particular service, competition between businesses based on their privacy policies is less likely. For example, in many geographical regions in the United States, there is only a single Internet Service Provider that offers broadband service with speeds that are acceptable to many consumers. In this case, the choice framework should reflect the lack of impact of competition upon privacy.

In either of these situations, while it still makes sense to allow such a business to mandate functional use in the terms and conditions of a service, when a business wishes to use personal information for non-functional purposes, or wishes to share personal information, the choice framework should further incentive the use of less identifiable forms of information. This can be accomplished by moving each type of personal information up one notch, e.g., from mandated to opt-out or from opt-out to opt-in. The resulting choice framework for communications providers or in a market without effective competition is illustrated in Table 8.

	Terms	Opt-out	Opt-in
Functional use, non-sensitive	N, P, I		
Functional use, sensitive	N, P, I		
Non-functional use, non-sensitive	N	P	I
Non-functional use, sensitive		N	P, I
Sharing, non-sensitive		N	P, I
Sharing, sensitive			N, P, I

Table 8. Proposed User Choice in a Market Without Effective Competition and for Communications Services

VI. EMPOWERING CONSUMERS WHO DESIRE PRIVACY-PRESERVING ADVERTISING

This section investigates how advertising can be implemented using different types of personal information. The goal is to understand if and how differentiating between different types of personal information may affect consumers.

This section of the article gives examples of advertising based on reasonably identifiable information, pseudonymous information, and non-trackable information. In each example, the following entities are considered:

- An ad venue, an entity which offers a venue in which ads appear, e.g., a website with ads on its webpages.
- An advertiser, an entity which offers ads to be published in ad venues, e.g., a business advertising a product.
- An ad broker, an entity which determines the ad venues on which a particular ad will appear, e.g., a business that contracts with both ad venues and advertisers and that determines the placement of each ad.

The examples do not address other businesses that are part of the ecosystem. They presume that the advertiser and the ad broker have a contract

131. 47 U.S.C. § 605(a).

under which the advertiser pays the ad broker to place an ad, and that the ad broker and the ad venue have a contract under which the ad broker pays the ad venue to have the ad appear. The examples presume that none of the entities have market power.

They also distinguish between the acts of "placing" and "publishing" an ad. *Placing* an ad is the function of determining the ad venues on which an ad appears; the examples assume this is done by the ad broker. *Publishing* an ad is the technological function of causing the ad to appear; the examples assume this may be done by any of the parties.

Both the GDPR and the CCPA distinguish between entities that make decisions about the collection, use, and sharing of personal information versus entities that are hired to implement specific tasks involving the collection and use of personal information.[132] The GDPR calls the former *controllers* and the latter *processors*.[133] The CCPA calls the former *businesses* and the latter *service providers* or *contractors*.[134] This article uses the term *controller* to describe the entity that makes decisions about collection, use, and sharing. When a controller shares personal information with a third party, this article calls that third party a *contractor* if and only if there is a contract between the controller and the third party under which the third party uses that personal information only for the purposes specified by the controller. These terms are defined, and the contractual terms are discussed in Part VIII.

For each advertising example, the types of personal information collected and used by each party, and the types disclosed or shared between parties, are considered. How the information may be classified is discussed. Whether each entity might be a controller or a contractor is also considered. Finally, the impact of the proposed user choice framework is discussed.

This section starts with a privacy-invasive example that is commonplace today, and then works through a sequence of increasingly less privacy-invasive examples.

A. Using Reasonably Identifiable Information for Behavioral Ads Published by an Ad Broker

First, this article considers the use of reasonably identifiable information to place behavioral ads. In this example, the advertiser chooses to advertise based on the behavior of people in the desired audience. *Behavioral advertising* can describe this form.

Imagine that SmithLuxuryCars.com wishes to advertise to people who are interested in luxury automobiles. SmithLuxuryCars.com purchases a service from AbcAdBroker.com to place ads that will be seen only by people who are interested in luxury automobiles based on detailed profiles of these people. AbcAdBroker.com contracts with websites (including CarReviews.com) that are often visited by people who are interested in luxury automobiles and that have detailed profiles of their website visitors.

132. Jordan, *supra* note 3, at 15-16.
133. *Id.*
134. *Id.*

When a person visits CarReviews.com, the website collects the person's email address and advertising identifier, and looks up a profile that was previously compiled based on the person's activity on the website. CarReviews.com shares the person's IP address, advertising identifier, and profile with AbcAdBroker.com, which shares this information with advertisers, and auctions off the ad. SmithLuxuryCars.com wins the auction, and AbcAdBroker.com tells CarReviews.com to redirect the website visitor to SmithLuxuryCars.com to obtain the ad. The ad is thus seen only be people whose profiles demonstrate that they are interested in luxury automobiles.

The collection, use, and sharing of personal information is shown in Figure 1. The combination of the person's IP address, email address, advertising identifier, and profile is *reasonably identifiable information*. The information shared with the ad broker and the advertiser remain *reasonably identifiable information*, presuming that the contracts between the ad venue, ad broker, and advertiser do not prohibit the ad broker or the advertiser from using the IP address and advertising identifier to identify the person. Furthermore, since the profile contains web browsing history, the information is *sensitive*.

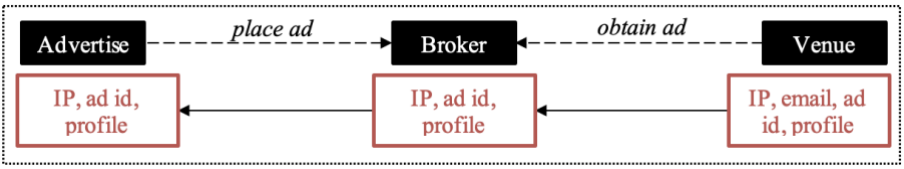

Figure 1. Behavioral Ads

The ad venue is a controller, since it determines the purposes and means of its collection and use of personal information. The ad broker and advertiser are also controllers, since neither is limited to using the information shared with it solely for the purposes of placing the ad.

The ad venue is using and sharing sensitive reasonably identifiable information. Under the proposed user choice framework, it would need to first obtain opt-in consent from the website visitor for this non-functional use and for sharing. If it does so, it would presumably pass this consent on to the ad broker for it to use and share this information, which would presumably pass this consent on to the advertiser to use this information.

This type of advertising is common, but privacy-invasive since it uses the most identifiable form of information. The proposed user choice framework thus places a high threshold on behavioral advertising. Because the information is both sensitive and reasonably identifiable, opt-in consent is required.

B. Using Pseudonymous Information for Audience Segment Ads with Tracking

Next, consider the use of pseudonymous information to place audience segment ads. In this example, the advertiser chooses to advertise to people

who fall into specified audience segments based on prior tracking of these people.

For example, SmithLuxuryCars.com wishes to advertise to people who are interested in luxury automobiles. SmithLuxuryCars.com purchases a service from AbcAdBroker.com to place ads that will be seen only by people who fall into a luxury automobile audience segment, based on prior tracking. AbcAdBroker.com contracts with websites (including CarReviews.com) that are often visited by people who are interested in luxury automobiles and that can determine if its website visitors fall into the luxury automobile audience segment.

When a person visits CarReviews.com, the website collects the person's advertising identifier, and looks up a profile that was previously compiled based on the person's activity on the website. However, instead of sharing the person's profile with AbcAdBroker.com, CarReviews.com selects audience segments based on the profile, and only shares the person's IP address, advertising identifier, and audience segments. AbcAdBroker.com awards the ad to SmithLuxuryCars.com, who is the advertiser willing to pay the most to place an ad to a person in the luxury automobile audience segment. AbcAdBroker.com tells CarReviews.com to redirect the website visitor to AbcAdBroker.com to obtain the ad. AbcAdBroker.com generates summary statistics about its ad placements for SmithLuxuryCars.com, but it does not share information about the individual people who saw the ad.

The collection, use, and sharing of personal information is shown in Figure 2. Since a consumer may be reasonably identified using the consumer's IP address, the combination of the person's IP address, advertising identifier, and profile is *reasonably identifiable information* if there are no legal controls preventing this identification. However, if the legal controls proposed in Part VIII are in place, then the personal information is *sensitive pseudonymous information*, and all entities using and sharing this information would commit to maintaining in a pseudonymous form. In addition, when the ad venue converts the profile information into audience segments, the information is transformed from *sensitive* to *non-sensitive* (shown as a dashed rectangle in the figure), and thus the combination of the person's IP address, advertising identifier, and audience segments shared with the ad broker are *non-sensitive pseudonymous information*, if the contract between the ad broker and the ad venue commits the ad broker to implement the corresponding legal controls (including not re-identifying the person) and to maintain the information in *non-sensitive* form. The advertiser only receives summary statistics, which qualify as *anonymous information*.

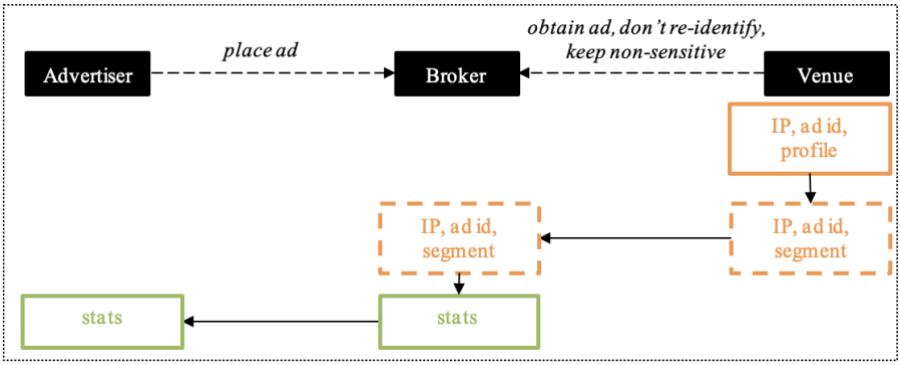

Figure 2. Audience Segment Ads with Tracking

As in the previous example, all three entities are *controllers*. The ad venue is using *sensitive pseudonymous information*. Under the proposed user choice framework, it would need to give the website visitor the ability to opt-out of this non-functional use. The ad venue is also sharing *non-sensitive pseudonymous information* with the ad broker, and it must separately give the website visitor the ability to opt-out of this sharing. The ad broker's non-functional use of *non-sensitive pseudonymous information* does not require an opt-out choice, but the website visitor can prohibit that use by simply opting out from the ad venue's sharing of that information. Finally, the advertiser only collects *anonymous information*, which is exempt from choice requirements.

The proposed user choice framework thus places a moderate threshold on audience segment ads with tracking. Because the information used by the ad venue is sensitive but pseudonymous, an opt-out choice is required for this use. Because the information shared by the ad venue is also pseudonymous but non-sensitive, an opt-out choice is also required for this sharing. The threshold is lower than on behavioral ads, which required opt-in consent. This lower threshold incentivizes the use of pseudonymous information instead of readily identifiable information, allowing consumers to remain pseudonymous.

C. Audience Segment Ads Without Tracking

The advertiser chooses to advertise to people who fall into specified audience segments, based solely on the current interaction with these people.

For example, SmithLuxuryCars.com wishes to advertise to people who are interested in luxury automobiles. SmithLuxuryCars.com purchases a service from AbcAdBroker.com to place ads that will be seen only by people who fall into a luxury automobile audience segment, based solely on the current interaction with these people. AbcAdBroker.com contracts with websites (including CarReviews.com) that are often visited by people who are interested in luxury automobiles and that can determine if its website visitors fall into the luxury automobile audience segment based on the current website visit.

When a person visits CarReviews.com, the website collects the person's advertising identifier, and determines audience segments, based on the current website visit only. It generates a one-time identifier, and shares that one-time identifier and audience segments with AbcAdBroker.com, who awards the ad to SmithLuxuryCars.com, the advertiser willing to pay the most to place an ad to a person in the luxury automobile audience segment. AbcAdBroker.com tells CarReviews.com to publish SmithLuxuryCars.com's ad. AbcAdBroker.com generates summary statistics about its ad placements for SmithLuxuryCars.com, but it does not share information about the individual people who saw the ad.

The collection, use, and sharing of personal information is shown in Figure 3. The combination of the person's IP address, advertising identifier, and profile is sensitive pseudonymous information, if the ad venue implements the corresponding legal controls discussed in Part VIII (including not re-identifying the person). However, when the ad venue converts the profile information into audience segments and pairs it with a one-time identifier instead of an IP address, the information is transformed from sensitive to non-sensitive and from trackable to non-trackable. Thus, the combination of the one-time identifier and audience segments shared with the ad broker are non-sensitive non-trackable information, if the contract between the ad broker and the ad venue commits the ad broker to implement the corresponding legal controls (including maintaining the information in non-trackable form). The advertiser only receives summary statistics, which qualify as anonymous information.

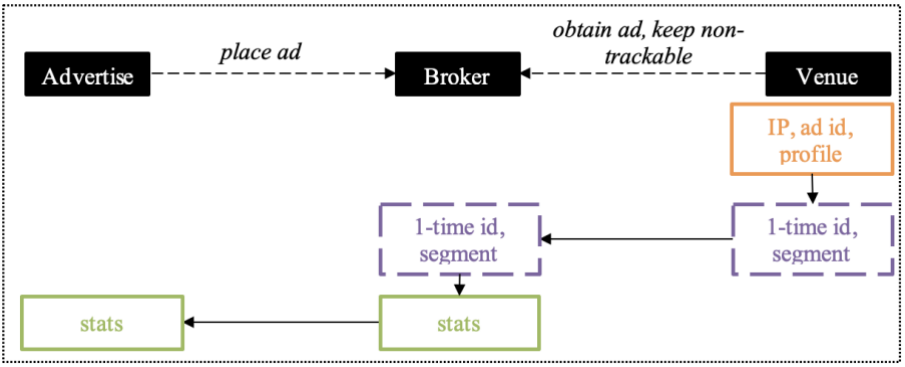

Figure 3. Audience Segment Ads Without Tracking

As in the previous examples, all three entities are controllers. As in the example with tracking, the ad venue is using sensitive pseudonymous information, and this it would need to give the website visitor the ability to opt-out of this non-functional use. However, the ad venue is only sharing non-sensitive non-trackable information with the ad broker, and under the proposed user choice framework it does not need to give the website visitor a separate opt-out choice from this sharing.

There is an alternative advertising model that results in similar consequences, but which allows the ad broker to publish the ad. Suppose the ad broker commits to acting as a contractor for the ad venue, by processing

the shared information solely for the purposes of obtaining ads for the venue. Then the ad venue may share IP addresses with the ad broker instead of one-time identifiers, and the ad venue can publish the ad instead of asking the ad venue to do so. In this situation, because the ad broker is acting as a contractor, the ad venue similarly needs to give the website visitor the ability to opt-out of this non-functional use.

The proposed user choice framework thus places a low threshold on audience segment ads without tracking. Because the information used by the ad venue is sensitive but pseudonymous, an opt-out choice is required for this use. However, because the information shared by the ad venue is both non-sensitive and non-trackable, no additional choice is required for this sharing. The threshold is lower than on ads with audience segment ads with tracking, which required an opt-out choice from both use and sharing. This lower threshold incentivizes the use of one-time identifiers and thereby reduces tracking.

D. Contextual Ads

An advertiser advertises basely solely on characteristics of the ad venue. This article uses the term contextual advertising to describe this form.

For example, SmithLuxuryCars.com wishes to advertise on websites that are frequently viewed by people who are interested in luxury automobiles. SmithLuxuryCars.com purchases a service from AbcAdBroker.com to place ads on such websites. AbcAdBroker.com contracts with websites (including CarReviews.com) that provide summary statistics to show that they are often visited by people who are interested in luxury automobiles.

When people visit CarReviews.com, the website keeps track of the types of automobiles they are interested in, but it does not store any identifiers of its website visitors. In addition, it generalizes this information. Based on the generalized information, CarReviews.com generates summary statistics, including the percentage of its website visitors who are interested in luxury automobiles. It shares these statistics with AbcAdBroker.com, which auctions ads based on these statistics, and SmithLuxuryCars.com wins the auction. AbcAdBroker.com tells CarReviews.com to publish SmithLuxuryCars.com's ad.

The collection, use, and sharing of personal information is shown in Figure 4. The generalized information used by the ad venue may qualify as non-sensitive de-identified information if the ad venue implements the corresponding legal controls (including maintaining the information in de-identified form). The ad broker and the advertiser only receive summary statistics, which qualify as anonymous information.

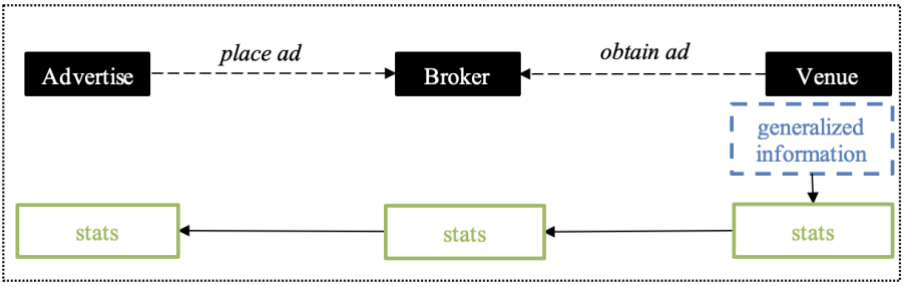

Figure 4. Contextual Ads

As in the previous examples, all three entities are *controllers*. However, the ad venue only uses *non-sensitive de-identified information*, and thus under the proposed user choice framework can require this use in its terms and conditions.

The proposed user choice framework thus places no threshold on contextual advertising. The threshold is lower than on ads with audience segment ads without tracking, which required an opt-out choice. This lower threshold incentivizes contextual advertising over audience segment ads.

VII. PROPOSED NOTICE REQUIREMENTS

In this section, transparency regarding collection, use, and sharing of personal information is considered. One of the goals of transparency is to allow consumers and privacy experts to understand collection, use, and sharing. Another goal of transparency is to empower consumers to make choices.

A. Types of Notice

The GDPR and the CCPA both require transparency, but they require different types of notices at different points in time.[135]

The GDPR requires notices from controllers, but not from processors, about processing of personal data, which includes collection, use, and sharing.[136] The content of required notices is considered in the following subsections. When a controller obtains personal data directly from the individual whom the personal data concerns, the GDPR requires that the notice be given "at the time when personal data are obtained."[137] 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 provide notice to the person "within a reasonable period after obtaining the personal data, but at the latest within one month."[138] When personal data is shared, the GDPR requires that the corresponding

135. Jordan, *supra* note 3, at 16-25.
136. *Id.*
137. GDPR, *supra* note 1, at art. 13(1).
138. *Id.* at art. 14(3)(a).

notice be given "when the personal data are first disclosed to the recipient."[139] The GDPR doesn't specify whether these notices must be public (e.g., in a publicly accessible privacy policy) and/or must be given directly to the person concerned, other than to say that the notices must be in an "easily accessible form." [140] The GDPR requires that notices from controllers include information about processing by the controller's processors.[141]

The CCPA similarly requires notices from businesses, but not from service providers or contractors, about collection, use, and sharing of personal information.[142] Unlike the GDPR, the CCPA does not distinguish between businesses that collect personal information directly from the individual whom the information concerns and those that collect personal information from an intermediary, and the CCPA does not have a separate requirement for notice to be provided at the point of sharing of personal information.[143] However, unlike the GDPR, the CCPA specifies that notices must be provided both in "its online privacy policy … or its internet website" [144] and "at or before the point of collection."[145] Similar to the GDPR, the CCPA requires that notices from businesses include information about collection, use, and sharing by the business's service providers and contractors.[146]

In addition to notices about collection, use, and sharing of personal information, both the GDPR and the CCPA require notices about user rights of access, correction, deletion, and consent.[147] However, these additional notices are outside the scope of this article.

B. Contents of Notices About Collection and Use

Most privacy policies today give separate disconnected disclosures about a business's collection of personal information, its use of personal information, and its sharing of personal information. However, collection and use are tightly connected, and notices about collection and use should be combined so that consumers may understand how each category of personal information is used. In contrast, sharing is conceptually distinct, and notices about sharing should be distinct. This approach also supports the choice framework proposed in Part V, which similarly treats use and sharing differently. Notices about collection and use are discussed in this subsection and notice about sharing is discussed in the following subsection.

---

139. *Id.* at art. 14(3)(c).

140. *Id.* at art. 13(1). Also *see id.* at recital 58, which envisions that notice may be "addressed to the public or to the data subject."

141. *Id.* at art. 28(3)(e).

142. Jordan, *supra* note 3, at 16-25.

143. *Id.*

144. CAL. CIV. CODE §1798.130(a)(5) (Deering, LEXIS through Ch. 11 of 2022 Reg. Sess.).

145. *Id.* § 1798.100(a).

146. *Id.* § 1798.130(a)(3)(A).

147. GDPR, *supra* note 1, at arts. 13(2)(b), 14(2)(c); CAL. CIV. CODE § 1798.130(a)(5)(A).

1. Categories of Personal Information

The CCPA requires that privacy policies include "the categories of personal information it *has collected* about consumers in the preceding twelve months,"[148] and that notices provided at or before the point of collection include "[t]he categories of personal information *to be collected*."[149] The CCPA also specifically requires that the categories of personal information include "the categories of sensitive personal information."[150] The GDPR has a similar requirement that notices include "the categories of personal data" the controller has collected.[151]

Notice of the categories of personal information collected is beneficial, but the disclosed categories are sometimes too broad to provide information sufficient for consumers to understand what personal information is collected. For example, while some privacy policies disclose that they collect the IP address and/or the IMEI of the device that a consumer is using,[152] other privacy policies merely disclose that they collect unspecified "device identifiers."[153] Similarly, while some privacy policies disclose that they collect the Apple and Android advertising identifiers,[154] other privacy policies merely disclose that they collect unspecified "[a]dvertising [identifiers]."[155]

Regarding the level of detail or granularity of these categories, the CCPA requires that they use "the specific terms set forth" in the definitions of personal information and sensitive personal information.[156] The CCPA regulations require that they be described "in a manner that provides consumers a meaningful understanding of the information being collected."[157] This is a good start, but the information should not only provide a meaningful understanding, it should also be sufficient for consumers to act upon the information.

---

148. CAL. CIV. CODE § 1798.130(a)(5)(B)(i) (emphasis added).

149. *Id.* § 1798.100(a)(1) (emphasis added).

150. *Id.* § 1798.100(a)(2).

151. GDPR, *supra* note 1, at art. 14(1)(d). The GPDR is explicit about this requirement for personal data that is not obtained directly from the individual whom the personal data concerns. Inexplicably, it is unclear whether the GDPR has a similar notice requirement when personal data is obtained directly from the individual; note the omission of such a requirement in GDPR, art. 13, as compared to its inclusion in art. 14(1)(d).

152. *See, e.g.*, *Google Privacy Policy*, GOOGLE, https://policies.google.com/privacy?hl=en-US (last updated July 1, 2021) (under "Unique identifiers") [https://perma.cc/L4AT-TSVF].

153. *See, e.g.*, *AT&T Privacy Policy*, AT&T, https://about.att.com/csr/home/privacy/full_privacy_policy.html (last updated Nov. 1, 2021) (under "The information we collect") [https://perma.cc/ZC34-JQJ8].

154. *See, e.g.*, *Privacy Policy*, THE WEATHER CO., https://weather.com/en-US/twc/privacy-policy (last updated Oct. 21, 2021) (under "Use of Advertising Identifiers") [https://perma.cc/R9UN-ZJM9].

155. *See, e.g.*, *Privacy Policy*, KAYAK, https://kayak.com/privacy (last updated July 1, 2021) (under "What are Cookies?") [https://perma.cc/SSM7-W36A].

156. CAL. CIV. CODE § 1798.130(c) (Deering, LEXIS through Ch. 11 of 2022 Reg. Sess.).

157. California Consumer Privacy Act Regulations, CAL. CODE REGS. tit. 11, §§ 999.300, .305(b)(1), .308(c)(1)(d) (2020) [hereinafter CCPA Regulations].

An important policy question is which type of personal information should be subject to disclosures about collection, use, and sharing. The GDPR requires disclosure about all personal data, which includes de-identified information but not anonymous information.[158] The CCPA requires disclosure about all personal information, which excludes both de-identified information and anonymous information.[159] However, neither de-identified information nor anonymous information should be subject to the proposed choice framework, as neither presents significant privacy risks. However, it is important to understand the collection, use, and sharing of both types of personal information in order to ensure that the personal information satisfies the characteristics required to be classified as de-identified information or anonymous information. Thus, notices about collection, use, and sharing should be applied not only to reasonably linkable information but to all personal information. A consumer privacy law should thus require:

> A controller shall maintain a publicly accessible privacy policy. The privacy policy shall disclose accurate information regarding the controller's collection, use, and sharing of personal information sufficient for consumers to make informed choices regarding the use of the controller's services.[160]

Notice of the categories of personal information collected is also insufficient to provide consumers with the information necessary to understand the degree of identifiability of the personal information collected and used. As will be discussed in Part VIII, privacy policies often assert that personal information is non-personal, that linkable information is anonymous, that reasonably linkable information is de-identified, that information including a resettable identifier is not trackable, that information including a device identifier is not identifiable, and that only information including a direct identifier is identifiable. More generally, consumers are rarely provided with notices that accurately explain whether personal information that is collected is anonymous, de-identified, trackable, or reasonably identifiable.

Clear definitions of each type of personal information can help. However, the corresponding information about the classification of each category of personal information collected and used should also be included in notices about collection and use. A consumer privacy law should thus require:

158. Jordan, *supra* note 3, at 13.

159. *Id.*

160. This language is modeled on the FCC's net neutrality transparency rule; *see* Protecting and Promoting the Open Internet, *Report and Order on Remand, Declaratory Ruling, and Order*, 30 FCC Rcd 5601, at para. 9 (2015).

> The privacy policy shall disclose the categories of personal information collected and used, and for each such category, the classification(s) of that category. The classifications shall consist of reasonably identifiable information, pseudonymous information, non-trackable information, de-identified information, and anonymous information.

2. Method and/or Source of the Collection of Personal Information

The method and/or source of personal information is also important, both to understand the information collected and to track personal information through the ecosystem.

Unfortunately, neither the GDPR nor the CCPA require a business that collects personal information directly from a consumer disclose the *methods* by which it collects this personal information.[161] 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.[162] 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.

In contrast to their lack of requirements about disclosure of *methods*, both the GDPR and the CCPA do include some requirements about disclosure of *sources*. Under the GDPR, if a controller collects personal data from an intermediary, then the controller must disclose "from which source the personal data originate, and if applicable, whether it came from publicly accessible sources."[163] In contrast, the CCPA only requires that disclose, in its privacy policy, "[t]he categories of sources from which the personal information is collected."[164]

Notice of only the categories of sources does not permit a consumer to identify and act upon the entity that originally collected and shared the consumer's personal information. There is no reason for lack of disclosure of sources that outweighs a consumer's right to follow the flow of their personal information through the ecosystem and to act upon this information.

It is unclear whether the GDPR requires a controller to disclose, *for each category* of personal data collected, the source of that category of personal data. Separate disconnected disclosures of categories and of sources are insufficient. For example, consider a business that discloses that it collects both your address and your browsing history, and that separately discloses

---

161. Jordan, *supra* note 3, at 18.

162. *See, e.g.*, AT&T, *supra* note 153 (under "Web browsing and app information").

163. GDPR, *supra* note 1, at art. 14(2)(d). However, if multiple sources have been used, the GDPR allows for the disclosure only of general information; see GDPR, recital 61.

164. CAL. CIV. CODE § 1798.110(c)(2) (Deering, LEXIS through Ch. 11 of 2022 Reg. Sess.).

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. A consumer privacy law should thus require:

> The privacy policy shall disclose, for each category of personal information collected: (a) the method of collection (if the personal information is collected by or on behalf of the controller) and (b) the sources of collection (if the personal information is shared with the controller by another entity).

3. Use of Personal Information

The GDPR requires that notices include "the purposes of the processing for which the personal data are intended."[165] The CCPA similarly requires a business to disclose "the purposes for which the categories of personal information are collected or used."[166]

However, it is unclear whether the GDPR or the CCPA requires a business to separately disclose, *for each category* of personal information collected, the purpose for collecting that category of personal information. Separate disconnected disclosures of categories and of purposes are insufficient. For example, consider a business that discloses that it collects the IP addresses of the websites you visit,[167] and that separately discloses that it collects personal information both to route your Internet traffic to the intended destination and for advertising.[168] 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).[169]

A consumer must be able to understand the purpose for the collection of each category of personal information in order to meaningfully exercise the consumer's right to consent. A consumer privacy law should thus require:

---

165. GDPR, *supra* note 1, at arts. 13(1)(c), 14(1)(c).

166. CAL. CIV. CODE §§ 1798.100(a)(1), .110(c)(3).

167. *See, e.g.*, *Our Privacy Policy Explained*, XFINITY, https://www.xfinity.com/privacy/policy (last updated Oct. 12, 2021) (under "The Personal Information We Collect and How We Collect It") (Comcast collects "Domain Name Server … searches and network traffic activity") [https://perma.cc/2ASV-UYJS].

168. *See, e.g.*, *id.* (under "Collection and Use of Personal Information," then under "Learn more about your rights if you are a California resident and how to exercise them") (Comcast uses "[i]nferences drawn from other personal information" consisting of a "[p]rofile reflecting a person's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes" to "provide marketing and advertising").

169. *See, e.g.*, *id.* (under "How and When We Use Information, Including for Marketing and Advertising") (Comcast asserts that "[w]here you go in the Internet is your business, not ours" and that Comcast has "never used [DNS] data for any sort of marketing or advertising").

> The privacy policy shall disclose, for each category of personal information collected or used, the purposes for which the category of personal information is collected or used.

In the proposed choice framework in Part V, user choice should be based in part on whether the personal information is collected for functional or for non-functional use.[170] In particular, non-functional use of reasonably identifiable information or of sensitive pseudonymous information should not be mandated in terms and conditions of a service. In order to exercise this choice, a consumer must be able to understand whether the use of a category of personal information will result in added functionality of the service or whether it will only result in non-functional uses such as advertising. A consumer privacy law should thus require:

> The privacy policy shall disclose, for each category of personal information collected or used and each such purpose, whether the use constitutes functional use, and if so, the functionality enabled by the collection and use of that category of personal information.

C. Contents of Notices About Sharing

Finally, this section turns to notices about sharing.

1. Categories of Personal Information Shared

The CCPA 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."[171] It also requires 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."[172] Surprisingly, it is unclear whether the GDPR has a similar requirement that a controller disclose the categories of personal data disclosed to third parties.

Regarding the level of detail or granularity of these categories, as with disclosure of collection and use, the CCPA requires that they "use the specific terms set forth" in the definitions of personal information and sensitive personal information.[173] However, disclosure of categories of personal information is insufficient to provide consumers with the information necessary to understand the degree of identifiability of the personal information shared. For example, some businesses appear to share the

170. A statutory definition of *functional use* was proposed in Part V.B.

171. CAL. CIV. CODE § 1798.130(a)(5)(C)(i) (Deering, LEXIS through Ch. 11 of 2022 Reg. Sess.).

172. *Id.* § 1798.130(a)(5)(C)(ii).

173. *Id.* § 1798.130(c).

combination of an advertising identifier and audience segments,[174] which might be classified as *pseudonymous information* if there are the corresponding legal controls in place. In contrast, other businesses appear to share the combination of an IP address and fine-grained user interests,[175] which are likely to be classified as *reasonably identifiable information*. For this reason, disclosure of the categories of personal information should be accompanied by the classification of each category:

> The privacy policy shall disclose the categories of personal information shared, and for each such category, the classification(s) of that category. The classifications shall consist of reasonably identifiable information, pseudonymous information, non-trackable information, de-identified information, and anonymous information.

2. Recipients of Personal Information

The GDPR requires controllers to disclose "the recipients or categories of recipients" to whom the personal data have been or will be disclosed. Somewhat similarly, the CCPA requires that privacy policies include the "categories of third parties to whom the business discloses consumers' personal information."[176] There are two issues here worth consideration: the granularity of the disclosure and the scope of the recipients that must be disclosed.

Regarding granularity, 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."[177] However, CCPA regulations also interpret the CCPA as also requiring the disclosure in privacy policies of the "third parties to whom [each category of personal information] was . . . sold."[178]

It is well known that personal information is widely shared amongst a large number of businesses that comprise an advertising and tracking ecosystem. One of the most fundamental issues in privacy regulation is how

---

174. *See, e.g.*, *Privacy Policy*, PINTEREST, https://policy.pinterest.com/en/privacy-policy (last updated July 1, 2021) (under "What we do with the info we collect") ("if you show an interest in camping tents on Pinterest, we may show you ads for other outdoor products") [https://perma.cc/K95L-W3QQ].

175. *See, e.g.*, *Data Policy*, FACEBOOK, https://www.facebook.com/policy.php (last updated Jan. 4, 2022) (under "Apps, websites, and third-party integrations on or using our Products") ("when you … use a Facebook Comment or Share button on a website, … the website … can receive a comment or link that you share from the website on Facebook") [https://perma.cc/S8SZ-7UNE].

176. CAL. CIV. CODE § 1798.130(a)(5)(B)(iv).

177. CCPA Regulations, *supra* note 157, at § 999.301(e).

178. *Id.* § 999.308(c)(1)(g)(1-2).

to address this widespread sharing. 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. There is no reason for lack of disclosure of a list of recipients that outweighs a consumer's right to follow the flow of their personal information through the ecosystem and to act upon this information.

The second issue is the scope of the recipients that must be disclosed. The GDPR defines a *recipient* as "a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not."[179] It thus requires disclosure of sharing of personal data with processors. In contrast, the CCPA only requires disclosure of sharing of personal information with third parties, which excludes service providers and contractors.

There is a fundamental choice to be made here. One option is to require disclosure when sharing personal information with contractors; to not hold controllers responsible for disclosure of collection, use, and sharing by its contractors; and to require contractors to disclose their collection, use, and sharing of personal information. However, this option is burdensome on consumers, who must examine the privacy policies of both the controller and all of its contractors to understand what personal information is collected, how it is used, and with whom it is shared. A superior option is to hold controllers responsible for disclosure of collection, use, and sharing by its contractors. In this case, disclosure of sharing of personal information with contractors need not be required, and contractors need not be required to disclose their collection, use, and sharing of personal information. A consumer privacy law should thus require:

> The privacy policy shall disclose the third parties with which the controller shares personal information.

Notices about sharing of personal information are of limited use unless a consumer also understands why a business is sharing their personal information. The CCPA requires a business to disclose in its privacy policy "the business or commercial purpose for . . . selling personal information."[180] Similarly, 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.

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).

179. GDPR, *supra* note 1, at art. 4(9).
180. CCPA Regulations, *supra* note 157, at § 999.308(c)(1)(f).

These two possibilities have very different consequences. For this reason, privacy policies should disclose the purpose for sharing each category of personal information.

The terms, if any, on which personal information is shared is also important. The definitions of several types of personal information (*de-identified information*, *non-trackable information*, and *pseudonymous information*) proposed in Part VIII include commitments to contractually obligate any third parties to whom the controller discloses the information to implement a set of legal controls that ensure that the information does not become more identifiable. These contractual obligations should be disclosed in a privacy policy whenever a controller shares personal information. A consumer privacy law should thus require:

> For each such third party, the privacy policy shall disclose the categories of personal information shared with that third party, the purposes for which the controller shares each category of personal information with that third party, and any contractual limits on the third party's use and further sharing of that personal information.

Finally, on the Internet it is common that as part of a consumer's interaction with a first party, the first party not only shares the IP address of the consumer with a third party but also enables the third party to directly collect further information from the consumer. In this case, a consumer has a right to know that, in addition to the first party sharing the consumer's information, that the first party is also enabling third parties to collect further information. A consumer privacy law should thus require:

> If a controller enables any third parties to collect additional personal information, the controller's privacy policy shall disclose the third parties so enabled and any contractual limits on such collection.

VIII. STATUTORY TEXT

Part VII presented proposed statutory text regarding notice. In this section, statutory text is developed to implement the choice framework proposed in Part V, as well as the supporting definitions.

A. Defining Personal Information and Reasonably Linkable Information

Notice and choice requirements typically apply only to information that is both personal and private. Privacy laws often call this type of information *personally identifiable information*, *personal information*, or *personal data*.

Many privacy policies lack any definition whatsoever of personally identifiable information. For example, Microsoft uses the term personal data,

but does not define it.[181] Pinterest uses the term personal information, but does not define it.[182] Twitter interchangeably uses the terms personal information and personal data, but does not define either of them.[183] By omitting a definition of personally identifiable information, the scope of such privacy policies is unknown, and consumers may be left wondering what personally identifiable information is collected that the privacy policy fails to disclose.

The GDPR defines *personal data* as "any information relating to an identified or identifiable natural person."[184]

The CCPA 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."[185]

In these definitions, both the GDPR and the CCPA combine the concept of personal information (e.g., information relating to a person) with the concept of identifiability (e.g., an identified or identifiable person). However, by combining these two concepts into a single definition, both the GDPR and the CCPA fail to address information that is personal but whose degree of identifiability falls short of relating to an "identifiable natural person."

Because of this conflation of personal and identifiable, the CCPA then goes back and separately defines other types of information—including *publicly available* information, *aggregate consumer information*, and *de-identified information*—and proceeds to exclude each of these from personal information.[186] In addition, the CCPA defines *pseudonymization*, but fails to address the relationship of pseudonymized information to personal information or to de-identified information.[187]

The GDPR exhibits similar problems, but to a worse degree. The GDPR uses the terms *aggregate data* and *anonymous information*, both of which it excludes from personal data.[188] In contrast to the CCPA, which excludes publicly available information from personal information, the GDPR uses (but not define) the term *public sector information*, which it appears to include in personal data.[189] Finally, the GDPR defines the term *pseudonymisation*, and treats pseudonymized data as a subset of personal data, but it fails to apply any different notice and choice requirements to pseudonymized data than to other personal data.[190]

Because of these problems, the next three subsections separately address personal information (i.e., information relating to a person), private

---

181. *Microsoft Privacy Statement*, MICROSOFT, https://privacy.microsoft.com/en-us/privacystatement (last updated Dec. 2021) [https://perma.cc/3XYR-LQM8].

182. PINTEREST, *supra* note 174.

183. *Twitter Privacy Policy*, TWITTER, https://www.twitter.com/en/privacy (last updated Aug. 19, 2021) [https://perma.cc/B29R-CWT4].

184. GDPR, *supra* note 1, at art. 4(1).

185. CAL. CIV. CODE § 1798.140(v)(1) (Deering, LEXIS through Ch. 11 of 2022 Reg. Sess.).

186. *Id.* § 1798.140(v).

187. *Id.* § 1798.140(aa).

188. GDPR, *supra* note 1, at recitals 26, 162.

189. *Id.* recital 154.

190. *Id.* recital 26.

information (i.e., information that is not public), and identifiable information (i.e., information relating to an identifiable person).

1. Is the Information Personal?

A consumer privacy bill is concerned with the privacy of people, not the privacy of organizations or businesses.

The GDPR limits personal data to "information relating to . . . [a] natural person."[191] The EU clarifies that a "natural person" means an individual, not a business, institution, or other entity.[192] 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."[193] As examples, the GDPR lists a "natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements."[194]

The CCPA's list of terms used in its definition of personal information similarly includes "information that . . . relates to [or] describes . . . a particular consumer."[195] It is unclear whether the CCPA's addition of the word "describes" broadens its definition, since it is unclear whether there is any information that "describes," but does not "relate to," a particular consumer.

A consumer privacy law should define personal information and should require that privacy policies adhere to this definition. Today, privacy policies often deny that much information relating to a person is actually personal. For example, Apple uses the term non-personal information to refer to "data in a form that does not, on its own, permit direct association with any specific individual."[196] Examples of non-personal information Apple collects and uses include occupation, location, and search queries.[197] However, the information is certainly personal, given that occupation, location, and search queries relate to a person.

Personal information should include, at a minimum, information which relates to an individual. However, there remains an important policy decision: should personal information also include information which relates to a household? Some identifiers used by services and apps to associate information identify a group of persons rather than a single person. Often, the group of persons constitutes a household. For example, a home postal address

191. *Id.* at art. 4(1).

192. EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS & COUNCIL OF EUROPE, HANDBOOK ON EUROPEAN DATA PROTECTION LAW 83-86 (2018) [hereinafter EU HANDBOOK].

193. *Id.* at 83, 86.

194. GDPR, *supra* note 1, at art. 4(4).

195. CAL. CIV. CODE § 1798.140(v)(1) (Deering, LEXIS through Ch. 11 of 2022 Reg. Sess.).

196. *Privacy Policy*, APPLE, https://web.archive.org/web/20200101005603/https:/www.apple.com/legal/privacy/en-ww/ (last updated Dec. 31, 2019) (under "Collection and Use of Non-Personal Information").

197. *Id.* (under "Collection and Use of Non-Personal Information").

or home telephone number may be associated with a household rather than with a single person.

However, privacy policies are often unclear about whether they consider information relating to a household to be included in the scope of personal information. Indeed, providers of services and apps often argue that they are not. For example, the California Chamber of Commerce, representing a wide variety of businesses, argued that information associated with households should be excluded from the CCPA's scope of personal information.[198]

The ambiguity of whether information relating to household is included in privacy policy disclosures demonstrates the importance of clearly spelling out in a privacy law the role of information associated with a group of people such as a household, and the rights of individuals within such a group.

The GDPR seems to include information relating to households in its scope of personal data, since it states that the regulation "applies to controllers or processors which provide the means for processing personal data for such personal or household activities."[199] However, this should have been made clear.

The CCPA is more explicit. In its definition of personal information, it includes information that relates to either a consumer or a household.[200] A household is defined as a group of consumers who reside at the same address and share a common device or service. The CCPA exempts businesses from certain specified obligations insofar as they concern household data, but it is unclear whether these exemptions include notice and choice obligations.[201]

A consumer privacy law should be explicit that information relating to a household qualifies as personal information. First, information relating to a household is clearly information relating to one or more natural persons in the household. Second, a household identifier has traditionally been treated as identification of a natural person, even if it is not sufficient to pin down which person within the household. For example, a home postal address and a home phone number are both always considered to be personal identifiers. For this reason, personal information should include information which relates to either an individual or a household.[202]

198. Letter from Tim Day & Harold Kim, Senior Vice President, Chamber Technology Engagement Ctr. & Chief Operating Officer, U.S. Chamber Inst. for Legal Reform, California Chamber of Com., to California Attorney Gen. Xavier Becerra, 4 (Mar. 8, 2019) (on file with California Chamber of Com.), https://www.uschamber.com/assets/documents/ca_ag_privacy_comments.pdf [https://perma.cc/G9JX-CJNR].

199. GDPR, *supra* note 1, at recital 18.

200. CAL. CIV. CODE § 1798.140(v)(1).

201. *Id.* § 1798.145(p).

202. However, there are peculiarities with other user rights, such as the right to inspect, when they concern household information.

2. Is the Information Private?

A consumer privacy bill should be concerned with the use of private information, not with the use of publicly available information.

The CCPA excludes from the scope of personal information any information that is publicly available. It defines *publicly available* information to include information in government records, information about a consumer that a consumer him or herself 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."[203]

The GDPR does not provide any similar exclusion from personal data for any type of publicly available information. It recognizes the existence of *public sector information*, which it does not define, but which appears by reference to consist of personal data that is held by a State, regional or local authority, by a body governed by public law, or by associations of such bodies.[204] Thus, unlike the CCPA, such public sector information remains a subset of personal data. The GDPR places the same notice requirements on public sector information as on other personal data, but it exempts public sector information from GDPR's choice requirements if public access to this information is provided for by EU or State law.[205]

The GDPR and the CCPA thus disagree on their approach to publicly available information. An intermediate approach would be in the public interest. As provided in the CCPA, information that a consumer has made publicly available should not be subject to notice and choice requirements, since the consumer has already decided to waive control over this information. However, CCPA's exemption goes beyond this. It also classifies information that a consumer has disclosed to a third party as *publicly available* if the consumer failed to restrict the third party's sharing of that information to a specific audience. This creates a chicken-and-egg situation. A consumer may wish to restrict sharing of personal information, but might not be accorded such a choice unless given this right by a privacy law. For this reason, the definition of *publicly available information* should not include such information.

In addition, even with respect to information in government records that are publicly available, the GDPR applies notice requirements, while the CCPA does not. While a consumer may benefit from transparency about a business's use of such publicly available information, applying notice requirements to information that is already publicly available goes beyond the mandate of a consumer privacy law that should be focused on private information.

Personal information should thus be defined as:

---

203. CAL. CIV. CODE § 1798.140(v)(2).
204. GDPR, *supra* note 1, at recital 154.
205. *Id.* at art. 86.

> The term "personal information" means any information relating to a natural person or to a household, excluding publicly available information.
> The term "publicly available information" means information relating to a natural person or to a household (a) in publicly available government records, (b) that the person or household to whom the personal information is related has made publicly available, or (c) that was made publicly available by widely distributed media.

Personal information is thus personal and private.

3. Is the Information Reasonably Linkable?

Having defined *personal information* as information that is both personal and private, this section now turns to the issue of whether it is identifiable information (i.e., information relating to an identifiable person).

There are several methods by which a person may be identifiable. The most obvious method is the use of person's name. The GDPR specifies that a natural person may be identified "by reference to an identifier such as a name . . . ."[206] The CCPA similarly specifies that a particular consumer may be identified using "a real name."[207] Other identifiers can also be used to reasonably establish a person's identity. For example, the CCPA specifies that a particular consumer may be identified using "a real name, . . . postal address, . . . email address, . . . social security number, driver's license number, [and a] passport number."[208] Thus, under both the GDPR and the CCPA, it is clear that a natural person may be identifiable through, at a minimum, a person's name, personal telephone number, personal email address, and government issued individual identifiers (e.g., driver's license number, social security number, or passport number).

Many privacy policies limit the scope of personally identifiable information to an identifier that itself identifies a person. For example, Apple defines personal information as "data that can be used to identify or contact a single person."[209] Cox defines personally identifiable information as "subscriber name, service and mailing addresses, telephone numbers, social security number, driver's license number, email address, billing and payment records (including credit card and bank account numbers used to pay for our services), subscriber credit information, or other information that potentially could be used to identify, contact, or locate you."[210] Chase uses the term

206. *Id.* at art. 4(1).
207. CAL. CIV. CODE § 1798.140(v)(1).
208. *Id.*
209. APPLE, *supra* note 196 (under "Collection and Use of Non-Personal Information").
210. *Your Privacy Rights as a Cox Customer and Related Information*, COX https://www.cox.com/aboutus/policies/annual-privacy-notice.html (last updated Jan. 1, 2022) (under "Your Information") [https://perma.cc/QM8X-NS4F].

personal information to describe contact information but excludes "usage and other information."[211]

However, often it is not the identifier itself that is personal. It is the information *associated* with an identifier that is personal. For example, a person may have a public telephone number listing, and hence that person's name and telephone number are public. However, a person's name and telephone number are often associated with information about that person's Internet browsing history, and it is the browsing history that is personal. By omitting information associated with an identifier from the scope of personally identifiable information, consumers may be left wondering what personally identifiable information is collected that the privacy policy fails to disclose.

Other privacy policies limit the scope of personally identifiable information to an identifier that itself identifies a person and to information that the provider of that service or app links to that identifier. For example, Google defines personal information as "information that you provide to us which personally identifies you, such as your name, email address, or billing information, or other data that can be reasonably linked to such information by Google, such as information we associate with your Google Account."[212]

However, limiting the scope of reasonably linkable information to an identifier that itself identifies a person and to information that the provider of that service or app links to that identifier is severely underinclusive in two separate ways. Identifiers are often used that uniquely identify a person, but not by name, telephone number, or email address. For example, Google and Facebook assign their own identifiers to each person they profile. Such identifiers are then associated with personal information such as browsing history or social network posts. Cox considers contact information to be personally identifiable information, but considers "general location, demographics, . . . usage, . . . and preferences" to be non-personally identifiable information unless it is directly linked to personally identifiable information.[213] Such definitions open up the possibility that these providers consider browsing history, social network posts, or usage information to be *excluded* from the scope of personally identifiable information, if not paired with an identifier that itself identifies a person, and thus not subject to disclosure requirements.

Although such privacy policies often then proceed to list categories of information that the service or app collects that do not fall into the severely limited scope of personally identifiable information as the provider defines it, the exclusion of information related to a person undermines the credibility that the privacy policy's disclosures are comprehensive.

In contrast, some privacy policies use definitions of personally identifiable information that either match or borrow language from those in

211. *Online Privacy Policy*, JPMORGAN CHASE & CO., https://www.chase.com/digital/resources/privacy-security/privacy/online-privacy-policy (last updated Dec. 10, 2020) (under "Information we collect") [https://perma.cc/5M6S-7NLF].

212. GOOGLE, *supra* note 152 (under "We want you to understand the types of information we collect as you use our services" in the pop-up window for "personal information").

213. COX, *supra* note 210 (under "Your Information").

the GDPR or the CCPA. AT&T uses the CCPA's definition of *personal information.*[214] Comcast defines personal information as "any information that is linked or reasonably linkable to you or your household,"[215] which includes part of (but not the full) CCPA definition. Comcast states that personal information "can include information that does not personally identify you—such as device numbers, IP addresses, and account numbers" and "may also include information that does personally identify you, such as your name, address, and telephone number."[216]

Finally, some privacy policies use different terms and definitions depending on the privacy law that applies in the person's location. In its nationwide privacy policy, Facebook avoids use of the term personal information, but characterizes "information that personally identifies you" as "information such as your name or email address that by itself can be used to contact you or identifies who you are."[217] In contrast, in its California privacy policy, Facebook uses the term personal information, and adopts a definition similar to (but not exactly the same as) the CCPA's definition.[218]

Both the GDPR and the CCPA also recognize that personal information may be used to establish a person's identity, even if the information lacks an identifier that itself establishes that identity. 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."[219] 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."[220] Thus, data records that contain no personal identifiers still relate to an identifiable natural person, 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.[221]

The CCPA takes a similar approach to the use of personal information to establish identity, albeit with different language. The CCPA's definition of *personal information* implies that a particular consumer may be identified using information that "is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer."[222] The phrase "could reasonably be linked, directly or indirectly, with" is similar to that used often used by the Federal Trade Commission.

---

214. AT&T, *supra* note 153 (under "When this Policy applies").

215. XFINITY, *supra* note 167 (under "Introduction" in the popup window for *personal information*).

216. *Id.* (under "The Personal Information We Collect and How We Collect It").

217. FACEBOOK, *supra* note 175 (under "Advertisers").

218. Facebook, *California Privacy Notice*, https://www.facebook.com/legal/policy/ccpa (last updated July 1, 2021), [https://perma.cc/9RP2-CZRY].

219. GDPR, *supra* note 1, at art. 4(1).

220. EU HANDBOOK, *supra* note 192, at 89 (quoting an opinion issued by the Article 29 Data Protection Working Party).

221. GDPR, *supra* note 1, at recital 26.

222. CAL. CIV. CODE § 1798.140(v)(1) (Deering, LEXIS through Ch. 11 of 2022 Reg. Sess.).

The concept of reasonable linkability is more familiar in the United States, and thus serves as a good starting point. However, the CCPA does not define the term.

Garfinkel defines *linkable information* as "information about or related to an individual for which there is a possibility of logical association with other information about the individual."[223] Adding a reasonableness test and leveraging the definition of *personal information* results in:

> The term "reasonably linkable information" means personal information for which there is a reasonable possibility of logical association with other information relating to the person or household to whom the personal information relates.

Reasonably linkable information is thus personal, private, and reasonably identifiable.

B. Defining Reasonably Identifiable Information, Pseudonymous Information, and Non-Trackable Information

The choice framework proposed in Part V differentiates between the use and sharing of three different types of reasonably linkable information. This subsection crafts definitions of each.

1. Is the Information Trackable?

The most privacy preserving form of reasonably linkable information is *non-trackable information*. Tracking is made possible by associating pieces of personal information with each other, even if they are not associated with a person by name.

Part III.B discussed information relating to a person or household that is identifiable but has not yet been identified, and that is *not* tracked over time. Such personal information typically involves the use of non-persistent identifiers such as randomized one-time identifiers. Polonetsky states that, in such personal information, direct identifiers have been removed or transformed so that they cannot link back to any individual, but indirect identifiers may remain intact if they have "no life outside of the specific context in which it was used."[224]

Consumer privacy laws increasingly are concerned with whether personal information can be used to track a person and create a profile, even if the person's name is not associated with the profile. The CCPA defines *profiling* as "any form of automated processing of personal information . . . to evaluate certain personal aspects relating to a natural person and in particular to analyze or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences,

223. GARFINKEL, *supra* note 97, at 42.
224. Polonetsky, et al., *supra* note 95, at 615.

interests, reliability, behavior, location, or movements."[225] The CCPA distinguishes between profiling versus "[s]hort-term, transient use" of personal information.[226] For example, if a consumer opts-out of sharing of personal information, the CCPA prohibits a business from profiling that consumer, but allows the business to use the consumer's personal information for non-personalized advertising shown as part of the consumer's current interaction with the business.[227] The GDPR also extensively discusses profiling. It requires that privacy notices specifically include disclosure of profiling,[228] and it gives consumers a right to opt-out of profiling used for direct marketing purposes.[229]

However, neither the GDPR nor the CCPA defines trackable information as an explicit subset of personal information. Instead, they consider profiling as a particular use of personal information. As a result, while they include specific provisions related to profiling, neither require disclosure of whether personal information is stored and use in a trackable form, and neither incorporate tracking directly into their choice framework.

A spirited debate has occurred about whether personal information is trackable when non-persistent identifiers are used. Many identifiers used by service and apps to associate information relating to a person are resettable. Common examples of resettable identifiers include dynamic IP addresses, advertising identifiers that can be reset using mobile device settings, and cookies that can be cleared using browser settings.

Most privacy policies are unclear about whether they consider resettable identifiers and information associated with them to be included in the scope of personally identifiable information. Indeed, providers of services and apps often argue that they are not. Apple argued that information "identified by non-personally identifiable identifiers such as those that are random, resettable, or rotating" should *not* be included in the scope of *personal information* under the CCPA.[230] 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. The Network Advertising Initiative thus argued that resettable identifiers "do not in fact relate to any one unique consumer," and hence it

225. CAL. CIV. CODE § 1798.140(z). The GDPR has an identical definition, except that it uses the term *personal data* instead of *personal information*; *see* GDPR, *supra* note 1, at art. 4(4).

226. *Id.* § 1798.140(e)(4).

227. *Id.* §§ 1798.135(f), .140(e)(4).

228. GDPR, *supra* note 1, at arts. 13(2)(f), 14(2)(g).

229. *Id.* at art. 21(2).

230. E-mail from Katie Kennedy, Priv. & Info. Sec. Counsel, Apple, Inc. to California Dep't of Just. Priv. Reguls. at 4, (Mar. 8, 2019, 3:10 PM) (on file with California Office of the Attorney Gen.), https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-public-comments.pdf.

proposed that probabilistic identifiers and information associated with them be *excluded* from the scope of *personal information*.[231]

The ambiguity of whether information relating to a person by reference to a resettable identifier is included in privacy policy disclosures demonstrates the importance of clearly spelling out in a consumer privacy law that resettable identifiers are a common method of tracking a person. The CCPA treats a resettable identifier, and the information associated with it, as *personal information* if it "can be used to recognize a consumer [or] a family . . . over time . . . ."[232] The CCPA further explicitly states that an IP address qualifies as *personal information* if it could be reasonably linked with a particular consumer or household.[233] The GDPR takes a slightly different tack, classifying a resettable identifier, and the information associated with it, as a *personal data* if and only if it can be reasonably used to identify an individual or household.[234] EU guidance states than an IP address is *personal data* if there is additional information reasonably available that identifies the person to whom the IP address has been assigned.[235]

Dynamic IP addresses are usually assigned by an Internet Service Provider to a house's modem for at least a day at a time, and they are usually renewed at the end of the IP address lease, so that a dynamic IP address is usually associated with a household for weeks or months at a time. Advertising identifiers and cookies are usually very persistent. In most situations, they are only cleared when a user explicitly does so.[236]

Many consumers have a higher sensitivity when their personal information is tracked over time than when it is used only in the current interaction with a business. However, whereas both the CCPA and the GDPR consider profiling to be a particular use of personal information, it is a cleaner approach to define a particular category of personal information that allows tracking to take place. The advantage of this approach is that *trackable information* takes it rightful place on the spectrum of identifiability, rather than being called out as a particular use of personal information. This helps guide an assignment of notice and consent obligations onto trackable information that is in the public interest and that is reasonable compared to the obligations placed onto other types of personal information.

Drawing on the CCPA's description of profiling as involving the linking of personal information from more than one interaction, and Polonetsky's description of it as involving the linking of personal information from more than one context, *non-trackable information* can be defined as:

---

231. Letter from David LeDuc, Vice President of Public Policy, The Networking Advert. Initiative, to California Attorney Gen. Xavier Becerra, 10 (Mar. 8, 2019) (on file with The Networking Advert. Initiative), https://thenai.org/wp-content/uploads/2021/07/naicommentletterccpaimplementingregulations.pdf [https://perma.cc/V9VY-XUP9].

232. CAL. CIV. CODE § 1798.140(aj) (Deering, LEXIS through Ch. 11 of 2022 Reg. Sess.).

233. *Id.* § 1798.140(v)(1).

234. GDPR, *supra* note 1, at recital 26.

235. EU HANDBOOK, *supra* note 192, at 91-92.

236. Less commonly, a user may have set a browser to automatically clear cookies upon exit.

> The term "non-trackable information" means reasonably linkable information for there is no reasonable possibility of logical association of the information with other information relating to the person or household obtained from another context or another interaction with the person or household.

The definition builds on the previous proposed definition of reasonably linkable information, but also requires that the logical association be not reasonably possible over time.

If reasonably linkable information fails to meet the definition of non-trackable information, then it remains trackable:

> The term "trackable information" means reasonably linkable information that is not non-trackable information.

2. Is the Information Reasonably Identifiable?

The second most privacy-preserving form of reasonably linkable information is *pseudonymous information*. Part III.A discussed information relating to a person or household that is identifiable but has not yet been identified, and that is tracked over time. Such personal information typically involves the use of persistent identifiers such as device identifiers or advertising identifiers that can be used to track a person or household over time.

Almost all online services and apps collect device identifiers. These device identifiers very often include IP addresses, see e.g., the privacy policies of Chase, Uber, and United.[237] Apps that run on mobile devices also often collect the IMEI identifiers of mobile devices, see e.g., the privacy policies of Google, Microsoft, and Apple.[238] Often, privacy policies state that they collect device identifiers, but fail to specify which ones, see e.g., the privacy policies of AT&T, Comcast, Facebook, Pinterest, and Twitter.[239]

Almost all online advertising-supported service and apps also collect advertising identifiers. Such advertising identifiers are usually associated with

---

237. JPMORGAN CHASE & CO., *supra* note 211 (under "Usage and Other Information" and "Chase Mobile"); *Uber Privacy Notice*, UBER TECHNOLOGIES INC., https://www.uber.com/legal/en/document/?name=privacy-notice&country=united-states&lang=en (last updated Dec. 22, 2021) (under III.A.2 "Device data") [https://perma.cc/LL9R-B9A5]; *Customer Data Privacy Policy*, UNITED AIRLINES INC., (last updated Mar. 12, 2021), https://www.united.com/ual/en/us/fly/privacy.html (under "Information we collect automatically" and "Information we collect through our mobile application(s)").

238. GOOGLE, *supra* note 152, at "Unique identifiers"; MICROSOFT, *supra* note 181, at "Personal data we collect"; Apple, *supra* note 196, at "What personal information we collect" and at "Cookies and Other Technologies."

239. AT&T, *supra* note 153 (under "The information we collect"); XFINITY, *supra* note 167 (under "The Personal Information We Collect and How We Collect It"); FACEBOOK, *supra* note 175 (under "Identifiers"); PINTEREST, *supra* note 174, under ("We also get technical information when you use Pinterest"); TWITTER, *supra* note 183 (under "You should read this policy in full, but here are a few key things we hope you take away from it" and then "Log Data").

a particular device, and thus serve as de-facto device identifiers. Most commonly, services and apps collect Apple and Android advertising identifiers, see e.g., the privacy policies of KAYAK, The Weather Channel, and Zillow.[240]

However, privacy policies differ in whether they include, in the scope of personally identifiable information, device identifiers and information that is associated with device identifiers. Many privacy policies limit the scope of personally identifiable information to an identifier that itself identifies a person, and perhaps to information that the provider of that service or app links to that identifier. Although such privacy policies almost always disclose that the service or app collects device identifiers, they do not typically discuss whether device identifiers are considered by the provider to qualify as a method of identification of a person. This leaves open the question of whether these privacy policies consider device identifiers, and information that is associated with device identifiers, to constitute personally identifiable information.

Indeed, providers of services and apps often argue that these device identifiers do *not* identify a person, and thus that information associated with device identifiers or advertising identifiers does *not* constitute personally identifiable information. Google argued that device identifiers are often *not* associated with a person's identity; and thus one should question whether Google's privacy policy considers information associated with a device identifier to constitute personally identifiable information.[241] The Internet & Television Association (NCTA), a trade association representing cable Internet Service Providers, argued that IP addresses *cannot* identify an individual on their own.[242] The Internet Advertising Bureau (IAB), a trade association representing Internet advertisers and ad brokers, argued that an "anonymous identifier" should *not* qualify as personally identifiable information.[243] The Network Advertising Initiative, a trade association representing Internet advertising companies, argued that IP addresses are not *personal information* under CCPA, unless a business "has linked it, or reasonably could link it, with additional pieces of information known by the

240. KAYAK, *supra* note 155 (under "Information We Collect and Use"); THE WEATHER CO., *supra* note 154 (under "1.B"); *Privacy Policy*, ZILLOW GRP., https://www.zillowgroup.com/zg-privacy-policy/ (last updated Jan. 29, 2021) (under "Device information") [https://perma.cc/3VNC-MSXN].

241. Comments of Google at 3, (Feb. 8, 2019) (on file with California Office of the Attorney Gen.) https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-public-comments.pdf ("where companies collect device-identifying information online and do not associate that information with a consumer's name, email address, or other identifying information").

242. Protecting the Privacy of Customers of Broadband and Other Telecomm. Servs., *Report and Order*, 31 FCC Rcd. 13911, para. 94 n.239 (2016) [hereinafter *FCC Order*].

243. *Id.*

business to identify a particular consumer or household, such as name or residential address."[244]

The ambiguity of whether information relating to a person by reference to a device identifier is included in privacy policy disclosures demonstrates the importance of clearly spelling out in a privacy law that device identifiers are a common method of linking information to a person. The GDPR classifies a device identifier, and any other information associated with it, as *personal data* if and only if it can be attributed to a natural person, including by the use of additional information.[245] So the question remains: can a device identifier be attributed to a person? EC guidance gives advertising identifiers as an example of *personal data* without limitation, but the question has likely not been definitively answered.[246] The CCPA is also less than clear on this issue. The original version of the CCPA explicitly included device identifiers in its definition of a *unique identifier*, which in turn implies that device identifiers are, without limitation, a form of identification of a person. However, the recently revised version of the CCPA may be interpreted to classify device identifiers and the information associated with it as *personal information* if and only if the device is "linked to" or "could be reasonably linked to" a consumer or family.[247]

The ability of a business to use a device identifier to establish the identity of a person depends on the nature of the device identifier and the availability of information that associates the device identifier with a natural person. Advertising identifiers are frequently shared by devices, and they are shared widely within the advertising ecosystem. There is additional reasonably available information that associates an advertising identifier with a natural person. It should be presumed that a person's identity can be reasonably established using an advertising identifier, and thus that the combination of an advertising identifier with other personal information constitutes *reasonably identifiable information*. It is possible that a device identifier is shared by a device only in a pseudonymous fashion, and that subsequent user actions do not render that identifier sufficient to identify a person. However, in general, any persistent identifier that is shared widely within the advertising ecosystem will render that identifier sufficient to identify a person, because eventually that information will be associated with a person's identity, e.g., when a person registers with a website or purchases an item.

---

244. E-mail from Leigh Freund, President & Chief Executive Officer, The Networking Advert. Initiative, to California Attorney Gen. Xavier Becerra, 4 (Feb. 25, 2020) (on file with The Networking Advert. Initiative), https://thenai.org/wp-content/uploads/2021/07/nai_comment_letter_-_ccpa_modified_proposed_regulations_february_25_2020-1.pdf [https://perma.cc/4KNC-ARWD].

245. GDPR, *supra* note 1, at recital 26.

246. *What is Personal Data?*, EUROPEAN COMM'N, https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_en [https://perma.cc/B9FF-ZY3A] (under "Examples of personal data").

247. CAL. CIV. CODE §§ 1798.140(x), .140(aj) (Deering, LEXIS through Ch. 11 of 2022 Reg. Sess.).

The GDPR does not distinguish between persistent and non-persistent indirect identifiers in its definition of *pseudonymisation*:

> [T]he processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.[248]

Thus, under the GDPR, the use of persistent indirect identifiers might result in pseudonymous personal data used for tracking, whereas the use of non-persistent indirect identifiers might result in pseudonymous personal data not used for tracking. The GDPR considers both types of information to be personal data.[249]

To avoid this confusing use of terminology, this proposal uses the term *non-trackable information* (as defined above) to describe the use of non-persistent indirect identifiers, and the term *pseudonymous information* to describe the use of persistent indirect identifiers. Drawing upon the GDPR's description of pseudonymous information as resulting in the inability to attribute the information to a specific person without the use of additional information, and adding a reasonableness test, *pseudonymous information* can be defined as:

> The term "pseudonymous information" means trackable information for which the related person or household is not reasonably identifiable using that personal information and other reasonably linkable information.

The definition builds on the previous proposed definition of *trackable information*, but also requires that the information cannot be associated with other reasonably linkable information such that the combined information can be used to reasonably identify the related person or household.

If *trackable information* fails to meet the definition of *pseudonymous information*, then it remains reasonably identifiable:

248. GDPR, *supra* note 1, at art. 4(5).
249. *Id.*

> The term "reasonably identifiable information" means trackable information that is not pseudonymous information.

C. Defining De-Identified Information and Anonymous Information

The GDPR defines *anonymous information*, but not *de-identified information*.[250] The CCPA defines *de-identified information*, but not *anonymous information*.[251] The two definitions are not the same. This subsection crafts definitions of both.

1. Is the Information Anonymous?

The GDPR defines *anonymous information* as "information which does not relate to an identified or identifiable natural person."[252]

This definition simply inverts the definition of *personal data*, and thus includes (a) information that is not personal and (b) information that is personal but whose degree of identifiability falls short of *personal data*. There are several problems with this definition. First, it needlessly includes information that does not relate to an individual or household, and thus conflates anonymous information with non-personal information. More critically, it fails to distinguish between anonymous information and de-identified information. The GDPR simply excludes both from *personal data*, and then exempts them from notice and choice requirements.

Polonetsky describes anonymous information as personal information in which both direct and indirect identifiers have been removed or transformed so that they cannot link back to any individual, and in which the method for removal or transformation includes mathematical and technical guarantees that are sufficient on their own to distort the data so as to prevent reidentification.[253] As an example of an anonymization technique that can provide such guarantees, Polonetsky mentions differential privacy algorithms, which can hide whether or not an individual is present in a dataset.

Privacy policies often overreach in their claims that personal information is anonymous. AT&T defines Anonymous Information as "[i]nformation that doesn't directly identify and can't reasonably be used to identify an individual customer or user."[254] Anonymous Information is thus defined by AT&T as all information that AT&T does not consider to be Personal Information, which it defines as "[i]nformation that directly identifies or reasonably can be used to figure out the identity of a customer or user, such as your name, address, phone number and e-mail address."[255] AT&T then explains that "[w]e treat identifiers like cookies, advertising

250. *Id.* at recital 26.
251. CAL. CIV. CODE § 1798.140(m).
252. GDPR, *supra* note 1, at recital 26.
253. Polonetsky et al., *supra* note 95, at 618.
254. AT&T, *supra* note 153 (under "Definitions").
255. *Id.*

identifiers, device identifiers, and household identifiers as Anonymous Information except in circumstances where they can be used to identify you." [256] However, the information is almost certainly personal, and is presumably private. If it includes an identifier such as an advertising identifier or device identifier, then it is also linkable, not de-identified, and trackable. Thus, it certainly does not qualify as *anonymous information.* Under the GDPR, it almost certainly would be categorized as *personal data*, and under the CCPA as *personal information*.

KAYAK defines Anonymized Information as "information that cannot be linked to you or any other specific user using any means available to us, either because it was collected anonymously or has been subsequently anonymized."[257] KAYAK states that "[i]nformation that is anonymous or has been anonymized is no longer considered 'personal information.'" [258] KAYAK appears to include in the scope of Anonymized Information, and thus exclude from the scope of Personal Information, information that it considers to be "de-identified usage data" that is associated with a mobile advertising identifier. [259] Indeed, KAYAK states that Anonymized Information "may be subsequently used for any purpose." [260] KAYAK's descriptions of Anonymized Information are inconsistent. If the information can truly not be linked to a person or household, including to a non-identifiable person or household, then it would qualify as *anonymous information*. However, if the information includes a mobile advertising identifier, then it neither qualifies as *anonymous information*, nor *de-identified information*, nor even as *non-trackable information*.

For its "eero" branded Wi-Fi products Amazon defines Anonymous Data as "data that, either in its original form or as the result of anonymization procedures that we perform on Personal Data, is not associated with or linked to your Personal Data."[261] Amazon asserts that "Anonymous Data does not, by itself, permit the identification of individual persons."[262] Amazon explains that, "[w]e may create Anonymous Data records from Personal Data by using various procedures to remove or obscure information (such as your name, email address, phone number or IP address) that makes the data personally identifiable to you," and then reserves the right to use and share Anonymous Data for any purposes, apparently without disclosure. [263] Amazon's description of Anonymous Data are too vague to allow classification. At best, Amazon's procedures to remove or obscure information may result in *anonymous information*, if the procedures include mathematical and technical guarantees that are sufficient on their own to prevent reidentification.

256. *Id.*
257. KAYAK, *supra* note 155 (under "How we use your information").
258. *Id.* (under "How we use your information").
259. *Id.* (under "Our Advertising Cookies").
260. *Id.* (under "How we use your information").
261. *Privacy for eero Devices, Applications and Services*, EERO https://eero.com/legal/privacy (last updated Feb. 28, 2020) (under "Types of data we collect") [https://perma.cc/3H7N-57YT].
262. *Id.* (under "Types of data we collect").
263. *Id.* (under "Use of your Personal Data").

However, Amazon's procedures to remove or obscure information may not have such guarantees, and may easily be *de-identified information, non-trackable information,* or *pseudonymous information*. Furthermore, given that Amazon only requires that Anonymous Data not "by itself" permit the identification of a person, it is possible that it is linkable to information that does permit the identification of a person, in which case the information is properly classified as *reasonably identifiable information*.

The ability, or lack thereof, to associate or link information to an individual or household features prominently in the distinction between anonymous information and other types of more identifiable personal information. Indeed, the CCPA's definition of *personal information* relies strongly on the concept: "information that . . . is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household."[264]

Following the guidance in Polonetsky that anonymous information includes mathematical and technical guarantees that are sufficient on their own to distort the data so as to prevent reidentification, this subsection focuses on the technical ability of associating information with a particular consumer or household; the following subsection considers whether the association can be reasonably made. Garfinkel (2015) defines linkable information as "information about or related to an individual for which there is a possibility of logical association with other information about the individual."[265]

This test can be adapted to the proposed definition of *personal information*:

> The term "anonymous information" means personal information for which there is no possibility of logical association with other information relating to the person or household to whom the personal information relates.

If *personal information* is not anonymous, it should be classified it as *linkable information*, defined as:

> The term "linkable information" means personal information that is not anonymous information.

Privacy laws sometimes also distinguish between anonymous information and aggregate information. Polonetsky considers aggregated anonymous information to be a subset of anonymous information. In aggregated anonymous information, the data are so highly aggregated that the aggregation itself serves as a mathematical and technical guarantee so as to prevent reidentification.[266]

---

264. CAL. CIV. CODE § 1798.140(v)(1) (Deering, LEXIS through Ch. 11 of 2022 Reg. Sess.).

265. GARFINKEL, *supra* note 97, at 42.

266. Polonetsky et al., *supra* note 95, at 618.

The CCPA defines *aggregate consumer 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," and then explains that it does not include "one or more individual consumer records that have been deidentified." [267] The CCPA then excludes *aggregate consumer information* from *personal information*. The GDPR similarly considers *aggregate data* to be a subset of *anonymous information*, and then excludes it from *personal data*.[268]

That said, there is no need to define in a consumer privacy law a category of aggregate information because it is typically afforded the same treatment as other types of *anonymous information*.

2. Is the Information De-Identified?

Polonetsky distinguishes de-identified information from anonymous information based on the difficulty of associating the information with the person to whom it is related. In order to qualify as either de-identified information or anonymous information, both direct and indirect identifiers must have been removed or transformed so that they cannot link back to any individual. Whereas for anonymous information the method for removal or transformation includes mathematical and technical guarantees that are sufficient on their own to distort the data so as to prevent reidentification, for de-identified information such mathematical and technical guarantees are absent and legal controls take the place of technological controls. As examples of de-identification techniques that remove both direct and indirect identifiers, but which cannot provide mathematical and technical guarantees, Polonetsky mentions suppression, generalization, perturbation, and swapping algorithms. Garfinkel provides an overview of these types of algorithms.[269]

Privacy policies often make overstated claims that personal information is de-identified. KAYAK classifies as "de-identified usage data" mobile advertising identifiers, "anonymous device identifiers," and cookies.[270] Such identifiers result in a reasonable possibility of logical association with other information relating to the person or household to whom the information relates, and thus it is not *de-identified information*. Furthermore, such identifiers are persistent, and thus the associated information is not *non-trackable information*.

The proposed definition of *anonymous information* already captures the subset of *personal information* in which reidentification is prevented solely using technological controls. If such technological controls are absent, the information remains classified as *linkable information*. It remains to delineate *linkable information* for which the logical association is possible but not

267. CAL. CIV. CODE § 1798.140(b).
268. GDPR, *supra* note 1, at recital 162.
269. GARFINKEL, *supra* note 97, at 20.
270. KAYAK, *supra* note 155 (under "Our Advertising Cookies").

reasonable given the current state of technology, the availability of information with which it can be associated, and legal controls.

The CCPA defines *de-identified information* as "information that cannot reasonably be used to infer information about, or otherwise be linked to, a particular consumer . . . ."[271]

The intent is to exempt from the CCPA's definition of *personal information* a category of information that can be logically associated with an individual or household, but for which the association cannot be reasonably made due to a combination of technological and legal controls.

The CCPA's definition can be adapted to build on the proposed definition of *linkable information*:

> The term "de-identified information" means linkable information for which there is no reasonable possibility of logical association with other information relating to the person or household to whom the linkable information relates.

This completes the set of definitions of different types of personal information. The logical flow used to classify them is illustrated in Figure 5.

271. CAL. CIV. CODE § 1798.140(m).

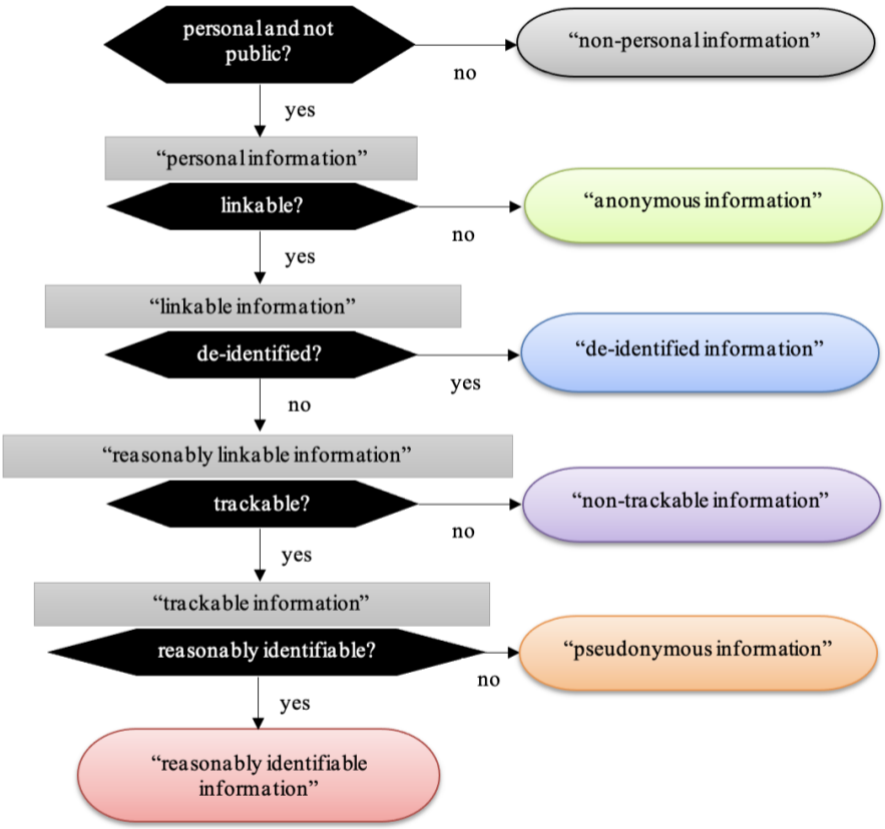

Figure 5. Classification of Information

D. Defining Sensitive Information and Functional Use

The choice framework proposed in Part V treats sensitive personal information differently than non-sensitive personal information, and it treats use for functional purposes differently than use for non-functional purposes. This subsection crafts definitions of these terms.

1. Sensitive Personal Information

The GDPR's category of sensitive personal data includes specific types of information relating to a person's physical characteristics: "genetic data, biometric data [processed] for the purpose of uniquely identifying a natural person, data concerning health" and "personal data revealing racial or ethnic origin."[272] 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."[273] The CCPA's definition of *sensitive personal information* similarly includes

272. GDPR, *supra* note 1, at art. 9(1).
273. *Id.*

genetic data, biometric information, health information, racial or ethnic origin, religious or philosophical beliefs, and sex life or sexual orientation.[274]

However, limiting the scope of sensitive information to these specific types is insufficient when personal information on the Internet is often not easily categorized. Personal information collected on the Internet often includes a list of websites that a consumer has visited, and it may include the content of communications. In 2016, the Federal Communications Commission (FCC) issued the Broadband Privacy Order, which focuses on consumer privacy for broadband Internet service.[275] Given this focus, the FCC Order is interesting for its guidance on which types of Internet related activity should be classified as sensitive. The Order classifies as sensitive "precise geo-location information," recognizing the prevalence of collection of personal information on mobile devices and the wealth of detail that location information can reveal.[276] The Order classifies as sensitive the "content of communications," citing the long legal history of protecting its privacy in different forms of communications.[277] The FCC Order also classifies as sensitive "web browsing history," 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, . . . a customer's financial status, familial status, race, religion, political leanings, age, and location.[278]

Finally, the FCC Order also classifies as sensitive "application usage history," explaining that:

274. CAL. CIV. CODE § 1798.140(ae).

275. *FCC Order*, *supra* note 242. The Order was repealed by the United States Congress in 2017. Joint Resolution, Pub. L. No. 115-22 (2017).

276. *Id.* at para. 179.

277. *Id.* at para. 180.

278. *Id.* at para. 183.

> [T]he 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.[279]

Precise geo-location information, the content of communications, web browsing history, and application usage history should all be classified as sensitive information. A definition that combines these types of information with the types given in the GDPR and the CCPA is:

> The term "sensitive," when used in conjunction with any type of personal information, means personal information that relates to sensitive characteristics of a person or household, including, but not limited to:
> (A) private personal identifiers, including social security number, driver's license number, state identification card number, and passport number;
> (B) private physical characteristics, including genetic data, biometric data, health data, and racial or ethnic origin; or
> (C) personal information about behavior or beliefs, including political opinions, religious or philosophical beliefs, union membership, sex life or sexual orientation, financial information, information pertaining to children, precise geo-location, content of communications, web browsing history, and application usage history.
> The term "non-sensitive," when used in conjunction with any type of personal information, means personal information that is not sensitive information.

2. Functional Use

The GDPR requires a lawful basis for processing of personal data.[280] One such lawful basis for the processing of non-sensitive personal data is a contract between the user and the controller, if the processing is necessary for the performance of the contract.[281] EU guidance explains that "what is 'necessary for the performance of a contract' is not simply an assessment of

279. *Id.* at para. 184.
280. GDPR, *supra* note 1, at art. 5(1).
281. *Id.* at art. 6(1)(b).

what is permitted by or written into the terms of a contract."[282] 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."[283] Personalization of content qualifies if it is "an intrinsic aspect" of the service."[284] However, processing of personal data for the purposes of improving a service is not considered necessary.[285] Neither is processing of personal data for the purposes of behavioral advertising.[286]

The CCPA limits the disclosure of personal information that may be mandated by terms and conditions of a service to those required for a *business purpose*, which it defines as the "use of personal information for a business's operational purposes . . . provided that the use of personal information shall be reasonably necessary and proportionate to achieve the purpose . . . ."[287] The use under this exception must be related to the functionality of the service. Behavioral advertising does not qualify.[288] But the CCPA then proceeds to give an exhaustive list of business purposes, including auditing, security, debugging, customer service, internal research, and non-personalized advertising.[289]

The GDPR's requirement that functional use be determined by a contract is unnecessarily limiting. Applications often offer elective functionality, e.g., a map can provide turn-by-turn directions if and only if the user allows it to access the user's location. Such elective functionality may not be written into any contract. The CCPA's requirement that functional use be limited to a specific list in the statute is also unnecessarily limiting. A better approach is to simply tie functional use to the functionality provided, and to exclude the use of personal information to subsidize a service:

> The term "functional use" means the technical use of personal information to provide functionality. Functional use does not include the use of personal information in exchange for consideration from a third party.

Any functional use of personal information under this definition should qualify under the GDPR as necessary for the performance of a contract if the functional use were incorporated into a contract between the user and the controller. However, this definition does not require a contract. Most of the uses of personal information that qualify under the CCPA as a business purpose would qualify as a functional use, including security, debugging, and

282. EUROPEAN DATA PROT. BD., 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 para. 23 (Oct. 8, 2019).

283. *Id.* at para. 30.

284. *Id.* at para. 57.

285. *Id.* at paras. 48-49.

286. *Id.* at paras. 51-56.

287. CAL. CIV. CODE § 1798.140(e) (Deering, LEXIS through Ch. 11 of 2022 Reg. Sess.).

288. *Id.* § 1798.140(e)(4).

289. *Id.* § 1798.140(e).

customer service. Internal research would not qualify as a functional use, despite its inclusion in the CCPA as a business purpose. Personalization features of an app, such as those discussed in Table 4 qualify as functional use, although they might not qualify under the CCPA as a business purpose.

E. Defining Processing and Choice

1. Collection, Use, and Sharing

The GDPR defines *processing* as:

> [A]ny 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.[290]

Processing thus includes collection, use, and sharing of personal data. Although some of the GDPR's requirements are specific to either collection, use, or sharing, the GDPR does not separately define these terms.

In contrast, the CCPA defines separate terms for collection and sharing, but not for use. It defines *collection* as "buying, renting, gathering, obtaining, receiving, or accessing any personal information pertaining to a consumer by any means."[291] It defines two types of sharing, both of which include "renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's personal information."[292] One type, called *selling*, involves the sale of personal information to another entity "for monetary or other valuable consideration."[293] The other type, called *sharing*, involves the sharing of personal information with another entity specifically for cross-context behavioral advertising, whether or not it involves monetary or other valuable consideration.[294] Both definitions exclude sharing of personal information for certain purposes, including consumer-directed disclosure.

It is helpful to distinguish between collection, use, and sharing when tailoring notice and consent requirements. Drawing from the terms defined in the GDPR and the CCPA, these terms could be defined as:

290. GDPR, *supra* note 1, at art. 4(2).
291. CAL. CIV. CODE § 1798.140(f).
292. *Id.* §§ 1798.140(ad), .140(ah).
293. *Id.* § 1798.140(ad).
294. *Id.* § 1798.140(ah).

> The term "collection" of personal information means access to personal information by any means, including but not limited to gathering, recording, storing, obtaining, receiving, buying, or renting.
> The term "use" of personal information means any operation or set of operations performed on personal information, including but not limited to organization, structuring, adaptation, alteration, retrieval, consultation, alignment, or combination of personal information.
> The term "sharing" of personal information means disclosure by any means, including but not limited to disclosure by transmission, dissemination, making available, releasing, transferring, renting, selling, or otherwise communicating, except that it excludes disclosure to a contractor.

This definition of *sharing* differs the CCPA's definitions of *selling* and *sharing*. First, there is no need to limit the term to disclosure for consideration, since even disclosure that does not involve consideration impacts privacy. Second, there is no need to specifically define disclosure for particular purposes (e.g., cross-context behavioral advertising) or to exclude sharing of personal information for certain purposes (e.g., consumer-directed disclosure). It is cleaner and more comprehensible to address the purposes for sharing of personal information when formulating notice and choice provisions. Part VIII.F discusses the role of contractors and the reason to exclude disclosure to a contractor.

2. Choice

The GDPR defines consent as "any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her."[295]

The CCPA includes a similar definition of consent.[296] EU guidance clarifies that the "freely given" requirement precludes "consent [that] is bundled up as a non-negotiable part of terms and conditions."[297] 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."[298] The GDPR's consent requirement is thus often described as opt-in consent. Incorporating the terms collection, use, and sharing results in:

295. GDPR, *supra* note 1, at art. 4(11).
296. CAL. CIV. CODE § 1798.140(h).
297. EUROPEAN DATA PROT. BD., *Guidelines 02/2020 on Consent Under Regulation 2016/679* 7 (May 4, 2020).
298. GDPR, *supra* note 1, at recital 32.

> The term "opt-in consent" to specified collection, use, and/or sharing of personal information means any freely given, specific, informed and unambiguous indication of the person's wishes, by a statement or by a clear affirmative action, by which the person signifies agreement to the specified collection, use, and/or sharing of personal information relating to that person.

The GDPR does not utilize the concept of an opt-out choice. The CCPA describes a user's right to opt-out of sharing or selling of personal information as "the right, at any time, to direct a business that sells or shares personal information about the consumer to third parties not to sell or share the consumer's personal information."[299]

Aligning this definition with that of *opt-in consent* gives:

> The term "opt-out choice" of specified collection, use, and/or sharing of personal information means a choice by which a person can withdraw consent to the specified collection, use, and/or sharing of personal information relating to that person.

F. Defining Various Entities

Notice and choice requirements are applied to certain types of entities that collect, use, and share personal information. A consumer privacy law must delineate the entities to which these requirements apply.

1. Controllers and Contractors

Consumer privacy laws often distinguish between entities that make decisions about the collection, use, and sharing of personal information versus entities that are hired to implement specific tasks involving the collection and use of personal information.

To describe entities that make decisions about the collection, use, and sharing of personal information, the GDPR first defines a *controller* as an entity that "alone or jointly with others, determines the purposes and means of the processing of personal data."[300]

The CCPA 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 the purposes and means of the processing of consumers' personal information."[301]

A comprehensive consumer privacy law may apply to a broader class of entities than businesses.[302] There is no need to limit the definition of a *controller* to entities that themselves collect personal information or that on

299. CAL. CIV. CODE § 1798.120(a).

300. GDPR, *supra* note 1, at art. 4(7).

301. CAL. CIV. CODE § 1798.140(d).

302. A privacy law must also determine whether notice and choice requirements apply to all controllers, only to for-profit controllers, or only to large for-profit controllers.

behalf of which personal information is collected. An entity that does not itself collect personal information or that on behalf of which personal information is collected, but which nevertheless determines the purposes and means of the processing of personal information, should still be treated as controller, since it remains the entity that controls the collection, use, and sharing of personal information. Incorporating the definitions of *collection*, *use*, and *sharing* into the GDPR's definition of *controller* results in:

> The term "controller" means an entity that alone or jointly with others determines the purposes and means of the collection, use, and/or sharing of personal information.

To describe entities that are hired to implement specific tasks involving the collection and use of personal information, the GDPR defines a *processor* as "a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller."[303]

The CCPA similarly defines a *service provider* as "a person that processes personal information on behalf of a business[,] and that receives from or on behalf of the business[,] a consumer's personal information . . . ."[304]

Both the GDPR and the CCPA intend that an entity should only qualify as a *processor* (resp. *service provider*) to the extent that its processing of personal information is limited to the specific tasks it was hired by a controller to do. The GDPR limits a processor's handling of personal data to that which is "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."[305]

The CCPA limits a service provider's handling of personal information to that

303. GDPR, *supra* note 1, at art. 4(8).

304. CAL. CIV. CODE § 1798.140(ag)(1). The CCPA also defines a related term, *contractor*; *see* CAL. CIV. CODE § 1798.140(j)(1).

305. GDPR, *supra* note 1, at art. 28(3).

> [F]or a business purpose pursuant to a written contract [that] prohibits the [service provider] from: (A) [s]elling or sharing the personal information; (B) [r]etaining, using, or disclosing the personal information for any purpose other than for the business purposes specified in the contract …; (C) [r]etaining, using, or disclosing the [personal] information outside of the direct business relationship between the service provider and the business; [and] (D) [c]ombining the personal information that the service provider receives from, or on behalf of, the business with personal information that it receives from, or on behalf of, another person or persons, or collects from its own interaction with the consumer . . . .[306]

It is thus intended that an entity that processes personal information, and that doesn't qualify as a *processor* (resp. *service provider*) with respect to that processing, should be classified as a *controller* (resp. *business*). Both the GDPR and the CCPA rely on the phrase "on behalf of" to convey this meaning. However, it would be better if the definition tied back into the phrase "determines the purposes and means" used in the definition of *controller* in order to make it clear that an entity that processes personal information cannot escape being designated as either a *controller* or a *processor*.

Neither the term *processor* nor *service provider* convey the intent of this distinction. Instead, this proposal uses the term *contractor*:

> The term "contractor" means an entity that collects, uses, and/or shares personal information but does not alone or jointly with others determine the purposes and means of the collection, use, and/or sharing of personal information. An entity does not alone or jointly with others determine the purposes and means of the collection, use, and/or sharing of personal information if and only if it collects, uses, and/or shares personal information solely pursuant to a written contract that prohibits the entity from collecting, using, and/or sharing personal information for any purposes or using any means other than that specified by the controller(s) of that personal information.[307]

Similar to the CCPA's definition of service provider (but unlike the GDPR's definition of processor), this definition directly incorporates the requirement for the contract. However, this definition of contractor differs from the CCPA's definition of service provider. The CCPA limits the purposes for the processing of personal information by a service provider to a specified list of business purposes, including auditing, security, debugging,

306. CAL. CIV. CODE § 1798.140(ag)(1). *See also* CAL. CIV. CODE § 1798.140(j)(1) for a similar provision regarding contractors.

307. This article's use of the term *contractor* is not exactly the same as the CCPA's use of the term *contractor*.

customer service, internal research, and non-personalized advertising.[308] There is no need to limit a contractor's activities to a defined list. Instead, notice and choice requirements should differentiate between functional and non-functional activities. This distinction is addressed below.

2. First and Third Parties

Consumer privacy laws often distinguish between first parties and third parties. The first party is the party with whom a consumer intentionally interacts. The CCPA defines a *third party* as "a person who is not . . . [t]he business with whom the consumer intentionally interacts . . . [a] service provider to the business; or [a] contractor."[309] It is cleaner to first define a *first party*:

> The term "first party" means an entity with whom a consumer intentionally interacts.

Third parties are usually considered to include all other parties that process personal information. However, under the GDPR, a controller is responsible for the activities of its processors, and thus the controller remains the first party with respect to the actions of its processors.[310] Similarly, under the CCPA, a business is responsible for the activities of its service providers and contractors, and thus the business remains the first party with respect to the actions of its service providers and contractors. C*ontractors* should thus be excluded from the definition of a *third party*:

> The term "third party" means any entity other than a first party or a first party's contractors.

First parties are often controllers that collect and use personal information. First parties may also share personal information with a third party, who then becomes a controller by virtue of having collected personal information from the first party.

On the Internet, it is common that, as part of a consumer's interaction with a first party, the first party not only shares the IP address of the consumer with a third party but also enables the third party to directly collect further information from the consumer. For example, the first party may be a website, and the third party may be an advertiser on that website. Some advertisements are displayed using software that has the ability to collect further information. Although the ensuing interaction between the third party and the consumer is direct, the consumer is typically unaware of the third party's further collection of personal information.

---

308. *See* CAL. CIV. CODE § 1798.140(e).

309. *Id.* § 1798.140(ai).

310. *See* GDPR, *supra* note 1, at art. 4(7)-(8). The GDPR defines *third party* somewhat similarly, but it uses the term exclusively in the context of consent; *see id.* at art. 4(10).

G. Legal Controls

The classification of various types of personal information relies on characteristics of that information. The CCPA recognizes that in order for information to maintain those characteristics, legal controls are often required.

1. Legal Controls on De-Identified Information

The discussion is most developed in the context of de-identified information. The FTC Report proposed three legal controls, but it framed these three legal controls as a safe harbor. Specifically, it proposed that information should be considered "not [] reasonably linkable to a particular consumer or device" if the business possessing the information implements three legal controls.[311] In contrast, the CCPA first requires that the information actually be de-identified, i.e. that it cannot reasonably be used to infer information about, or otherwise be linked to, a particular consumer, and then in addition requires that a business that possesses *deidentified* information implement three legal controls.

The CCPA's higher level of protection is appropriate. If there is a reasonable possibility of logical association of *linkable information* with other information relating to the person or household to whom the *linkable information* relates, then it should not qualify as *de-identified information*, even if a business possessing that information implements the specified legal controls intended to prevent such association but fails to accomplish that goal. For this reason, a consumer privacy law should require legal controls on de-identified information:

> In order to qualify as de-identified information, the entity possessing that information must implement controls (A1) to (D1) below.

The first legal control in the FTC Report is that the business "must achieve a reasonable level of justified confidence that the data cannot reasonably be used to infer information about, or otherwise be linked to, a particular consumer, computer, or other device."[312] The CCPA somewhat similarly requires that a business possessing de-identified information "[t]ake reasonable measures to ensure that the information cannot be associated with a consumer or household."[313]

The FTC Report and the CCPA maintain this legal control for different reasons. In the FTC Report, a business's "reasonable level of justified confidence" that the information is de-identified is the principal element of the safe harbor. In the CCPA, however, the legal control is in addition to the requirement that the information actually be de-identified. There remains a

311. *FTC Report*, *supra* note 91, at 21.
312. *Id.*
313. CAL. CIV. CODE § 1798.140(m)(1).

good reason to add a similar legal control because even if a business possesses de-identified information, it is in the public interest that the information not later be re-identified.

There is another difference between the FTC's phrasing and the CCPA's phrasing. The CCPA requires reasonable measures to ensure that the information "cannot be" re-identified, whereas the FTC requires reasonable measures to ensure that the information "cannot reasonably be" re-identified. The test should be "reasonably linkable," both to first qualify as *de-identified information* and also as a legal control.

Building on the proposed definition of *de-identified information*, the first legal control should be:

> (A1) It must take reasonable measures to ensure that the information remains in a form in which there is no reasonable possibility of logical association with other information relating to the person or household to whom the linkable information relates.

The second legal control in the FTC Report is that the business "must publicly commit to maintain and use the data in a de-identified fashion, and not to attempt to re-identify the data."[314] For the FTC, this legal control enables the FTC to act under Section 5 of the FTC Act if the commitment is violated. In a privacy law, there would likely be other and stronger methods of enforcement. Nevertheless, such a public commitment is in the public interest, and the CCPA mirrors this legal control.[315] Thus, the second and third legal controls should be:

> (B1) It must publicly commit to maintain and use the information only in a form in which there is no reasonable possibility of logical association with other information relating to the person or household to whom the linkable information relates.
> (C1) It must publicly commit to not attempt to associate the information with other information relating to the person or household to whom the linkable information relates.

The third legal control in the FTC Report is that if a business makes de-identified information available to other companies, it must "contractually prohibit such entities from attempting to re-identify the data."[316] This legal control ensures that the direct recipient of de-identified information doesn't re-identify the information. The CCPA takes this a step further, requiring that a business possessing de-identified information "[c]ontractually obligates any recipients of the information to comply with all provisions of this subdivision."[317] Thus, in addition to prohibiting direct recipients from re-

314. *FTC Report*, *supra* note 91, at 21.
315. CAL. CIV. CODE § 1798.140(m)(2).
316. *FTC Report*, *supra* note 91, at 21.
317. CAL. CIV. CODE § 1798.140(m)(3).

identification, it also requires recipients to make similar public commitments and to contractually prohibit any downstream recipients from re-identifying the information. This expanded legal control prohibits all downstream re-identification. The last legal control be:

> (D1) It must contractually obligate any third parties to whom it discloses the information to implement controls (A1) to (D1).

2. Legal Controls on Non-Trackable Information

As with de-identified information, the technological algorithm used to transform the personal information into non-trackable information is not sufficient to guarantee that tracking is not possible. There remains a need to add legal controls. Neither the GDPR nor the CCPA place legal controls on non-trackable information, since neither distinguishes such information from other types of personal data (under the GDPR) or personal information (under the CCPA). However, the legal controls placed in the previous subsection on de-identified information can be mirrored here:

> In order to qualify as non-trackable information, the entity possessing that information must implement controls (A2) to (D2) below.
> (A2) It must take reasonable measures to ensure that the information remains in a form in which there is no reasonable possibility of logical association of the information with other information relating to the person or household obtained from another context or another interaction with the person or household.
> (B2) It must publicly commit to maintain and use the information only in a form in which there is no reasonable possibility of logical association of the information with other information relating to the person or household obtained from another context or another interaction with the person or household.
> (C2) It must publicly commit to not attempt to associate the information with other information relating to the person or household obtained from another context or another interaction with the person or household.
> (D2) It must contractually obligate any third parties to whom it discloses the information to implement controls (A2) to (D2).

3. Legal Controls on Pseudonymous Information

Pseudonymous information requires legal controls to ensure that the related person or household is not identified. Neither the GDPR nor the CCPA place legal controls on trackable information, since neither distinguishes such information from other types of personal data (under the GDPR) or personal

information (under the CCPA). However, the legal controls used above can be mirrored here:

> In order to qualify as pseudonymous information, the entity possessing that information must implement controls (A3) to (D3) below.
> (A3) It must take reasonable measures to ensure that the information remains in a form in which the related person or household is not reasonably identifiable using that personal information and other reasonably linkable information.
> (B3) It must publicly commit to maintain and use the information only in a form in which the related person or household is not reasonably identifiable using that personal information and other reasonably linkable information.
> (C3) It must publicly commit to not attempt to identify the person or household to whom the information is related.
> (D3) It must contractually obligate any third parties to whom it discloses the information to implement controls (A3) to (D3).

IX. CONCLUSION

Part III presented a proposal for splitting the scope of personal data as defined in the GDPR or the CCPA into three different sets, based on whether or not personal information is reasonably identifiable and whether or not it is used for tracking. Statutory definitions of these three classifications were developed in Part VIII.

These three classifications of personal information enable the creation of choice framework that utilizes all three options: mandating use through terms and conditions, requiring an opt-out choice, and requiring opt-in consent. The proposed choice framework, developed in Part V, incentivizes the use of pseudonymous information instead of readily identifiable information, and incentivizes the use of one-time identifiers and thereby reduces tracking. Neither the GDPR nor the CCPA incentivizes pseudonymization or disincentivizes tracking through their choice frameworks.

Part VII presented a proposal for corresponding notice requirements. Businesses should disclose the classification of each category of personal information collected, so that consumers may understand the associated privacy risks and make informed choices whether to allow this personal information to be collected. Businesses should disclose whether each use of personal information enables functionality, so that consumers may make informed choices whether to allow each use of their personal information. The sources and recipients should be disclosed, so that consumers may make informed choices whether to allow their personal information to be shared.

There are clearly alternative policy options to these proposals for notice and choice. One could define fewer classifications of personal information, at the cost of not being able to distinguish between them in a choice framework.

One could modify the choice framework in Table 7, and either shift some uses and sharing from opt-out to opt-in to disincentivize them, or one could shift some uses and sharing from opt-in to opt-out to lower the disincentive. However, alternative policy options should be evaluated to determine the tradeoffs between simplicity, privacy protection, and economic impact.

Finally, any notice and choice requirements must be accompanied by statutory text that spells out how consumers can exercise their rights.

APPENDIX: STATUTORY TEXT

Sec. 1. Definitions

(1) **Anonymous Information:** The term 'anonymous information' means personal information for which there is no possibility of logical association with other information relating to the person or household to whom the personal information relates.

(2) **Collection:** The term 'collection' of personal information means access to personal information by any means, including but not limited to gathering, recording, storing, obtaining, receiving, buying, or renting.

(3) **Communications Service:** The term 'communications service' means interstate or foreign communications by wire or radio

(4) **Controller:** The term 'controller' means an entity that alone or jointly with others determines the purposes and means of the collection, use, and/or sharing of personal information.

(5) **Contractor:** The term 'contractor' means an entity that collects, uses, and/or shares personal information but does not alone or jointly with others determine the purposes and means of the collection, use, and/or sharing of personal information. An entity does not alone or jointly with others determine the purposes and means of the collection, use, and/or sharing of personal information if and only if it collects, uses, and/or shares personal information solely pursuant to a written contract that prohibits the entity from collecting, using, and/or sharing personal information for any purposes or using any means other than that specified by the controller(s) of that personal information.

(6) **De-Identified Information:** The term 'de-identified information' means linkable information for which there is no reasonable possibility of logical association with other information relating to the person or household to whom the linkable information relates, providing that the controller:

(A) takes reasonable measures to ensure that the information remains in a form in which there is no reasonable possibility of logical association with other information relating to the person or household to whom the linkable information relates,

(B) publicly commits to maintain and use the information only in a form in which there is no reasonable possibility of logical association with other information relating to the person or household to whom the linkable information relates,

(C) publicly commits to not attempt to associate the information with other information relating to the person or household to whom the linkable information relates, and

(D) contractually obligates any third parties to whom it discloses the information to implement controls (A), (B), and (C).

(7) **First Party:** The term 'first party' means an entity with whom a consumer intentionally interacts.

(8) **Functional Use:** The term 'functional use' means the technical use of personal information to provide functionality. Functional use does not include the use of personal information in exchange for consideration from a third party.

(9) **Linkable Information:** The term 'linkable information' means personal information that is not anonymous information.

(10) **Non-Trackable Information:** The term 'non-trackable information' means reasonably linkable information for there is no reasonable possibility of logical association of the information with other information relating to the person or household obtained from another context or another interaction with the person or household, providing that the controller:

(A) takes reasonable measures to ensure that the information remains in a form in which there is no reasonable possibility of logical association of the information with other information relating to the person or household obtained from another context or another interaction with the person or household,

(B) publicly commits to maintain and use the information only in a form in which there is no reasonable possibility of logical association of the information with other information relating to the person or household obtained from another context or another interaction with the person or household,

(C) publicly commits to not attempt to associate the information with other information relating to the person or household obtained from another context or another interaction with the person or household, and

(D) contractually obligates any third parties to whom it discloses the information to implement controls (A), (B), and (C).

(11) **Non-Sensitive:** The term 'non-sensitive', when used in conjunction with any type of personal information, means personal information that is not sensitive information.

(12) **Opt-In Consent:** The term 'opt-in consent' to specified collection, use, and/or sharing of personal information means any freely given, specific, informed and unambiguous indication of the person's wishes, by a statement or by a clear affirmative action, by which the

person signifies agreement to the specified collection, use, and/or sharing of personal information relating to that person.

(13) **Opt-Out Choice:** The term 'opt-out choice' of specified collection, use, and/or sharing of personal information means a choice by which a person can withdraw consent to the specified collection, use, and/or sharing of personal information relating to that person.

(14) **Personal Information:** The term 'personal information' means any information relating to a natural person or to a household, excluding publicly available information.

(15) **Pseudonymous Information:** The term 'pseudonymous information' means trackable information for which the related person or household is not reasonably identifiable using that personal information and other reasonably linkable information, providing that the controller:

(A) takes reasonable measures to ensure that the information remains in a form in which the related person or household is not reasonably identifiable using that personal information and other reasonably linkable information,

(B) publicly commits to maintain and use the information only in a form in which the related person or household is not reasonably identifiable using that personal information and other reasonably linkable information,

(C) publicly commits to not attempt to identify the person or household to whom the information is related, and

(D) contractually obligates any third parties to whom it discloses the information to implement controls (A), (B), and (C).

(16) **Publicly Available Information:** The term 'publicly available information' means information relating to a natural person or to a household (a) in publicly available government records, (b) that the person or household to whom the personal information is related has made publicly available, or (c) that was made publicly available by widely distributed media.

(17) **Reasonably Identifiable Information:** The term 'reasonably identifiable information' means trackable information that is not pseudonymous information.

(18) **Reasonably Linkable Information:** The term 'reasonably linkable information' means personal information for which there is a reasonable possibility of logical association with other information relating to the person or household to whom the personal information relates.

(19) **Sensitive:** The term 'sensitive', when used in conjunction with any type of personal information, means personal information that relates to sensitive characteristics of a person or household, including, but not limited to:

(A) private personal identifiers, including social security number, driver's license number, state identification card number, and passport number;

(B) private physical characteristics, including genetic data, biometric data, health data, and racial or ethnic origin; or

(C) personal information about behavior or beliefs, including political opinions, religious or philosophical beliefs, union membership, sex life or sexual orientation, financial information, information pertaining to children, precise geo-location, content of communications, web browsing history, and application usage history.

(20) **Sharing:** The term 'sharing' of personal information means disclosure by any means, including but not limited to disclosure by transmission, dissemination, making available, releasing, transferring, renting, selling, or otherwise communicating, except that it excludes disclosure to a contractor.

(21) **Third Party:** The term 'third party' means any entity other than a first party or a first party's contractors.

(22) **Trackable Information:** The term 'trackable information' means reasonably linkable information that is not non-trackable information.

(23) **Use:** The term 'use' of personal information means any operation or set of operations performed on personal information, including but not limited to organization, structuring, adaptation, alteration, retrieval, consultation, alignment, or combination of personal information.

Sec. 2. Notice

(a) **Privacy Policy:** A controller shall maintain a publicly accessible privacy policy. The privacy policy shall disclose accurate information regarding the controller's collection, use, and sharing of personal information sufficient for consumers to make informed choices regarding the use of the controller's services.

(b) **Categories Of Personal Information:** The privacy policy shall disclose the categories of personal information collected and used, and for each such category, the classification(s) of that category. The classifications shall consist of reasonably identifiable information, pseudonymous information, non-trackable information, de-identified information, and anonymous information.

(c) **Methods And Sources:** The privacy policy shall disclose, for each category of personal information collected:

(1) the method of collection (if the personal information is collected by or on behalf of the controller), and

(2) the sources of collection (if the personal information is shared with the controller by another entity).

(d) **Purposes:** The privacy policy shall disclose, for each category of personal information collected or used, the purposes for which the category of personal information is collected or used.

(e) **Functional Use:** The privacy policy shall disclose, for each category of personal information collected or used and each such purpose,

whether the use constitutes functional use, and if so, the functionality enabled by the collection and use of that category of personal information.

(f) **Shared Personal Information:** The privacy policy shall disclose the categories of personal information shared, and for each such category, the classification(s) of that category. The classifications shall consist of reasonably identifiable information, pseudonymous information, non-trackable information, de-identified information, and anonymous information.

(g) **Recipients:** The privacy policy shall disclose the third parties with which the controller shares personal information. For each such third party, the privacy policy shall disclose the categories of personal information shared with that third party, the purposes for which the controller shares each category of personal information with that third party, and any contractual limits on the third party's use and further sharing of that personal information. If a controller enables any third parties to collect additional personal information, the controller's privacy policy shall disclose the third parties so enabled and any contractual limits on such collection.

Sec. 2. Choice

(a) **Markets With Effective Competition:** A controller in a market with effective competition, except for a controller offering telecommunications (insofar as it receives or obtains personal information by virtue of its provision of telecommunications), shall

(1) **Opt-Out of Non-Functional Use:** offer consumers an opt-out choice from the controller's collection and use for non-functional purposes (if any) of the consumer's non-sensitive reasonably identifiable information and sensitive pseudonymous information,

(2) **Opt-In To Non-Functional Use:** obtain opt-in consent for the controller's collection and use for non-functional purposes (if any) of the consumer's sensitive reasonably identifiable information,

(3) **Opt-Out of Sharing:** offer consumers an opt-out choice from the controller's sharing (if any) of the consumer's non-sensitive pseudonymous information and sensitive non-trackable information, and

(4) **Opt-In To Sharing:** obtain opt-in consent for the controller's sharing (if any) of the consumer's reasonably identifiable information and sensitive pseudonymous information.

(b) **Markets Without Effective Competition and Communications Services:** A controller in a market without effective competition, and a controller offering a communications service (insofar as it receives or obtains personal information by virtue of its provision of a communications service), shall

(1) **Opt-Out of Non-Functional Use:** offer consumers an opt-out choice from the controller's collection and use for non-functional purposes (if any) of the consumer's non-sensitive pseudonymous information and sensitive non-trackable information,

(2) **Opt-In To Non-Functional Use:** obtain opt-in consent for the controller's collection and use for non-functional purposes (if any) of the consumer's reasonably identifiable information and sensitive pseudonymous information,

(3) **Opt-Out of Sharing:** offer consumers an opt-out choice from the controller's sharing (if any) of the consumer's non-sensitive non-trackable information, and

(4) **Opt-In To Sharing:** obtain opt-in consent for the controller's sharing (if any) of the consumer's reasonably identifiable information, pseudonymous information, and sensitive non-trackable information.