Richmond Journal of Law & Technology

Volume 29 | Issue 1 Article 2

11-30-2022

The CCPA, "Inferences Drawn," and Federal Preemption

Jordan M. Blanke
Mercer University

Richmond Journal of Law & Technology Volume XXIX, Issue 1

THE CCPA, "INFERENCES DRAWN," AND FEDERAL PREEMPTION

Jordan M. Blanke*

Cite as: Jordan M. Blanke, *The CCPA, "Inferences Drawn," and Federal Preemption*, 29 RICH. J.L. & TECH. 53 (2022).

* Jordan "Jody" Blanke is the Ernest L. Baskin, Jr. Distinguished Professor of Computer Science and Law at the Stetson-Hatcher School of Business at Mercer University in Atlanta, Georgia. I would like to thank Ignacio Cofone, Kim Houser, Bill McGeveran and Dan Solove for their insightful comments and suggestions.

ABSTRACT

In 2018, California passed an extensive data privacy law. One of its most significant features was the inclusion of "inferences drawn" within its definition of "personal information." The law was significantly strengthened in 2020 with the expansion of rights for California consumers, and new obligations on businesses, including the incorporation of GDPR-like principles of data minimization, purpose limitation, storage limitation, and the creation of an independent agency to enforce these laws. In 2022, the Attorney General of California issued an Opinion that provided for an extremely broad interpretation of "inferences drawn." Thereafter, the American Data Privacy Protection Act was introduced in the United States Congress. This law does not provide nearly the protection for inferences that California law does, and this federal bill threatens to preempt almost all of California's data privacy law. This article argues that, given the importance of California being able to finally regulate "inferences drawn," any federal bill must either provide similar protection, exclude California law from preemption, or be opposed.

I. INTRODUCTION

A. Inferences

[1] The recognition of the significance of inferences drawn from data has been acknowledged for some time now.[1] As Omer Tene and Jules Polonetsky noted in 2013, "what calls for scrutiny is often not the accuracy of the *raw data* but rather the accuracy of the *inferences* drawn from the data."[2] Much has been written recently about the importance of these inferences.[3] Ignacio Cofone observed that "[p]ersonal data . . . is about

[1] *See* Omer Tene & Jules Polonetsky, *Big Data for All: Privacy and User Control in the Age of Analytics*, 11 NW. J. TECH. & INTELL. PROP. 239, 270 (2013) (explaining the importance of inferences back in 2013).

[2] *Id.* at 270.

[3] *See generally* Hideyuki Matsumi, *Predictions and Privacy: Should There Be Rules About Using Personal Data to Forecast the Future?*, 48 CUMB. L. REV. 149 (2018) (discussing the use of personal data to make predictions); Sandra Wachter & Brent Mittelstadt*, A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI*, 2019 COLUM. BUS. L. REV. 494 (2019) (discussing how individuals have little control over how their personal data is used to make inferences about them); Jordan M. Blanke, *Protection for 'Inferences Drawn:' A Comparison Between the General Data Protection Rule and the California Consumer Privacy Act*, 2 GLOB. PRIV. L. REV. 81 (2020) (comparing the protection provided for inferential data between the European Union's General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA)); Alicia Solow-Niederman, *Information Privacy and the Inference Economy*, 117 NW. U.L. REV. 357 (2022) (discussing how information privacy protections should be reframed to account for inferential data); Daniel J. Solove, *The Limitation of Privacy Rights*, 98 NOTRE DAME L. REV. (forthcoming 2023) (arguing how current privacy rights alone are insufficient to regulate data information protection); Ignacio Cofone, *Privacy Standing*, 4 U. ILL. L. REV. 1367 (2022) (distinguishing between privacy harms and other data harms caused by inferences and discussing how they affect the law of standing).

inferences."[4] Only recently, however, have efforts to regulate inferences begun.[5]

[2] One of the earliest examples of the power of data analytics occurred in 2002, when J.P. Martin, an executive at Canadian Tire, started examining some of the credit card data he had available.[6] He discovered that people who bought furniture pads were good credit risks and people who bought cheap motor oil were not.[7] While not an earth-shattering revelation, Mr. Martin's discovery clearly signaled the advent of a new age of digital knowledge, and serves as an example of how inferences can be drawn from commonly produced personal data.

[3] Probably the most famous example of both the accuracy of predictive data analytics and its potential for intrusion upon privacy occurred in 2012.[8] Target observed that women who bought unscented lotion, and several weeks later, calcium, magnesium, and zinc supplements,

---

[4] Ignacio Cofone, *Beyond Data Ownership*, 43 CARDOZO L. REV. 501, 533 (2021); *see also* Cofone, *supra* note 3, at 1384 ("[H]armful information is rarely collected information and is frequently inferred information– produced by aggregating different pieces of seemingly inoffensive collected information.").

[5] California Consumer Privacy Act of 2018, CAL. CIV. CODE § 1798.140(o)(1)(K) (Deering 2022) [hereinafter CCPA] (including inferential data as "personal data") (The California Consumer Privacy Act was the first piece of United States legislation to specifically include "inferences drawn" within the definition of personal data or personal information.).

[6] Charles Duhigg, *What Does Your Credit-Card Company Know About You?*, N.Y. TIMES MAG. (May 12, 2009), https://www.nytimes.com/2009/05/17/magazine/17credit-t.html [https://perma.cc/XGP7-2ADZ]; *see* Blanke, *supra* note 3, at 81.

[7] Blanke, *supra* note 3, at 81.

[8] *Id.* at 82.

were likely pregnant.[9] Target mailed one of these people a letter congratulating her on her pregnancy and included some coupons for use at the store.[10] The father of this 16-year old girl, who happened to open the letter, was shocked and angry to read of such preposterous news.[11] The rest, as they say, is history.

[4] Companies collect enormous amounts of information from our habits, or raw data, and create profiles containing raw data and the inferences drawn from that data. "In 2012 it was reported that Acxiom executives stated that 'its database contains information about 500 million active consumers worldwide, with more than 1,500 data points per person.'"[12] By 2014, Acxiom explained that "[f]or every consumer we have more than 5,000 attributes of customer data."[13] In 2017, Wolfie Christl wrote that Facebook had profiles on 1.9 billion Facebook users, 1.2 billion WhatsApp users, and 600 million Instagram users.[14] At the same time,

[9] Charles Duhigg, *How Companies Learn Your Secrets*, N.Y. TIMES MAG. (Feb. 16, 2012), https://www.nytimes.com/2012/02/19/magazine/shopping-habits.html [https://perma.cc/7XDR-K9SG]; Blanke, *supra* note 3, at 82.

[10] Blanke, *supra* note 3, at 82.

[11] *Id.*

[12] *Id*. at 83 (quoting Natasha Singer, *Mapping, and Sharing, the Human Genome*, N.Y. TIMES (June 16, 2012), https://www.nytimes.com/2012/06/17/technology/acxiom-the-quiet-giant-of-consumer-database-marketing.html [https://perma.cc/KD77-Q4HN]).

[13] Jeff Chester, *Acxiom: 'For Every Consumer We Have More Than 5,000 Attributes of Customer Data'*, CTR. FOR DIGIT. DEMOCRACY (Jan. 10, 2014), https://www.democraticmedia.org/acxiom-every-consumer-we-have-more-5000-attributes-customer-data [https://perma.cc/T3TH-N7L7].

[14] Wolfie Christl, *Corporate Surveillance in Everyday Life*, CRACKED LABS (June 2017), https://crackedlabs.org/en/corporate-surveillance/ [https://perma.cc/7TU7-ZUQ2].

Google had profiles on 2 billion Android users, over 1 billion Gmail users, and over 1 billion YouTube users and Apple had profiles on 1 billion iOS users.[15]

[5] Many studies have shown that personal information can easily be inferred from readily available data.[16] One study "demonstrated how Social Security numbers could be inferred from birth data and readily available information from data brokers and social network profiles."[17] Another study "showed how Facebook likes can infer private traits and characteristics, such as gender, religion, political affiliation, and sexual orientation."[18] Yet another study "showed how publicly available geographic information from Tweets could accurately infer 'average income based on one's neighborhood, average housing cost, debt, and other demographic information, such as political views.'"[19]

[6] Several problems permeate the collection and combination of such vast amounts of raw data, along with the inferences drawn from it. One problem with using raw data like this is the accuracy of the data itself. Sometimes data is inaccurate because people intentionally provide false information to protect their privacy, and sometimes inaccuracies happen simply from the collection of inaccurate data.[20] Another problem is that data

[15] *Id.*

[16] *See* Blanke, *supra* note 3, at 84 (discussing multiple studies that inferred an individual's identity from publicly available information).

[17] *Id.*

[18] *Id.*

[19] *Id.*

[20] *See id.* at 84–85.

analytics and predictive analytics may perpetuate existing discriminatory practices, or even create new ones.[21] Finally, inferences made can be based upon mere coincidence rather than causal evidence.[22]

[7] I highlighted issues surrounding inferences in a previous article:

> Inferences drawn from data can be problematic both in building a profile and in later extracting information from it. As data is collected about a person, inferences may be drawn from the data and stored as part of the profile as if it were independently collected data. Unless there is a distinction made in the profile about which data is *raw* and which is inferred, all of it may appear to be *raw*. Certainly, … this data that has now been saved to the profile and will likely thereafter be considered as factual and verified data that becomes a permanent and persistent part of that profile.[23]

[8] In writing about the General Data Protection Regulation's (GDPR) focus on "automated" decisions, Daniel Solove observed that inferences

[21] *See generally* Solon Barocas & Andrew D. Selbst, *Big Data's Disparate Impact*, 104 CALIF. L. REV. 671 (2016) (examining unintentional discrimination from algorithms through the lens of American antidiscrimination law); James Grimmelmann & Daniel Westreich, *Incomprehensible Discrimination*, 7 CALIF. L .REV. 164 (2017) (analyzing the problems that come from using algorithmically derived models to make employment decisions through a fictional hypothetical case); Danielle Keats Citron & Frank Pasquale, *The Scored Society: Due Process for Automated Predictions*, 89 WASH. L. REV. 1 (2014) (examining the problems that arise from credit scoring); Tal Z. Zarsky, *Understanding Discrimination in the Scored Society*, 89 WASH. L. REV. 1375 (2014) (discussing discrimination-based concerns from scoring practices performed by big data).

[22] Blanke, *supra* note 3, at 84.

[23] *Id.* at 84–85.

should be receiving more attention than "automated" decisions.[24] "Inference involves using existing data to generate new data about a person or to make predictions about them. Inference, much more than automation, is what the law should regulate."[25] What is particularly ironic about inferences is that it is arguable as to which is potentially more dangerous: "bad" inferences, for example, those based upon inaccurate data, discriminatory practices, or without a causal basis, or "good" inferences, for example, the one in the Target case, where clever analytics resulted in an accurate, but privacy-invasive conclusion.

B. Regulation

[9] In 2018, California became the first state to pass an extensive data privacy act — the California Consumer Privacy Act (CCPA).[26] The CCPA became effective on January 1, 2020.[27] California subsequently passed the Consumer Privacy Rights Act of 2020 (CPRA) in November of 2020.[28] The CPRA amends and builds upon the CCPA and will become effective on January 1, 2023.[29]

---

[24] Solove, *supra* note 3, at 48.

[25] *Id.*

[26] CCPA § 1798.100–199; *CCPA vs CPRA: What's the Difference?*, BLOOMBERG LAW (Jul. 31, 2021), https://pro.bloomberglaw.com/brief/the-far-reaching-implications-of-the-california-consumer-privacy-act-ccpa [https://perma.cc/5RC2-L4U9].

[27] *CCPA vs CPRA: What's the Difference?*, *supra* note 26.

[28] *Id.*

[29] *Id.*; California Privacy Rights Act of 2020, CAL. CIV. CODE § 1798.100–199 (Deering 2022) (effective Jan. 1, 2023).

[10] The CCPA and CPRA are the boldest attempts in the United States to provide for the protection of personal information.[30] In some regards, California's laws provide more protection for consumer data than does the GDPR for citizens of the European Union.[31] The CCPA bestowed upon the Attorney General of California unprecedented power to regulate data privacy protection.[32] The CPRA authorized the creation of the California Privacy Protection Agency (CPPA), which will share the power to regulate data privacy protection with the Attorney General, but will likely take the lead in everyday enforcement of the law.[33] Most significantly, however, the CPRA will not only provide an array of rights for consumers regarding their personal information, but will place significant obligations on businesses that collect, use, share, and store raw data; all of these new requirements will be monitored and enforced by the CPPA.[34]

[11] One of the least discussed, but most important provisions in the CCPA is the inclusion of "inferences drawn" within the extremely broad definition of "personal information."[35] In March of 2022, the Attorney General of California issued an opinion pursuant to a request for

[30] Unless otherwise stated, I will use the terms "personal information" and "personal data" synonymously. Likewise, I will use the terms "information privacy," "data protection," and "data privacy protection" synonymously.

[31] *See* Wachter & Mittelstadt, *supra* note 3, at 499; Blanke, *supra* note 3, at 81.

[32] *See* Blanke, *supra* note 3, at 91.

[33] *See* Lydia de la Torre & Glenn Brown, *What is the California Privacy Protection Agency?*, IAPP (Nov. 23, 2020), https://iapp.org/news/a/what-is-the-california-privacy-protection-agency/ [https://perma.cc/ZD62-PSZQ].

[34] *See The California Consumer Privacy Act Explained*, COOKIE SCRIPT (Apr. 28, 2022), https://cookie-script.com/privacy-laws/cpra [https://perma.cc/8JV5-6AZY].

[35] *See* CCPA § 1798.140(o)(1)(K).

clarification about that section.[36] The opinion could not have interpreted "inferences drawn" any more broadly, and this interpretation helps bolster the strength of the CCPA.

[12] In June of 2022, the American Data Privacy Protection Act (ADPPA) was introduced in Congress.[37] Although it provides many privacy protections, it contains a preemption section.[38] The result of this preemption section is that almost all of the CPRA would be preempted, eliminating the broad definition of personal information and inferences drawn and precluding California from enforcing the powerful GDPR-like obligations in the CCPA against businesses.[39]

[13] I argue in this article that California's bold and novel attempt to regulate inferences must survive either by incorporation of similar provisions in federal law or by exemption from preemption. Any federal bill that fails to implement one of these solutions must be opposed.

[14] Part II of this article will discuss the sections of the CCPA relevant to "inferences drawn." Part III will address the changes made to the CCPA by the CPRA relevant to those sections. Part IV will discuss the March 2022 Opinion of the California Attorney General. Part V will explore the provisions of the proposed federal legislation that would preempt the relevant sections of California law without providing comparable protection. Finally, Part VI will argue that unless a federal bill adopts the same protections provided under the CCPA pertaining to "inferences

[36] 105 Ops. Cal. Att'y Gen. 26 (2022), 2022 WL 815641.

[37] American Data Privacy Protection Act, H.R. 8152, 117th Cong. (as introduced in House June 21, 2022) [hereinafter June Bill].

[38] *See id.* § 404(b).

[39] *See id.*

drawn," any federal bill must either carve out an exception to preemption for California law or be opposed.

II. THE ORIGINAL CCPA

[15] The CCPA provides an extremely broad and comprehensive definition of "personal information":

> "Personal information" means 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. Personal information includes:
> .
> .
> *(K) Inferences drawn from any of the information identified in this subdivision to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.*[40]

[40] The full definition reads:

> "Personal information" means 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. Personal information includes, but is not limited to, the following if it identifies, relates to, describes, is [reasonably] capable of being associated with, or could be reasonably linked, directly or indirectly, with a particular consumer or household:
>
> (A) Identifiers such as a real name, alias, postal address, unique personal identifier, online identifier, Internet Protocol address, email address, account name, social security number, driver's license number, passport number, or other similar identifiers.
>
> (B) Any personal information described in subdivision (e) of Section 1798.80.

[16] Section K is significant because it includes within its definition any information that is collected, matched, derived, inferred, or otherwise gathered to create a profile from any of the many sources listed in the other sections of the definition of personal information. Section K encompasses all data which could create a profile reflecting a person's "preferences, characteristics, psychological trends, predispositions, behavior, attitudes,

> (C) Characteristics of protected classifications under California or federal law.
> (D) Commercial information, including records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies.
> (E) Biometric information.
> (F) Internet or other electronic network activity information, including, but not limited to, browsing history, search history, and information regarding a consumer's interaction with an Internet Web site, application, or advertisement.
> (G) Geolocation data.
> (H) Audio, electronic, visual, thermal, olfactory, or similar information.
> (I) Professional or employment-related information.
> (J) Education information, defined as information that is not publicly available personally identifiable information as defined in the Family Educational Rights and Privacy Act (20 U.S.C. Sec. 1232g; 34 C.F.R. Part 99).
> (K) Inferences drawn from any of the information identified in this subdivision to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.

CCPA § 1798.140(o)(1) (emphasis added).

In Part II of this article, I use "CCPA" to refer to the original section numbers of the CCPA as passed in 2018. Some of the numbering was amended by the CRPA. In subsequent Parts of this article, I use references to CAL. CIV. CODE. For example, after passage of the CPRA, this section is now cited as CAL. CIV. CODE § 1798.140(v)(1). The only significant change made by the CPRA to this definition of "personal information" was the deletion of the bracketed words, "reasonably."

intelligence, abilities, and aptitudes."[41] The definition of personal information and inferences drawn could not be broader.

[17] The breadth of these definitions is significant when it comes to the rights provided by the original CCPA to a California consumer, who:

1. can request from any business that collects personal information about the consumer to disclose to the consumer the categories and specific pieces of information collected;[42]

2. can expect that a business that collects personal information inform the consumer of the categories of information collected and the purposes for which that information is used;[43]

3. can expect that a business shall not collect additional categories of personal information without providing the consumer appropriate notice;[44]

4. can request a business to delete any personal information about the consumer that the business collected from the consumer;[45]

5. can request a business that sells the consumer's information to disclose the categories of personal information collected about the consumer, the categories of personal information that the business

[41] *Id.* § 1798.140(o)(1)(K).

[42] *Id.* § 1798.100(a).

[43] *Id.* § 1798.100(a)(1).

[44] *Id.*

[45] CCPA § 1798.105(a).

sold about the consumer, and the categories of personal information that the business disclosed about the consumer for a business purpose;[46] and

6. can direct a business that sells personal information about the consumer not to sell that information.[47]

[18] Other than rights that may be provided under specifically targeted legislation like HIPAA,[48] FERPA,[49] or the FCRA,[50] the rights provided by the CCPA became the closest thing available in the U.S. to the data rights provided to citizens of the EU by the GDPR.[51] Since California passed the CCPA (and the CPRA), several other states have passed data privacy legislation, but none of them provide the protection that California law does.[52] The protection is not as comprehensive as the CCPA if for no other reason, because of the states' failure to include protection for inferences.[53]

---

[46] *Id.* § 1798.115(a).

[47] *Id.* § 1798.120(a).

[48] Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (codified as amended in scattered sections of 18, 26, 29, and 42 U.S.C.).

[49] Family Educational Rights and Privacy Act, 20 U.S.C. § 1232(g).

[50] Fair Credit Reporting Act, 15 U.S.C. § 1681.

[51] Regulation 2016/679, 2016 O.J. (L 119) 1 (EU).

[52] *See Data Privacy Laws by State: Comparison Charts*, BLOOMBERG L. (Feb. 2, 2022), https://pro.bloomberglaw.com/brief/data-privacy-laws-in-the-u-s/ [https://perma.cc/Z56N-KJTW].

[53] *See* Virginia Consumer Data Protection Act, VA. CODE ANN. § 59.1-575 to -585 (2022); Colorado Privacy Act, COLO. REV. STAT. § 6-1-1301 to -1313 (2022); S.B. 6,

III. THE CPRA

[19] In November of 2020, California voters approved the CPRA.[54] Some provisions of the CPRA added new sections to the CCPA, but many merely amended existing sections.[55] Accordingly, unless necessary to make a distinction, I will refer to the changes made by the CPRA to the CCPA, in its entirety, as "the CCPA as amended."

[20] In focusing on the relevant changes to the inferences drawn section of the definition of personal information, there are several changes of significance. First, the CCPA as amended provides for a new item within the definition of personal information, called "sensitive personal information."[56] This addition is important because all the categories of

2022 Conn. Gen. Assemb., Reg. Sess. (2022); Utah Consumer Privacy Act, UTAH CODE ANN. § 13-61-101 to -404 (LexisNexis 2022).

[54] *CCPA vs CPRA: What's the Difference?*, *supra* note 26.

[55] *Id.*

[56] "Sensitive personal information" is defined as:

(1) Personal information that reveals:

(A) A consumer's social security, driver's license, state identification card, or passport number.

(B) A consumer's account log-in, financial account, debit card, or credit card number in combination with any required security or access code, password, or credentials allowing access to an account.

(C) A consumer's precise geolocation.

(D) A consumer's racial or ethnic origin, religious or philosophical beliefs, or union membership.

(E) The contents of a consumer's mail, email, and text messages unless the business is the intended recipient of the communication.

(F) A consumer's genetic data.

(2)

(A) The processing of biometric information for the purpose of uniquely identifying a consumer.

sensitive personal information are now specifically incorporated into the definition of personal information, from which inferences may be drawn. In turn, inferences drawn from sensitive personal information are now considered to be part of one's personal information under the law, broadening consumer protections. This addition is also noteworthy because it echoes the language of Article 9 of the GDPR.[57]

[21] The second significant change is the addition of a specific definition for "profiling," which is "any form of automated processing of personal information … and in particular to analyze or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location, or movements."[58] This definition mirrors protection provided in the GDPR that permits individuals to opt-out of automated decision-making and profiling.[59]

(B) Personal information collected and analyzed concerning a consumer's health.

(C) Personal information collected and analyzed concerning a consumer's sex life or sexual orientation.

(3) Sensitive personal information that is "publicly available" pursuant to paragraph (2) of subdivision (v) shall not be considered sensitive personal information or personal information.

CAL. CIV. CODE § 1798.140(ae) (Deering 2022).

[57] *See* Regulation 2016/679, art. 9, 2016 O.J. (L 119) 1, 38 (EU).

[58] CAL. CIV. CODE § 1798.140(z).

[59] *See* Regulation 2016/679, art. 22, 2016 O.J. (L 119) 1, 46 (EU).

[22] The third important change created by the CPRA is that the CCPA as amended strengthens some existing consumer rights included in the original CCPA and adds several more.[60] These rights are particularly significant because they all include inferences drawn as part of personal information:

1. Under the original CCPA, the right to know what information is being collected, the right to access such information, and the right to know what information is sold or shared was generally limited to the 12-month period prior to the request.[61] For these rights, as well as the right to delete and the new right to correct, consumers will now be able to "request that the business disclose the required information beyond the 12-month period and the business shall be required to provide such information unless doing so proves impossible or would involve a disproportionate effort."[62]

2. The right to delete will now require a business to not only delete the requested information, but to "notify all third parties to whom the business has sold or shared such personal information, to delete the consumer's personal information, unless this proves impossible or involves disproportionate effort."[63]

3. A new right was created to request that a "business that maintains inaccurate personal information about the consumer correct such

[60] *See CCPA vs CPRA: What's the Difference?*, *supra* note 26.

[61] CAL. CIV. CODE § 1798.130(a)(2).

[62] *Id.* § 1798.130(a)(2)(B).

[63] *Id.* § 1798.105(c).

inaccurate personal information."[64] This is another move by California to provide rights similar to those under the GDPR.[65]

4. A new right to limit the use and disclosure of sensitive personal information was also created.[66] Along with the new definition of sensitive personal information came the right for a consumer, "at any time, to direct a business that collects sensitive personal information about the consumer to limit its use of the consumer's sensitive personal information to that use which is necessary to perform the services or provide the goods reasonably expected by an average consumer."[67] This adds yet another familiar GDPR principle, that of purpose limitation.[68]

[23] The fourth and arguably the most significant change, at least in terms of the nature of protection provided, is that California specifically adopted several fundamental privacy principles that have long been part of the GDPR. The principles of data minimization (that businesses should collect only the minimum amount of information necessary for the transaction) and purpose limitation (that the information be limited to the purposes for which it is being collected) are specifically referenced in the recitals addressing the Responsibilities of Businesses in the Purpose and Intent section introducing the CPRA legislation.[69]

---

[64] *Id.* § 1798.106(a).

[65] *See* Regulation 2016/679, art. 5, 2016 O.J. (L 119) 1, 35 (EU).

[66] CAL. CIV. CODE § 1798.121.

[67] *Id.*

[68] *See id.* § 1798.121(a).

[69] *See* ALEX PADILLA, CAL. SEC'Y OF STATE, TEXT OF PROPOSED LAWS: CALIFORNIA GENERAL ELECTION 44 (2020).

[24] Principles of data minimization are further evident in the CPRA additions requiring the collection, use, retention, and sharing of personal information be "reasonably necessary and proportionate."[70] Principles of purpose limitation are plainly enunciated among the General Duties of Businesses that Collect Personal Information, which state that a "business shall not collect additional categories of personal information or use personal information collected for additional purposes that are incompatible with the disclosed purpose for which the personal information was collected, without providing the consumer with notice consistent with this section."[71] Furthermore, the GDPR principle of storage limitation is also included among the General Duties of Businesses that Collect Personal Information; "a business shall not retain a consumer's personal information or sensitive personal information for each disclosed purpose for which the personal information was collected for longer than is reasonably necessary for that disclosed purpose."[72]

[25] The fifth significant change, in what may likely become the *most* important addition from the CPRA and because it is independent of all the notice and disclosure requirements of the CCPA as amended, is a new affirmative obligation on businesses to handle personal information consistent with the principles of data minimization and purpose and storage limitations:

> A business's collection, use, retention, and sharing of a consumer's personal information shall be reasonably necessary and proportionate to achieve the purposes for

[70] CAL CIV. CODE §§ 1798.100(c), 1798.105(d)(2), 1798.140(e)–(e)(2).

[71] *Id.* § 1798.100(a)(1); *see also id.* § 1798.100(a)(2) (highlighting a similar restriction for the collection of "sensitive personal information.").

[72] *Id.* § 1798.100(a)(3).

> which the personal information was collected or processed, or for another disclosed purpose that is compatible with the context in which the personal information was collected, and not further processed in a manner that is incompatible with those purposes.[73]

[26] The GDPR and the original CCPA have been distinguished by the complete absence in the CCPA of "purpose limitation…, data minimization…, [and] data retention (limiting storage of data to periods justified by those purposes)[.]"[74] These principles are all present in the CCPA as amended.[75] Other differences highlighted also included the CCPA's "few requirements concerning the purposes for data collection or the proportionality of data handling to those purposes."[76] That notion is clearly evident in the CCPA as amended in the "reasonably necessary and proportionate" mandate in the section on the General Duties of Businesses that Collect Personal Information.[77] Thus, the CCPA as amended provides not only for consumer rights, but also a substantive obligation on businesses to collect, process, use, and retain personal information in manners consistent with the principles of data minimization, purpose limitation, and storage limitation.

---

[73] *Id.* § 1798.100(c).

[74] Anupam Chander et al., *Catalyzing Privacy Law*, 105 U. MINN. L. REV. 1733, 1756 (2021).

[75] Steven Nakasone, *Get Ready for the Amended California Consumer Privacy Act*, BUCHALTER (Aug. 1, 2022), https://www.buchalter.com/publication/get-ready-for-the-amended-california-consumer-privacy-act [https://perma.cc/3P7Y-YLQS].

[76] Chander et al., *supra* note 74, at 1757.

[77] CAL. CIV. CODE § 1798.100(c).

[27] Last, but certainly not least, the CPRA created the California Privacy Protection Agency.[78] The CPPA has the power to enforce the CCPA as amended through administrative actions and, along with the Attorney General, has rulemaking authority.[79] The CCPA as amended has an entire section devoted to rulemaking and lists over twenty issues that it expects rules to address in the future.[80] The CPPA is charged to "[a]dminister, implement, and enforce through administrative actions this title" and to "protect the fundamental privacy rights of natural persons with respect to the use of their personal information."[81] In short, the CPPA has become the most powerful enforcer of data privacy laws in the United States.

IV. THE CALIFORNIA ATTORNEY GENERAL OPINION

[28] On March 10, 2022, the Attorney General of California issued an Opinion pursuant to his authority to give opinions on questions of law to specified public officials upon their request (hereinafter referred to as "the Opinion").[82] California Assemblyman Kevin Kiley asked whether, under the CCPA, "a consumer's right to receive the specific pieces of information that a business has collected about that consumer applies to internally generated inferences."[83]

[78] *Id.* § 1798.199.10(a).

[79] *Id.*

[80] *See id.* § 1798.185.

[81] *Id.* §§ 1798.199.40(a)–(c).

[82] *See* 105 Ops. Cal. Att'y Gen. 26 (2022), 2022 WL 815641, at *1.

[83] *Id.* at *5.

[29] The Opinion recited the definition of inference from the CCPA[84] and further explained:

> An inference is essentially a characteristic deduced about a consumer (such as "married," "homeowner," "online shopper," or "likely voter") that is based on other information a business has collected (such as online transactions, social network posts, or public records). Some businesses create inferences using their own proprietary methods, and then sell or transfer the inferences to others for commercial purposes.[85]

[30] The Opinion discussed the fact that many pieces of personal information can be inferred from other pieces of information.[86] For example, "that a person's date of birth and place of birth, in combination with public databases, can be used to predict their social security number[.]"[87] The Opinion stated that "the plain language of the statute, as well as the legislative history, persuade us that the CCPA purposefully gives consumers a right to receive inferences, regardless of whether the inferences were generated internally by the responding business or obtained by the responding business from another source."[88]

[84] CAL. CIV. CODE § 1798.140(r); *id.*

[85] 105 Ops. Cal. Att'y Gen. 26 (2022), 2022 WL 815641, at *5.

[86] *See id.* at *6.

[87] *Id.* at *5.

[88] *Id.*

[31] The Opinion cited the CCPA definitions for personal information and inferences drawn as being most relevant to its analysis:[89]

> "Inferences" are themselves "personal information" for purposes of the CCPA (and therefore disclosable) when two conditions exist. First, the inference is drawn "from any of the information identified in this subdivision." Second, the inference is used to "create a profile about a consumer," or in other words to predict a salient consumer characteristic.

[32] Regarding the first condition, the Opinion said that an inference must be drawn from among the many items listed in the definition of personal information. The Opinion made clear that if a business holds a consumer's personal information, regardless of whether it "gathered the information from the consumer, found the information in public repositories, bought the information from a broker, inferred the information through some proprietary process of the business's own invention, or any combination thereof [,]" it must disclose that information to consumer.[90] The first condition is satisfied regardless of whether the personal information was generated internally or collected from another source.[91]

[33] Concerning the second condition, the Opinion asserted that in order to be disclosable, the personal information must be used to "create a profile about the consumer."[92] For example, a business may use information to derive a consumer's 9-digit zip code from a provided 5-digit zip code

[89] *Id.* at *6.

[90] 105 Ops. Cal. Att'y Gen. 26 (2022), 2022 WL 815641, at *6.

[91] *Id.*

[92] *Id*. at *7.

combined with other sources of information available to the business.[93] The Opinion explained further that "this would not give rise to a disclosable inference within the meaning of the statute."[94] However, whenever information is collected to predict, target, or affect consumer behavior, there would be a different result.[95] "[W]hen a business processes personal information to make an inference about the consumer's propensities, then the inference itself becomes part of the consumer's profile, and must be disclosed."[96]

[34] The Opinion discussed some of the various abuses of personal data, like Cambridge Analytica and Facebook, and focused on the purposes of the CCPA.[97] It acknowledged that "inferences appear to be at the heart of the problems that the CCPA seeks to address."[98] "[C]onsumers may never know that they are being excluded from seeing certain ads, offers, or listings based on discriminatory automated decisions. In almost every case, the source as well as the substance of these inferences is invisible to consumers."[99] The CCPA "gives consumers the right to receive all information collected 'about' [them], not just information collected from the consumer."[100] Whenever a "business creates (or buys or otherwise

[93] *Id.*

[94] *Id*.

[95] 105 Ops. Cal. Att'y Gen. 26 (2022), 2022 WL 815641, at *7.

[96] *Id.*

[97] *Id.* at *2, *7.

[98] *Id.* at *7.

[99] *Id.*

[100] 105 Ops. Cal. Att'y Gen. 26 (2022), 2022 WL 815641, at *8.

collects) inferences about a consumer, those inferences constitute a part of the consumer's unique identity and become part of the body of information that the business has 'collected about' the consumer" and must be disclosed upon request.[101]

[35] The Attorney General's extremely broad interpretation of "inferences drawn" likely provides protection against inferences that may not even exist under the GDPR.[102] California had the benefit of observing the growth of technology and its ramifications and was able to provide a significantly stronger definition of personal information that includes inferences drawn.[103] The Attorney General's Opinion emphasized the importance of that inclusion. California law now provides the strongest protection in the world against the ubiquitous collection of inferential data.

V. PROPOSED FEDERAL LEGISLATION

[36] On June 21, 2022, the American Data Privacy and Protection Act (ADPPA) was introduced in the House.[104] The bill contains considerably

[101] *Id.*

[102] *See* Wachter & Mittelstadt, *supra* note 3, at 494–95:

> "[I]nferences are effectively 'economy class' personal data in the [GDPR]. Data subjects' rights to know about . . ., rectify . . ., delete . . ., object to . . ., or port . . . personal data are significantly curtailed for inferences. The GDPR alsoprovides insufficient protection against sensitive inferences . . . or remedies to challenge inferences or important decisions based on them . . . [A] new data protection right, the 'right to reasonable inferences,' is needed to help close the accountability gap currently posed by 'high risk inferences[.]'"

[103] Blanke, *supra* note 3, 91–92.

[104] June Bill, *supra* note 37. A discussion draft of the bill had been released on June 3, 2022. *House and Senate Leaders Release Bipartisan Discussion Draft of Comprehensive Data Privacy Bill*, H. COMM. ON ENERGY & COM. (June 3, 2022),

more privacy protection than most privacy advocates would have predicted. It speaks of data minimization and duties of loyalty and privacy by design.[105] The bill provides for consumer data rights and data ownership and control.[106] It contains definitions for sensitive covered data, targeted advertising, and affirmative express consent.[107] It provides for a right to withdraw consent and to opt out of data transfers and targeted advertising.[108]

[37] The ADPPA even provides for required algorithm impact assessments and a limited private right of action.[109] However, the federal bill would, if enacted, preempt most state laws that pertain to privacy, including the "inferences drawn" provision of the CCPA, as well as the CPPA's ability to enforce both related rights given to California consumers and obligations placed on businesses that collect such data.[110]

---

https://energycommerce.house.gov/newsroom/press-releases/house-and-senate-leaders-release-bipartisan-discussion-draft-of [https://perma.cc/SHG6-9CE5]; To Provide Consumers with Foundational Data Privacy Rights, Create Strong Oversight Mechanisms, and Establish Meaningful Enforcement, 117th Cong. (2022) (discussion draft), https://energycommerce.house.gov/sites/democrats.energycommerce.house.gov/files/documents/Bipartisan_Privacy_Discussion_Draft_Bill_Text.pdf [https://perma.cc/JF35-6KF2] [hereinafter Discussion Draft]. A subsequent amended bill was later introduced on July 20, 2022. H.R. 8152, 117th Cong. (as reported by the H. Comm. on Energy and Com., July 20, 2022) [hereinafter July Bill].

[105] *See* June Bill, *supra* note 37, § 101(a).

[106] *See id.* § 203.

[107] *Id.* §§ 2(1), (24), (30).

[108] *Id.* § 204(a)–(c).

[109] *Id.* §§ 207(c), 403.

[110] *See generally* Emily Catron & Gary Kibel, *Federal data privacy legislation: Differences with state laws raise preemption issues*, REUTERS (Aug. 10, 2022, 10:19 AM), https://www.reuters.com/legal/legalindustry/federal-data-privacy-legislation-

[38] Most of the operative provisions of the ADPPA focus on "covered data." Covered data is "information that identifies or is linked or reasonably linkable, alone or in combination with other information, to an individual or a device that identifies or is linked or reasonably linkable to an individual, and may include derived data and unique identifiers."[111] The Discussion Draft definition for covered data stated that the term "does not include— (i) de-identified data; (ii) employee data; or (iii) publicly available information."[112] The June bill added and the July bill retained a fourth exclusion: "(iv) inferences made exclusively from multiple independent sources of publicly available information that do not reveal sensitive covered data with respect to an individual."[113] This conflicts with California's CCPA.

[39] The bill defines derived data as "covered data that is created by the derivation of information, data, assumptions, *correlations, inferences, predictions,* or conclusions from facts, evidence, or another source of information or data about an individual or an individual's device."[114] The Discussion Draft of the bill did not have the italicized language and it was unclear whether derived data would include inferences.[115] The italicized language added and retained in the June and July bills make it clear that

differences-with-state-laws-raise-preemption-2022-08-10/ [https://perma.cc/LNR6-ZDSJ] (detailing a basic overview of how the ADPPA will impact existing state laws).

[111] June Bill, *supra* note 37, § 2(8)(A).

[112] Discussion Draft, s*upra* note 104, § 2(8)(B).

[113] June Bill, *supra* note 104, § 2(8)(B)(iv); July Bill, *supra* note 104 § 2(8)(B)(iv).

[114] July Bill, *supra* note 104, § 2(13) (emphasis added).

[115] Discussion Draft, *supra* note 37, § 2(11).

inferences are included within the definition of derived data.[116] A problem, however, is that the bill's definition of covered data specifically excludes some inferences.

[40] Two questions arise. First, why does the bill specifically include inferences within the definition of derived data, but then exclude some of them within the definition of covered data? Second, what is anticipated to be excluded by potentially restricting terms like "exclusively," "multiple," "independent," and "publicly available information that do not reveal sensitive covered data?" While there is a satisfactory definition of sensitive covered data,[117] there is a somewhat circular reference in the definition of publicly available information as it pertains to covered data. The definition of publicly available information predictably includes things like government records, widely distributed media, and websites or online services made available to the public, but it also specifically excludes "any inference made exclusively from multiple independent sources of publicly available information that do not reveal sensitive covered data with respect to an individual"[118] – the very same language used in the exclusion to the definition of covered data.

[41] It is difficult to determine why the same language was added to both definitions and what the specific restricting descriptors were expected to accomplish. The exclusion would fail if the inference were any of the following: 1) not derived "exclusively," 2) not derived from "multiple" sources, 3) not derived from "independent sources," or 4) derived from "publicly available information that reveals sensitive covered data."[119] Does

[116] June Bill, *supra* note 104, § 2(11); July Bill, *supra* note 104, § 2(13).

[117] July Bill, *supra* note 104, § 2(28).

[118] *Id.* § 2(27)(B)(ii)(II).

[119] *Id.*

that mean that the inference "likely voter" would not be covered data if it was not inferred "*exclusively*" from "multiple independent sources," or if it was not inferred from "*multiple* independent sources," or if those sources were not "*publicly available*[?]" Presumably, if this bill were to advance, further editing of these definitions would be necessary. It is not clear if these exclusions are intended to broaden or narrow the scope of inferences as covered data.

[42] The most significant provision of the ADPPA is that it would preempt the vast majority of the CCPA as amended. The bill provides nineteen specific carve-outs to preemption, including one CCPA provision pertaining to security breaches, but otherwise preempts the entirety of the CCPA as amended.[120] Interestingly, the July bill added a provision regarding the existence of the CPPA, which stated "[n]otwithstanding any other provisions of law, the California Privacy Protection Agency established under 1798.199.10(a) of the California Privacy Rights Act may enforce this Act, in the same manner, it would otherwise enforce the California Consumer Privacy Act[.]"[121] While this may provide some solace as to the continued existence of the CPPA, unless the ADPPA is significantly amended, there will be less substance of the CCPA as amended for the CPPA to enforce, including the novel and potentially game-changing "inferences drawn" provision.

VI. WHY PREEMPTION MUST BE OPPOSED

[43] The CCPA as amended provides the strongest protection for information privacy ever before seen in the U.S. When the provisions added by the CPRA become effective in 2023, there will be an opportunity to see

[120] *Id.* § 404(b)(2)(A)–(S).

[121] *Id.* § 404(b)(3).

how a regulator (the CPPA) may be able to change long-standing practices regarding the collection and use of personal information. One of the strongest tools available to the CPPA will be the broad scope afforded by the inferences drawn language of the statute. It would be a shame to see this opportunity eliminated by preemption from a potentially weaker federal law.

[44] While it would certainly be preferable to have a federal law that provides significant information privacy and data protection, it is unlikely that we will see such a bill in the near future. It is doubtful whether any federal bill would provide the promise afforded by the CCPA as amended, along with enforcement by the CPPA.[122] There might be optimism about a strong federal law, but prior experience suggests otherwise.[123] It was not long ago that we saw many states use their laboratories[124] to pass anti-spam laws, only to see a much-lobbied, watered-down federal bill preempt their creative efforts.[125] In fact, by the time the CAN-SPAM Act of 2003 reached

[122] In fact, it is likely that the tech industry will support federal legislation like the ADPPA for the very purpose of preempting California's strict requirements. *See*, *e.g.*, W. Gregory Voss & Kimberly A. Houser, *Personal Data and the GDPR: Providing a Competitive Advantage for U.S. Companies*, 56 AM. BUS. L.J. 287 (2019) ("[The tech industry] would prefer to have the FTC enforce a watered-down federal privacy statute.").

[123] *See, e.g.*, Jordan M. Blanke, *Canned Spam: New State and Federal Legislation Attempts to Put a Lid on It*, 8 COMPUT. L. REV. & TECH. J. 305, 318 (2004) (discussing the long anticipated but disappointing CAN-SPAM Act of 2003).

[124] Sarah M. Morehouse & Malcolm E. Jewell, *States as Laboratories: A Reprise*, 7 ANN. REV. POL. SCI. 177, 177 (2004) ("In 1932, Supreme Court Justice Louis Brandeis coined the famous phrase 'laboratories of democracy' to refer to the states because he viewed them as sources of experimentation, with new solutions to social and economic questions. At that time, the states were responding to the birth of our industrial economy.").

[125] *See* Blanke, *supra* note 123, at 318.

a final vote in the United States Congress, 44 state attorneys general had announced that they would not support the bill because it would preempt the stronger laws already enacted in many states.[126]

[45] At the same time, states are finally beginning to push for change in data protection laws in the U.S. Beyond California, four more states including Virginia, Colorado, Connecticut, and Utah, have enacted privacy laws.[127] While not as strong as California's law, in part because they do not include specific reference to inferences drawn within their definitions[128], they do signal a call for change.

[46] Daniel Solove writes very convincingly about the shortcomings of rights-based enforcement of information privacy and data protection laws.[129] Most laws in the U.S., including the original CCPA and the four other state laws, rely on the enforcement of privacy rights by individuals.[130] This places a near impossible burden on individuals to keep up with the enormous amounts of data collected about them by a multitude of data processors.[131]

---

[126] *Id.* at 317.

[127] Virginia Consumer Data Protection Act, VA. CODE ANN. § 59.1-575 to -585 (2022); Colorado Privacy Act, COLO. REV. STAT. § 6-1-1301 to -1313 (2022); S.B. 6, 2022 Gen. Assemb., Reg. Sess. (Conn. 2022); Utah Consumer Privacy Act, UTAH CODE ANN. § 13-61-101 to -404 (LexisNexis 2022).

[128] *Compare* CAL. CIV. CODE § 1798.140(v)(1)(K) (Deering 2022) (including "inferences drawn" as an example of "personal data") *with* VA. CODE ANN. § 59.1-575 (2022) (missing any reference to inferential data in its definition section).

[129] Solove, *supra* note 3.

[130] *See, e.g.*, CAL. CIV. CODE § 1798.105–.125 (listing out only the rights that individuals may exercise in order to protect their personal information).

[131] Solove, *supra* note 3.

[47] Solove traces the history of rights-based privacy laws from the Federal Fair Credit Reporting Act to HEW's Fair Information Privacy Principles (FIPPs) and beyond to the various privacy laws that emerged in the 1970s and 1980s.[132] Solove discusses the South American ARCO rights of the 1990s, the EU's Data Protection Directive of 1995, and the General Data Protection Regulation of 2016.[133] He observes that not only do these laws "present individuals with an endless burden of chores,"[134] but they can also "lead to the unfair blaming of individual when they fail to exercise their rights."[135] These laws have "merely armed people with a tiny dagger to slay a vast army – a quest that is doomed to failure."[136] Solove highlights another problem regarding enforcement of privacy rights: unlike many other constitutional or statutory challenges whereby successes are applied to other individuals in similar circumstances, privacy victories often reward only the individual victor.[137] Everyone must fight their own battles. There is "no larger societal impact."[138]

[48] Sandra Wachter and Brent Mittelstadt have questioned whether the GDPR provides sufficient protection for inferences and argued for a right to reasonable inferences.[139] They wrote that "[i]ronically, inferences receive

[132] *Id.*

[133] *Id.*

[134] *Id.*

[135] *Id*.

[136] Solove, *supra* note 3.

[137] *Id*.

[138] *Id*.

[139] Wachter, *supra* note 3, at 580.

the least protection of all the types of data addressed in data protection law, and yet now pose perhaps the greatest risks in terms of privacy and discrimination."[140] In comparing the protection provided by the GDPR and by California law, California has a much tighter definition for inferences drawn because it had the benefit of time.[141] There is no question that "inferences derived from other pieces of personal information are considered themselves to be personal information."[142]

[49] Alicia Solow-Niederman writes persuasively about the emerging inference economy fueled by artificial intelligence and, in particular, machine language (ML), which "disempowers individuals about whom references are made, yet who have no control over the data sources from which the inferential model is generated."[143] "ML thus exposes the need to recognize two categories of data: one, personal data, and two, data that can be processed to make inferences about persons. Information privacy law today targets only the former category."[144] While scholars have applauded the expansion of coverage of inferences drawn in the CCPA, some still believe it is not enough.[145] "[T]his broader coverage does not represent a new strategy for how the information is regulated. Instead, the statute remains focused on individual rights. . .. This intervention, in the end, comes

[140] *Id.* at 575.

[141] Blanke, *supra* note 3, at 91–92.

[142] *Id.*

[143] Solow-Niederman, *supra* note 3, at 362.

[144] *Id.*

[145] *Id.* at 373–74.

down to the same linear approach of notice, consent, and control by the affected person." [146]

[50] Solove discusses the social nature of privacy and how interrelated personal data has become.[147] "In today's 'inference economy,' machine learning and other forms of algorithmic decision-making work by making inferences based on data sets. Everyone's data in the data set is used to make inferences, which are often then used to make decisions affecting people."[148]

[51] Regarding automated decisions, Solove writes:

> The GDPR focuses on "automated" decisions, but automation is not really the key feature of what makes certain decisions problematic. A more apt focus is on the use of inference in decisions. Inference involves using existing data to generate new data about a person or to make predictions about them. Inference, much more than automation, is what the law should regulate.

[52] The extremely broad interpretation of inferences drawn as personal information becomes even more important with the expanded rights provided by the CPRA. Under the CCPA as amended, businesses would be required to disclose all these inferred pieces of personal information whenever requested pursuant to a consumer's rights to delete personal

[146] *Id.* (I believe that Professor Solow-Niederman's article may have been written before the passage of the CRPA and it is possible that she may have different thoughts about the effectiveness of the CCPA as amended.).

[147] Solove, *supra* note 3.

[148] *Id.*

information, to correct inaccurate personal information, to know what personal information is being collected, to access personal information, to know what personal information is sold or shared and to whom, and to limit use and disclosure of sensitive information.[149]

[53] Even more importantly, however, the CCPA as amended now incorporates the principles of data minimization, purpose limitation, and storage limitation and requires that businesses ensure that their "collection, use, retention, and sharing of a consumer's personal information … be reasonably necessary and proportionate to achieve the purposes for which the personal information was collected or processed … and not further processed in a manner that is incompatible with those purposes."[150] There is now an agency in California charged with protecting the "fundamental privacy rights of natural persons with respect to the use of their personal information."[151] Starting in 2023, the CPPA will have the opportunity to not only help enforce the privacy rights asserted by individuals, but also to aggressively enforce the obligations imposed on businesses that collect personal information, including inferences drawn.[152] We may actually see the beginning of the kind of enforcement envisioned by scholars that does not rely solely upon the assertion of a given individual's rights.

[54] Finally, as we have seen when both the GDPR and the CCPA first became effective, everyone benefits from the trickle-down effect of changes made by businesses that attempt to comply with new laws, whether or not we are citizens of the EU or of California.

---

[149] CAL. CIV. CODE § 1798.100(a)(1)– (2) (Deering 2022).

[150] *Id.* § 1798.100(c).

[151] *Id.* § 1798.199.40(c).

[152] *Id.* § 1798.100.

VII. CONCLUSION

[55] California law provides unique protection for inferences. Even more so than the GDPR, it promises to provide an effective tool to combat the ubiquitous proliferation of inferential data collection and use in our inference economy. At least for the near future, it is unlikely that a federal bill will provide as broad a definition for personal information and inferences drawn as the one in the CCPA as amended. It is also unlikely that a federal bill would provide GDPR-like obligations on business to employ the principles of data minimization, purpose limitation, and storage limitation, nor an independent agency charged with the enforcement of these provisions. All of the provisions of California law will become fully effective on January 1, 2023.[153] Unless and until a federal bill provides the same important and powerful tools now emerging in California, any such bill must either specifically exempt the CCPA from preemption or be opposed. We are finally on the cusp of real change in data protection law in the U.S. and we must not permit the opportunity to be wasted.

[153] *CCPA vs CPRA: What's the Difference? supra* note 26.