California Data Privacy Law and Automated Decision-Making

Jena N. Lisowski*

* J.D. Candidate, The University of Iowa College of Law, 2024; B.A. Political Science, Luther College, 2020. I thank Bill Pipal and Alicia Solow-Niederman for encouraging my interest in data privacy law. I also thank the Volume 49 editors of the *Journal of Corporation Law*, especially Michael O'Rear, Adam Skendzel, Samantha Savala, and William Dix for their support throughout the editorial process.

I. INTRODUCTION

The United States lacks comprehensive data privacy legislation.[1] The California Privacy Rights Act (CPRA), effective January 1, 2023,[2] establishes greater protection for consumer data.[3] This Note focuses on the CPRA, specifically examining the balance between consumer data privacy protection and maintenance of a practical landscape for data controllers. Part II of this Note explores data privacy law in the United States generally and then focuses on California's efforts to provide consumers with a right against automated decision-making. Part III considers potential complications and interests at stake in restricting the use of automated decision-making. Part IV recommends that the California Privacy Protection Agency (CPPA) take steps in its rulemaking to effectively balance these interests. Part V concludes the discussion.

1. *See* Thorin Klosowski, *The State of Consumer Data Privacy Laws in the US (And Why It Matters)*, N.Y. TIMES (Sept. 6, 2021), https://www.nytimes.com/wirecutter/blog/state-of-privacy-laws-in-us [https://perma.cc/XK8P-F9BX] (stating that the United States historically "ha[d] a bunch of disparate federal [and state] laws" and that the United States "doesn't have a singular law that covers the privacy of all types of data" (second alteration in original)); Fredric D. Bellamy, *U.S. Data Privacy Laws to Enter New Era in 2023*, THOMSON REUTERS (Jan. 12, 2023), https://www.reuters.com/legal/legalindustry/us-data-privacy-laws-enter-new-era-2023-2023-01-12/ (on file with the *Journal of Corporation Law*) ("Historically[,] data privacy laws [in the United States] have been rooted in a 'harms-prevention-based' hodgepodge of privacy protections, seeking to prevent or mitigate harms in specific sectors.").

2. *See* CAL. CIV. CODE § 1798 (West 2024); *see also Frequently Asked Questions (FAQ)*, CAL. PRIV. PROT. AGENCY, https://cppa.ca.gov/faq.html [https://perma.cc/4YGE-E47P] ("The CPRA amendments to the CCPA went into effect on January 1, 2023.").

3. *See Frequently Asked Questions (FAQ)*, *supra* note 2 (stating that the CPRA "amended the CCPA[, California's initial privacy law passed in 2018 to protect consumers' personal information,] by adding additional consumer privacy rights").

II. BACKGROUND: THE DATA PRIVACY LANDSCAPE

A. Data Collection in the Shadow of Consumer Knowledge

For much of its existence, commercial use of personal data has largely gone unregulated.[4] The rise in popularity of mobile applications,[5] increasing internet presence,[6] and technological advancements in everything from cars to smart appliances has led to a generation of voluminously available consumer data.[7] This data obtains significant market

4. *See* Hossein Rahnama & Alex "Sandy" Pentland, *The New Rules of Data Privacy*, HARV. BUS. REV. (Feb. 25, 2022), https://hbr.org/2022/02/the-new-rules-of-data-privacy [https://perma.cc/P7ML-TNBE] ("For the past two decades, the commercial use of personal data has grown in wild-west fashion . . . . [and] the data economy was structured around a 'digital curtain' designed to obscure the industry's practices from lawmakers and the public."); Dmitri Shelest, *Insufficient Data Privacy Legislation Is Costing Companies: Three Ways Businesses Are Suffering*, FORBES (Dec. 22, 2022), https://www.forbes.com/sites/forbestechcouncil/2022/12/22/insufficient-data-privacy-legislation-is-costing-companies-three-ways-businesses-are-suffering/ [https://perma.cc/QGG7-V8X5] (noting a lack of data privacy protection in the United States); Nuala O'Connor, *Reforming the U.S. Approach to Data Protection and Privacy*, COUNCIL ON FOREIGN RELS. (Jan. 30, 2018), https://www.cfr.org/report/reforming-us-approach-data-protection [https://perma.cc/6MA9-UR3U] ("[R]ecord-shattering data breaches and inadequate data-protection practices have produced only piecemeal legislative responses at the federal level, competing state laws, and a myriad of enforcement regimes.").

5. *See* Peter Leonard, *Beyond Data Privacy: Data "Ownership" and Regulation of Data-Driven Business*, AM. BAR ASS'N (Jan. 17, 2020), https://www.americanbar.org/groups/science_technology/publications/scitech_lawyer/2020/winter/beyond-data-privacy-data-ownership-and-regulation-datadriven-business [https://perma.cc/HG7E-6LZN] (stating that "[s]martphone data is the richest enduring record of how, why, when, and where we act, go, think, see, and feel").

6. *See* Brian X. Chen, *The Battle for Digital Privacy Is Reshaping the Internet*, N.Y. TIMES (June 23, 2023), https://www.nytimes.com/2021/09/16/technology/digital-privacy.html [https://perma.cc/846R-K2TX] (noting that with the rise of the internet, advertising methods adapted to "track[people] from site to site by technologies such as 'cookies,' and . . . personal data was used to target [these people] with relevant marketing"); *Data Collection: Defining the Customer*, MASS. INST. TECH., https://web.mit.edu/ecom/www/Project98/G2/data.htm [https://perma.cc/J8V9-HB33] (explaining that web marketers collect data about consumers via the internet by both passive and active user data collection).

7. While popular discourse often focuses on smartphones as a source of data collection, many other items people regularly use collect personal data as well. *See, e.g.*, Byron Tau & Catherine Stupp, *California Opens Privacy Probe into Who Controls, Shares the Data Your Car Is Collecting*, WALL ST. J. (July 31, 2023), https://www.wsj.com/articles/california-privacy-agency-opens-probe-into-private-data-collected-by-cars-d17ec917 (on file with the *Journal of Corporation Law*) (stating that modern cars "are effectively connected computers on wheels" that are "able to collect a wealth of information via built-in apps, sensors, and cameras, which can monitor people both inside and near the vehicle"); Alfred Ng, *What Your Car Knows About You*, POLITICO (Aug. 2, 2022), https://www.politico.com/newsletters/digital-future-daily/2022/08/02/car-knows-about-you-data-collection-privacy-00049309 [https://perma.cc/9BCA-VB76] (reporting that cars "are capable of amassing data on nearly every aspect of a drive," that "there's a growing market for more personal driver data," and that "[c]ar location data is among the most valuable" that collectors can gather because it is "far more accurate and voluminous than phone data"); José Rodriguez, Jr., *Your New Car Is Watching You and Collecting Your Data*, JALOPNIK (June 23, 2023), https://jalopnik.com/your-new-car-is-watching-you-and-collecting-your-data-1850571329 [https://perma.cc/XX2H-YH39] (mentioning that "[m]odern cars have come to rival smartphones in terms of data collection" and that many cars are "sharing all your sensitive data," such as drivers' names, date and time of the driver's use of the vehicle, vehicle speed, acceleration and braking information, location and route data, and for some cars, even facial recognition and fingerprint data). As data collection skyrocketed, other common items began collecting personal data. *See, e.g.*, Daniel Wroclawski, *Smart Appliances Promise Convenience and Innovation. But Is Your Privacy Worth the Price?*, CONSUMER REPS. (July 24, 2023), https://www.consumerreports.org/electronics/privacy/smart-appliances-and-privacy-a1186358482

value when amassed and then analyzed into data sets that help businesses more accurately predict consumer preferences and insights.[8] Data controllers, the corporations with access to consumers' personal information, have often structured their operations in a data "black box," obscuring from the public what these companies do with consumer data.[9] However, as practices of the data market begin to surface, consumers and governments alike have recognized the need for greater data privacy protection.[10]

Consumer mistrust has spurred recent change in the data privacy landscape.[11] Companies' current practices of collecting and selling data are generally perceived by the

---

[https://perma.cc/6BRW-E49Z] (explaining that many household appliances, including refrigerators, washing machines, clothes dryers, ranges and cooktops, built-in microwaves, dishwashers, and ovens, can collect and share personal data); Tate Ryan-Mosley, *How to Hack a Smart Fridge*, MIT TECH. REV. (May 8, 2023), https://www.technologyreview.com/2023/05/08/1072708/hack-smart-fridge-digital-forensics [https://perma.cc/Z2VL-K9M3] (describing that internet-connected appliances, including thermostats, refrigerators, and televisions, are relatively easy to hack into and to extract "a treasure trove of personal details" from).

8. *See* Patience Haggin, *Personal Data Is Worth Billions. These Startups Want You to Get a Cut.*, WALL ST. J. (Dec. 4, 2021), https://www.wsj.com/articles/personal-data-is-worth-billions-these-startups-want-you-to-get-a-cut-11638633640 (on file with the *Journal of Corporation Law*) ("Personal data is behind the $455.3 billion digital-ad market."); Leslie K. John, Tami Kim & Kate Barasz, *Ads That Don't Overstep*, HARV. BUS. REV., Jan–Feb. 2018, at 62, 62 ("With users regularly sharing personal data online and web cookies tracking every click, marketers have been able to gain unprecedented insight into consumers and serve up solutions tailored to their individual needs."); Max Freedman, *How Businesses Are Collecting Data (And What They're Doing with It)*, BUS. NEWS DAILY (May 30, 2023), https://www.businessnewsdaily.com/10625-businesses-collecting-data.html [https://web.archive.org/web/20230807130910/https://www.businessnewsdaily.com/10625-businesses-collecting-data.html] ("Businesses may collect consumer data and use it to power better customer experiences and marketing strategies. They may also sell this data for revenue."); Sarah Spiekermann et al., *The Challenges of Personal Data Markets and Privacy*, 25 ELEC. MKTS. 161, 161 (2015) (stating that "[p]ersonal data can . . . become strategic capital that allows businesses to derive superior market intelligence or improve existing operations," and that "[b]usinesses can also build competitive advantage[s] or create market entry barriers by using personal information to lock customers in"); Meglena Kuneva, Eur. Consumer Comm'r, Eur. Comm'n, Keynote Speech at the Roundtable on Online Data Collection, Targeting, and Profiling (Mar. 31, 2009), https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_09_156 [https://perma.cc/UFQ5-BM6J] ("Internet is an advertisement supported service and the development of marketing based on profiling and personal data is what makes it go round. Personal data is the new oil of the internet and the new currency of the digital world.").

9. *See* Rahnama & Pentland, *supra* note 4 (noting the lack of transparency businesses have historically provided about their policies and procedures for handling consumers' personal information).

10. For example, a survey by the Pew Research Center found that most Americans surveyed "think their personal data is less secure now, that data collection poses more risks than benefits, and believe it is not possible to go through daily life without being tracked." Brooke Auxier et al., *Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information*, PEW RSCH. CTR. (Nov. 15, 2019), https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/ [https://perma.cc/MS3J-P8QD]. Pew Research also reports that 79% of Americans do not feel confident that companies will admit mistakes and take responsibility when compromising or misusing personal information. *Id.*

11. Pew Research reports that six in ten Americans believe "it is [not] possible to go through daily life *without having data collected about them* by companies or the government," and that 81% of Americans believe they have "very little or no control over" the data companies collect about them. *Id.* A separate survey by the Associated Press NORC Center for Public Affairs Research and MeriTalk indicates that the majority of Americans "don't believe their personal information is secure online and aren't satisfied with the federal government's efforts to protect it." Matt O'Brien, *Americans Have Little Trust in Online Security: AP-NORC*

public as intrusive and ethically suspect. Shoshana Zuboff, Professor emerita of the Harvard Business School, calls this "surveillance capitalism," or in other words, an "economic system built on the secret extraction and manipulation of human data."[12] Zuboff notes:

> [S]urveillance capitalism [i]s the unilateral claiming of private human experience as free raw material for translation into behavioral data. These data are then computed and packaged as prediction products and sold into behavioral futures markets—business customers with a commercial interest in knowing what we will do now, soon, and later.[13]

In sum, the use of consumer data has been largely obscure, to the benefit of data controllers. Zuboff further states that "[r]ight from the start . . . [corporations] understood that users were unlikely to agree to this unilateral claiming of their experience and its translation into behavioral data. It was understood that these methods had to be undetectable."[14] While average consumers had little to no understanding of how corporations collected and sold their data, businesses carried on these practices, profiting heavily.[15]

In recent years, as consumers discover that corporations frequently buy and use their data without consent, legislation restricting surveillance capitalism has gained traction.[16] The growing notion is that consumers own their personal data, and thus, companies in possession of this data should be restricted in the processing, use, and sale of it.[17] Where the data market once existed as an unregulated territory in which businesses freely gathered and economically exploited personal data, current legislative trends beginning in the European Union and stretching to the United States indicate the emergence of greater controls in the data market.[18]

Poll, ASSOCIATED PRESS (Sept. 16, 2021), https://apnews.com/article/technology-business-data-privacy-only-on-ap-4ff0652fac750b770a456c1177c54dc1 [https://perma.cc/P57H-9QYM].

12. Rahnama & Pentland, *supra* note 4.

13. John Laidler, *High Tech Is Watching You*, HARV. GAZETTE (Mar. 4, 2019), https://news.harvard.edu/gazette/story/2019/03/harvard-professor-says-surveillance-capitalism-is-undermining-democracy/ [https://perma.cc/8DJU-SN7M].

14. *Id.*

15. For example, one category of personal information often collected and sold is geolocation data. The New York Times reports that companies track geolocation data from approximately 200 million phones, which in turn facilitates a $21 billion secondary market for location data. Jennifer Valentino-DeVries et al., *Your Apps Know Where You Were Last Night, and They're Not Keeping It Secret*, N.Y. TIMES (Dec. 10, 2018), https://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html [https://perma.cc/54NR-43KV].

16. *See, e.g.*, Andrew Folks, *US State Privacy Legislation Tracker*, INT'L ASS'N OF PRIV. PROS. (Feb. 16, 2024), https://iapp.org/resources/article/us-state-privacy-legislation-tracker/ [https://perma.cc/QNH8-MW3M] (noting that as of February 2024, 13 states have enacted comprehensive data privacy laws and several other states have similar bills in various stages of the legislative process).

17. *See* Rahnama & Pentland, *supra* note 4 (discussing consumer desire for regulation restricting companies' abilities to process and use personal data).

18. *See infra* Part II.B (discussing the current legislative trends in the European Union).

B. The European Union's General Data Protection Regulation

The European Union has the leading framework for data privacy regulation.[19] The 1950 European Convention on Human Rights recognized that data privacy, as a right, deserves legal protection.[20] The European Union's privacy laws have changed as technology developed, first with the European Data Protection Directive of 1995.[21] The evolution of the internet and wide availability of data-producing technology later sparked a need for the General Data Protection Regulation (GDPR), which the European Parliament passed in 2016.[22] By May of 2018, the GDPR required all businesses interacting with E.U. citizens to exercise full compliance.[23]

The GDPR provides the most restrictive data privacy provisions in the world.[24] The law is expansive and provides few exceptions, and fines for violations can easily exceed tens of millions of euros.[25] The GDPR has a wide scope, applying to anyone who collects

---

19. The International Association of Privacy Professionals states that the "GDPR offers a framework for data protection with increased obligations for organizations" and that "its reach is far and wide." *EU General Data Protection Regulation*, INT'L ASS'N PRIV. PROS., https://iapp.org/resources/topics/eu-gdpr/ (last visited Sept. 24, 2023); *see also* Graham Greenleaf, *Now 157 Countries: 12 Data Privacy Laws in 2021/22*, 176 PRIV. L. & BUS.: INT'L REP., Apr. 2022, at 1, 1 (explaining that "most [new data privacy] laws are influenced substantially by the E.U.'s GDPR").

20. Convention for the Protection of Human Rights and Fundamental Freedoms and Protocol, Council of Eur., art. 8, Nov. 28, 1950, E.T.S. No. 5, https://www.echr.coe.int/documents/d/echr/Archives_1950_Convention_ENG [https://perma.cc/727N-RF6X] ("Everyone has the right to respect for his private and family life, his home and his correspondence."); *see generally Impact of the European Convention on Human Rights: Right to Privacy*, COUNCIL OF EUR., https://www.coe.int/en/web/impact-convention-human-rights/right-to-privacy [https://perma.cc/D5MC-QPV6] (discussing the effects of the European Convention on Human Rights on privacy protection).

21. Directive 95/46/EC, of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing Data and on the Free Movement of Such Data 1995 O.J. (L 281); *see also* Ben Wolford, *What Is GDPR, the E.U.'s New Data Protection Law?*, PROTON TECHS. AG, https://gdpr.eu/what-is-gdpr/ [https://perma.cc/8TEW-5SE9] (noting that the European Data Protection Directive of 1995 "establish[ed] minimum data privacy and security standards, upon which each member state based its own implementing law" to enhance legislation in light of modern technology).

22. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation) 2016 O.J. (L 119) 1 [hereinafter Regulation (EU) 2016/679]; *see also* Wolford, *supra* note 21 ("The GDPR entered into force in 2016 after passing European Parliament, and as of May 25, 2018, all organizations were required to be compliant.").

23. Regulation (EU) 2016/679, *supra* note 22, at art. 51, 84, 85, 88, 90 ("Each Member State shall notify to the Commission those provisions of its law which it adopts pursuant to [the GDPR] by 25 May 2018 and, without delay, any subsequent amendment affecting them."); Wolford, *supra* note 21.

24. *See, e.g.*, Wolford, *supra* note 21 ("The General Data Protection Regulation (GDPR) is the toughest privacy and security law in the world.").

25. Regulation (EU) 2016/679, *supra* note 22, at art. 83 (stating that penalties for some GDPR violations include fines of €10 million or up to 2% of a company's global revenue, whichever is greater, and that penalties for other GDPR violations include fines of the greater of €20 million or 4% of a company's global revenue); *see also What if My Company/Organisation Fails to Comply with the Data Protection Rules?*, EUR. COMM'N, https://commission.europa.eu/law/law-topic/data-protection/reform/rules-business-and-organisations/enforcement-and-sanctions/sanctions/what-if-my-companyorganisation-fails-comply-data-protection-rules_en [https://perma.cc/DK7G-WGLY] (explaining that fines for GDPR violations are determined based on "a number of factors such as the nature, gravity and duration of the infringement, its intentional or negligent character, any action taken to mitigate the damage suffered by individuals, [and] the degree of

or processes personal data of E.U. citizens or residents, or who offers products or services to these people.[26] This means that the GDPR can reach businesses physically located beyond the European Union, given that a business meets the other threshold requirements.[27]

The GDPR outlines basic rights for consumers to make decisions about their personal data. The eight basic rights are: (1) a right to be informed;[28] (2) a right of access;[29] (3) a right to rectification;[30] (4) a right to erasure;[31] (5) a right to restrict processing;[32] (6) a right to data portability;[33] (7) a right to object;[34] and (8) rights related to automated decision-

---

cooperation of the organization"); Niall McCarthy, *The Biggest GDPR Fines of 2022*, EQS GRP. (Jan. 31, 2023), https://www.eqs.com/compliance-blog/biggest-gdpr-fines [https://perma.cc/5YGC-DA5U] (stating that "GDPR fines are designed to make non-compliance around data security a costly mistake," and that determination of fines often centers around the seriousness of the violation).

26. Regulation (EU) 2016/679, *supra* note 22, art. 2–3 (listing the material and territorial scope of the GDPR); *Who Does the Data Protection Law Apply To?*, EUR. COMM'N, https://commission.europa.eu/law/law-topic/data-protection/reform/rules-business-and-organisations/application-regulation/who-does-data-protection-law-apply_en [https://perma.cc/6TLK-TXTZ].

27. *Who Does the Data Protection Law Apply To?*, *supra* note 26.

28. *See* Regulation (EU) 2016/679, *supra* note 22, at art. 13–14 (specifying that certain information must be provided where personal data is collected from a data subject and where personal data has not been obtained from the data subject); *see also GDPR: Right to Be Informed*, INTERSOFT CONSULTING, https://gdpr-info.eu/issues/right-to-be-informed [https://perma.cc/PG2U-RZQ6] ("[T]he General Data Protection Regulation (GDPR) gives individuals a right to be informed about the collection and use of their personal data, which leads to a variety of information obligations by the controller.").

29. *See* Regulation (EU) 2016/679, *supra* note 22, at art. 15 (listing right of access requirements); *see also GDPR: Right of Access*, INTERSOFT CONSULTING, https://gdpr-info.eu/issues/right-to-be-informed [https://perma.cc/PG2U-RZQ6] (explaining how data controllers subject to the GDPR must make information accessible to consumers).

30. *See* Regulation (EU) 2016/679, *supra* note 22, at art. 16 (stating the right to rectification); *see also Right to Rectification of Personal Data*, THOMSON REUTERS PRAC. L., https://uk.practicallaw.thomsonreuters.com/w-014-8203?transitionType=Default&contextData=(sc.Default)&firstPage=true [https://perma.cc/3Q4S-5FAE] (describing rectification as "[t]he right of an individual to have inaccurate or incomplete personal data corrected").

31. *See* Regulation (EU) 2016/679, *supra* note 22, at art. 17 (providing the right to erasure); *see also Right to Erasure, also Known as the "Right to Be Forgotten,"* THOMSON REUTERS PRAC. L., https://uk.practicallaw.thomsonreuters.com/w-014-8201?transitionType=Default&contextData=(sc.Default) [https://perma.cc/BCC8-LFF4] (explaining that the GDPR allows consumers "to request erasure of their personal data or information").

32. *See* Regulation (EU) 2016/679, *supra* note 22, at art. 18 (providing the right to restriction of processing); *see also Right to Restriction of Processing*, THOMSON REUTERS PRAC. L., https://uk.practicallaw.thomsonreuters.com/w-014-8204?transitionType=Default&contextData=(sc.Default) [https://perma.cc/NBS4-EXGS] (stating that the right allows consumers "to limit the way that a controller . . . uses their personal data").

33. *See* Regulation (EU) 2016/679, *supra* note 22, at art. 20 (noting the right to data portability); *see also Data Subject Rights Under the GDPR*, THOMSON REUTERS PRAC. L., https://uk.practicallaw.thomsonreuters.com/w-006-7553 [https://perma.cc/NT5Q-J9C2] (noting that data portability "give[s] data subjects more control . . . when switching from one service provider to another by allowing the data subject to easily move, copy, or transmit their personal data").

34. *See* Regulation (EU) 2016/679, *supra* note 22, at art. 21 (stating the right to object); *see also Right to Object to Processing*, THOMSON REUTERS PRAC. L., https://uk.practicallaw.thomsonreuters.com/w-014-8202?transitionType=Default&contextData=(sc.Default) [https://perma.cc/XE3A-GPD7] (summarizing that the right allows consumers "to object to the processing of their personal data or information in certain circumstances").

making and profiling.[35] The law contains seven primary data protection measures that processors must follow: (1) measures for transparency;[36] (2) use of data for limited purposes;[37] (3) data minimization;[38] (4) accuracy targets;[39] (5) storage limitations;[40] (6) integrity and confidentiality provisions;[41] and (7) accountability measures.[42] It also requires, in most circumstances, a consumer's affirmative opt-in consent before controllers can process the data.[43]

The GDPR brought pivotal change to data privacy law. Many European citizens better understand their privacy rights,[44] and have filed complaints with data protection authorities when companies violate those rights.[45] Other countries have followed the E.U. Member States' lead: 71% of countries have data protection legislation and 9% of countries currently have draft legislation.[46]

35. *See* Regulation (EU) 2016/679, *supra* note 22, at art. 22 (listing the right to automated individual decision-making, including profiling).

36. *See id.* at art. 12 (providing rights to transparent information for data subjects).

37. *See id.* at art. 5 (noting that personal data shall only be "collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes").

38. *See id.* (stating that personal data shall be "adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed").

39. *See id.* (providing that collected personal data shall be "accurate and, where necessary, kept up to date").

40. *See* Regulation (EU) 2016/679, *supra* note 22, at art. 5 (stating that personal data must be "kept in a form which permits identification of data subjects for no longer than in necessary for the purposes for which the personal data [is] processed").

41. *See id.* (noting that personal data must be "processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures").

42. *See id.* (stating that "[t]he controller shall be responsible for, and be able to demonstrate compliance with," the primary data protection measures outlined in the GDPR).

43. *See id.* ("Consent should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her . . . .").

44. The Fundamental Rights Survey conducted by the Fundamental Rights Agency reports that as of 2020, 69% of respondents over the age of 16 in the European Union knew of the GDPR, and that 51% were aware of a law that allows them to access their personal data from private companies. *Your Rights Matter: Data Protection and Privacy*, at 12–13 (June 18, 2020), https://fra.europa.eu/en/publication/2020/fundamental-rights-survey-data-protection [https://perma.cc/EZL7-HNAD]; *see also Communication from the Commission to the European Parliament and the Council: Data Protection as a Pillar of Citizens' Empowerment and the EU's Approach to the Digital Transition—Two Years of Application of the General Data Protection Regulation*, at 8, COM (2020) 264 final (June 24, 2020).

45. *See Commission Staff Working Document: Data Protection as a Pillar of Citizens' Empowerment and the EU's Approach to the Digital Transition—Two Years of Application of the General Data Protection Regulation*, at 20, SWD (2020) 115 final (June 24, 2020) (noting that between May 2018 and November 2019, consumers registered complaints in Germany (67,000), the Netherlands (37,000), Spain (18,000), France (18,000), Italy (14,000), Poland (12,000), and Ireland (12,000), among others).

46. *Data Protection and Privacy Legislation Worldwide*, U.N. CONF. ON TRADE & DEV., https://unctad.org/page/data-protection-and-privacy-legislation-worldwide [https://perma.cc/U9C9-YZKE].

C. Data Privacy Protection in the United States

Data privacy law in the United States has developed into a patchwork of state and narrowly-tailored federal laws.[47] Federal statutes come in three primary categories. The first category focuses "on the modality used to collect or transmit personally identifiable information."[48] These laws address narrow privacy issues. One example is the Telephone Consumer Protection Act of 1991, which regulates phone spamming and robocalls.[49] The second category relates to "the type of data collected and transmitted."[50] Laws in this category handle industry-specific data. An example is the Fair Credit Reporting Act, which addresses information about consumer credit history and identity.[51] The third category of federal data privacy laws aims to protect specific groups of people.[52] The Children's Online Privacy Protection Act, which excludes children from certain forms of data collection, is an example.[53] In sum, the landscape of data privacy legislation in the United States is most accurately defined as a patchwork of state and federal laws of a narrow scope, as opposed to the European Union's sweeping data privacy regulation.[54]

After the European Union enacted the GDPR, enthusiasm for data protection in the United States rose.[55] In 2018, the first state to implement its own data privacy statute was California, which loosely modeled its law on the GDPR's framework.[56] A handful of other states have since signed data privacy statutes into law, which went into effect as early as 2023.[57] State-level data privacy laws vary in the rights granted to consumers, but they

---

47. *Compare* Klosowski, *supra* note 1 (stating that "[t]he United States doesn't have a singular law that covers the privacy of all types of data. Instead, it has a mix of laws" that are "a cluttered mess of different sectoral rules"), *with European Union—Data Privacy and Protection*, INT'L TRADE ADMIN., https://www.trade.gov/european-union-data-privacy-and-protection [https://perma.cc/N98H-4Z54] (describing the GDPR as "comprehensive privacy legislation that applies across sectors and to companies of all sizes," "broad in scope," and "designed to provide a high level of privacy protection for personal data").

48. Stuart L. Pardau, *The California Consumer Privacy Act: Towards a European-Style Privacy Regime in the United States?*, 23 J. TECH. L. & POL'Y 68, 74 (2018).

49. Telephone Consumer Protection Act, 47 U.S.C. § 227.

50. Pardau, *supra* note 48, at 74.

51. Fair Credit Reporting Act, 15 U.S.C. § 1681.

52. Pardau, *supra* note 48, at 74.

53. Children's Online Privacy Protection Act, 15 U.S.C. § 6501.

54. *See supra* notes 1, 47 and accompanying text.

55. *See* Todd Ehret, *Data Privacy and GDPR at One Year, a U.S. Perspective. Part Two—U.S. Challenges Ahead*, THOMSON REUTERS (May 29, 2019), https://www.reuters.com/article/us-bc-finreg-gdpr-report-card-2/data-privacy-and-gdpr-at-one-year-a-u-s-perspective-part-two-u-s-challenges-ahead-idUSKCN1SZ1US [https://perma.cc/ZL57-N4S7] ("Without question, [the] GDPR set a new standard for privacy laws and the rest of the world has taken notice . . . . Although there have been calls for similar federal regulations on privacy in the United States, there has been little action at the federal level and a patchwork of state regulations is beginning to unfold.").

56. *See* CAL. CIV. CODE § 1798.100 (West 2024); *see also California Consumer Privacy Laws*, BLOOMBERG L., https://pro.bloomberglaw.com/brief/california-consumer-privacy-laws-ccpa-cpra [https://perma.cc/8P2R-Q4EN] (stating that the CCPA was "the first comprehensive consumer privacy legislation in the U.S.").

57. In 2023, the California Privacy Rights Act, largely an expansion of the existing California Consumer Privacy Act, went into effect, as well as data privacy legislation in Virginia, Colorado, Connecticut, and Utah. Folks, *supra* note 16. As of February 2024, more states (including Iowa, Delaware, Indiana, Montana, and Oregon) have signed laws, and others (including Minnesota, Illinois, New York, Pennsylvania, and Maryland) have bills moving through the legislative process. *Id.*

generally share certain characteristics, such as the right to access collected data from a business.[58] Along with providing rights for consumers, state-level data privacy laws contain requirements for data controllers.[59]

D. California: A Leader in U.S. Data Privacy Law

California leads the United States in data privacy law innovation. The state enacted the California Consumer Privacy Act (CCPA) in 2018.[60] Not only is the CCPA the first state-level data privacy law in the United States, but its applicability has so far been the widest.[61] Businesses that meet the threshold applicability criteria must provide CCPA rights for all consumers who are California residents.[62] The law contains six basic rights for consumers: (1) the right to know about personal information that a business collects about consumers and how that information is used or shared;[63] (2) the right to delete collected personal information;[64] (3) the right to opt-out of the sale or sharing of personal information;[65] (4) the right for children to opt-in to data collection;[66] (5) the right to non-retaliation for exercising data privacy rights;[67] and (6) a private right of action in the case of a data breach.[68]

California signed the California Privacy Rights Act (CPRA) in 2020, and the law went into effect on January 1, 2023.[69] The CPRA changed the applicability requirements from those in the CCPA. This means that a business will need to meet at least one of the following for the law to apply: (1) have $25 million in annual gross revenues as of January 1 of the preceding calendar year; (2) buy, sell, or share the personal information of 100,000 California consumers; or (3) derive 50% or more of its revenues from selling or sharing personal information.[70] Further, the CPRA established the California Privacy Protection

58. *See generally* INT'L ASS'N OF PRIV. PROS., US STATE PRIVACY LEGISLATION TRACKER: COMPREHENSIVE CONSUMER PRIVACY BILLS 1 (2023).

59. *Id.*

60. *California Consumer Privacy Laws*, *supra* note 56.

61. *Id.* (stating that the CCPA "created an array of consumer privacy rights and business obligations related to the collection and sale of personal information").

62. *See* CAL. CIV. CODE § 1798.140 (West 2024) (listing the threshold criteria that qualifies an organization as a "business" under the CCPA).

63. *Id.* §§ 1798.110, .115.

64. CAL. CIV. CODE § 1798.105 (West 2024).

65. CAL. CIV. CODE § 1798.120(a) (West 2024).

66. CAL. CIV. CODE § 1798.120(c) (West 2024) (stating that a business cannot sell or share information about a consumer if the business has actual knowledge that the consumer is less than 16 years old, unless (1) the consumer is at least 13 years old and opts-in, or (2) the consumer is younger than 13 years old but has a parent or guardian authorize an opt-in on the consumer's behalf).

67. *Id.* § 1798.125.

68. *See* CAL. CIV. CODE § 1798.150 (West 2024) (providing a private right of action in the case of personal information security breaches when "unauthorized access and exfiltration, theft, or disclosure [of consumer data] . . . result[s because] of the business's violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information").

69. *Frequently Asked Questions (FAQs)*, CAL. PRIV. PROT. AGENCY, https://cppa.ca.gov/faq.html [https://perma.cc/AXG5-2F3C]; *see California Consumer Privacy Act (CCPA)*, CAL. DEP'T OF JUST. OFF. OF THE ATT'Y GEN. (May 10, 2023), https://oag.ca.gov/privacy/ccpa#sectionc [https://perma.cc/T3UA-SP6V] (noting that in November of 2020, "California voters approved Proposition 24, the CPRA, which amended the CCPA and added new additional privacy protections").

70. CAL. CIV. CODE § 1798.140(d)(1)(A)–(C) (West 2024).

Agency (CPPA), a regulatory body with rulemaking and enforcement authority.[71] Rulemaking authority was transferred from California's Office of the Attorney General to the CPPA on April 21, 2022.[72] The CPRA maintains the six primary rights of the CCPA, and will likely lead to the addition of new rights, including the right to opt-out of automated decision-making technology.[73]

In the CPRA, the California legislature did not elaborate on what the right to opt-out of automated decision-making will entail.[74] Most likely, a consumer can request that controllers be prevented from using their information in systems that analyze personal data without human intervention for the purposes of profiling or implementing targeted advertisements. However, the CPPA has not detailed what the automated decision-making restriction will involve and how far its scope will extend.

As of March 1, 2024, the CPPA has engaged in preliminary rulemaking activities to address cybersecurity audits, risk assessments, and automated decision-making.[75] The preliminary public comment period closed on March 27, 2023, and the CPPA's rulemaking process is ongoing.[76]

III. THE RIGHT AGAINST AUTOMATED DECISION-MAKING

Data controllers and consumers will likely seek guidance on the scope and specificity of the right against automated decision-making. The CPPA's current rulemaking procedures address automated decision-making.[77] This Part assesses potential complications with this right. Specifically, this Part analyzes the explainability of algorithms, the scope of the term "solely automated," multi-step decision-making systems, automated decisions in high-risk activities, bias in algorithms, and the inherent tension points between artificial intelligence and law.

---

71. *See generally About CPPA*, CAL. PRIV. PROT. AGENCY, https://cppa.ca.gov/about_us [https://perma.cc/XQ4E-RQHX] (describing the structure of the CPPA).

72. CAL. CIV. CODE § 1798.199.10 (West 2024) (establishing the CPPA); *Meet the California Privacy Protection Agency (CPPA)*, OSANO (July 27, 2022), https://www.osano.com/articles/california-privacy-protection-agency [https://perma.cc/V5MP-YZYM].

73. The CPRA does not expressly list a right against automated decision-making. However, it establishes the CPPA and gives the agency the scope to "[i]ssu[e] regulations governing access and opt-out rights with respect to businesses' use of automated decision-making technology." CAL. CIV. CODE § 1798.185(a)(16) (West 2024). The agency has conducted rulemaking to address automated decision-making. *See Preliminary Rulemaking Activities on Cybersecurity Audits, Risk Assessments, and Automated Decisionmaking*, CAL. PRIV. PROT. AGENCY, https://cppa.ca.gov/regulations/pre_rulemaking_activities_pr_02-2023.html [https://perma.cc/ENX9-GG74].

74. *See supra* note 73 and accompanying text.

75. *Preliminary Rulemaking Activities on Cybersecurity Audits*, *supra* note 73.

76. *Id.*

77. The CPPA's Invitation for Preliminary Comments asks the public to advise on issues related to access and opt-out rights concerning businesses' use of automated decision-making technologies. CAL. PRIV. PROT. AGENCY, INVITATION FOR PRELIMINARY COMMENTS ON PROPOSED RULEMAKING: CYBERSECURITY AUDITS, RISK ASSESSMENTS, AND AUTOMATED DECISION-MAKING 1–3 (2023), https://cppa.ca.gov/regulations/pdf/invitation_for_comments_pr_02-2023.pdf [https://perma.cc/VT59-88XS].

A. The Difficulty of Explainability

Because California's data privacy law loosely tracks the E.U.'s GDPR, the CPPA may look to European legislation to define California's right against automated decision-making. The GDPR includes a right of explanation along with its right against automated decision-making.[78] Some interpret the additional right to require that companies explain how their algorithms reach the eventual results.[79] In other words, this argument highlights that the GDPR encourages companies to provide information about the algorithms their automated decision-making systems use. The rationale is that with transparency in the automated decision-making processes, consumers can assess for themselves whether a company has made an inaccurate or biased decision with the consumer's personal data.[80]

Proponents of including a right to explainability in data privacy legislation generally state that providing this information will help ensure that the decision-making process is fair.[81] For example, giving a data subject an explanation about how that person's data is used and processed may aid that individual in understanding how the automated system reached its eventual decision.[82] Various methods of explainability include process-based disclosures (giving information about the design of the automated system) and outcome-based disclosures (helping users understand how the system reached its eventual result).[83]

---

78. *See* Regulation (EU) 2016/679, *supra* note 22, at art. 13 § 2(f) (stating that "meaningful information about the logic involved" must be provided where data is subject to automated decision-making); *id.* at recital 71 ("[P]rocessing should be subject to suitable safeguards, which should include . . . [the right] to obtain an explanation of the decision reached . . . ."); Andrew D. Selbst & Julia Powles, *Meaningful Information and the Right to Explanation*, 7 INT'L DATA PRIV. L. 233, 233 (2017) ("Articles 13–15 provide rights to 'meaningful information about the logic involved' in automated decisions. This is a right to explanation . . . .").

79. University of Oxford scholars Bryce Goodman and Seth Flaxman provide one of the predominant interpretations of the GDPR's right to explanation. They note, "[A]n algorithm can only be explained if the trained model can be articulated and understood by a human . . . [which] at a minimum, provide[s] an account of how input features relate to predictions, allowing one to answer questions [about the AI's reasoning]." Bryce Goodman & Seth Flaxman, *European Union Regulations on Algorithmic Decision-Making and a "Right to Explanation*," AI MAG., Fall 2017, at 50, 55; *see also* Selbst & Powles, *supra* note 78, at 235 (discussing the right to explanation).

80. Bryan Casey, Ashkon Farhangi & Roland Vogl, *Rethinking Explainable Machines: The GDPR's "Right to Explanation" Debate and the Rise of Algorithmic Audits in Enterprise*, 34 BERKELEY TECH. L.J. 143, 149 (2019) ("Many view the GDPR's 'right to explanation' as a promising new mechanism for promoting fairness, accountability, and transparency in a world pervaded by complex algorithmic systems that can be difficult for observers to understand."); *AI and the Right to an Explanation*, DPO CTR. (Jan. 24, 2022), https://www.dpocentre.com/ai-and-the-right-to-an-explanation/ [https://perma.cc/SV46-XHB4] ("Providing data subjects with an explanation is important as individuals have the right to be informed of how their personal data is being processed, particularly when there is the existence of solely automated decision-making . . . .").

81. *See supra* note 80 and accompanying text (listing arguments for and proponents of explainability rights).

82. *See generally AI and the Right to an Explanation*, *supra* note 80 (exploring arguments in favor of a right to explanation).

83. *See* INFO. COMM'R'S OFF. & THE ALAN TURING INST., EXPLAINING DECISIONS MADE WITH AI 23 (2020), https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/artificial-intelligence/explaining-decisions-made-with-artificial-intelligence/ [https://perma.cc/G9X2-AEL6] (defining process-based explanations as "demonstrating that [the data controller has] followed good governance processes and best practices" in using consumer data, and defining outcome-based explanations as "clarifying the results of a specific decision," which involves "explaining the reasoning behind a particular algorithmically-generated outcome in plain, easily understandable, and everyday language").

However, the right of explainability has been fraught with difficulty in its implementation, complicating a potential American model in this area of law.[84] Many algorithms constantly change. The AI that powers automated decision-making systems often functions with algorithms that adapt as the system interprets new data.[85] Nick Wallace, a Brussels-based policy analyst, notes that "the challenge of explaining an algorithmic decision comes not from the complexity of the algorithm, but the difficulty of giving meaning to the data it draws on."[86] AI foundation models initially train using a single system with large data sets and then adapt as needed with the input of new data.[87] The system does this by using deep neural networks, described as a complex version of pattern matching.[88] Thus, a model exposed to a larger amount of data learns how to form more complex patterns and correlations.[89] The system's changing nature means that enabling a right to explainability, such as that in the GDPR, becomes difficult if not impossible to implement in practice.[90]

---

84. *See* Casey, Farhangi & Vogl, *supra* note 80, at 158 (stating that, as late as 2019, "much uncertainty continues to shroud the Regulation's so-called 'right to explanation'" and that "the precise contours of the 'right to explanation' have been the subject of much speculation—giving rise to an 'explosive' debate").

85. *See* Sara Brown, *Machine Learning, Explained*, MASS. INST. TECH. MGMT.: SLOAN SCH. (Apr. 21, 2021), https://mitsloan.mit.edu/ideas-made-to-matter/machine-learning-explained [https://perma.cc/R7ZX-7T4R] ("Machine learning takes the approach of letting computers learn to program themselves through experience."). Brown notes that many companies use machine learning to tailor recommendation algorithms, image analysis and object detection, and fraud detection, among other services. *Id.*

86. Nick Wallace, *EU's Right to Explanation: A Harmful Restriction on Artificial Intelligence*, TECHZONE360 (Jan. 25, 2017), https://www.techzone360.com/topics/techzone/articles/2017/01/25/429101-eus-right-explanation-harmful-restriction-artificial-intelligence.htm [https://perma.cc/WP5T-WZ64].

87. *See* Aaron J. Snoswell & Dan Hunter, *Robots Are Creating Images and Telling Jokes: 5 Things to Know About Foundation Models and the Next Generation of AI*, THE CONVERSATION (Apr. 13, 2022), https://theconversation.com/robots-are-creating-images-and-telling-jokes-5-things-to-know-about-foundation-models-and-the-next-generation-of-ai-181150 [https://perma.cc/WBW3-5XGG] (explaining how AI systems are trained); *Artificial Intelligence (AI) vs. Machine Learning*, COLUMBIA UNIV.: THE FU FOUND. SCH. OF ENG'G & APPLIED SCI., https://ai.engineering.columbia.edu/ai-vs-machine-learning/ [https://perma.cc/PN5K-V3WQ] (explaining that algorithms train by machine learning, which "refers to the technologies . . . that enable systems to identify patterns, make decisions, and improve themselves through experience and data"); Brown, *supra* note 85 (describing machine learning as "a subfield of artificial intelligence that gives computers the ability to learn without explicitly being programmed").

88. Snoswell & Hunter, *supra* note 87; *see also* Brown, *supra* note 85 (describing neural networks as programs "modeled on the human brain, in which thousands or millions of processing nodes are interconnected and organized into layers" and deep learning networks as "neural networks with many layers . . . [that] can process extensive amounts of data and determine the 'weight' of each link in the network").

89. Snoswell & Hunter, *supra* note 87; *see* Karen Hao, *What Is Machine Learning?*, MASS. INST. TECH.: TECH. REV. (Nov. 17, 2018), https://www.technologyreview.com/2018/11/17/103781/what-is-machine-learning-we-drew-you-another-flowchart [https://perma.cc/Q98G-SPZF] ("Deep learning is machine learning on steroids: it uses a technique that gives machines an enhanced ability to find—and amplify—even the smallest patterns. This technique is called a deep neural network—deep because it has many, many layers of simple computational nodes that work together to munch through data and deliver a final result in the form of the prediction.").

90. Brown, *supra* note 85 ("One area of concern is . . . explainability, or the ability to be clear about what the machine learning models are doing and how they make decisions."); *What is Explainable A.I.?*, IBM, https://www.ibm.com/topics/explainable-ai [https://perma.cc/QW5H-HNZL] ("As AI becomes more advanced, humans are challenged to comprehend and retrace how the algorithm came to a result. The whole calculation process is turned into what is commonly referred to as a 'black box' that is impossible to interpret. These black box models are created directly from the data. And, not even the engineers or data scientists who create the

Even if feasible, transparency of an automated decision-making system's code would likely provide a low return for consumers. When people explain how an individual makes a decision, they often rely on explanations that lay out logical steps and rules. When humans see an explanation step-by-step, they can trace how a particular individual reaches a specific conclusion. By contrast, transparency in AI does not function in the same manner. For example, the machine-learning tool SearchInk can examine handwritten documents and predict whether a name is attributed to a male or female writer based not on the name itself, but rather, on the order of the writer's pen strokes.[91] While SearchInk's predictions fall within 80% accuracy, Harald Gölles, the startup's Chief Technology Officer and co-founder, states that "something in the handwriting . . . reveals what the writer knows about the subject, such as whether a person is male or female" and that "the machine can spot it."[92] Nonetheless, when trying to explain how the AI determines this, SearchInk's employees "don't even know what it is."[93] Wallace notes that this issue extends beyond the AI at SearchInk:

> [The problem] is not because the algorithm is a "black box," but [is instead] because [it] cannot make specific claims about the relationship between psychology and graphology. An algorithm can spot a correlation, but it cannot explain the link between [the data and the ultimate decision] because it cannot infer meaning the way a human can. AI can only imitate human semantics . . . it does not actually understand anything.[94]

The nature of constantly evolving AI systems means that explaining how the code makes its decisions in some cases is not possible. Even if an explanation of AI systems were possible, average consumers may not understand the explanations without an extensive understanding of AI technology.[95]

---

algorithm can understand or explain what exactly is happening inside them or how the AI algorithm arrived at a specific result."); Jessica Newman, Commentary, *Explainability Won't Save AI*, BROOKINGS (May 19, 2021), https://www.brookings.edu/articles/explainability-wont-save-ai/ [https://perma.cc/LT75-FTU] (noting that the explainable AI field "has generally struggled to realize the goals of understandable, trustworthy, and controllable AI in practice" in part because "it [is] difficult to provide explanations to end-users because of . . . the challenges of providing real-time information of sufficiently high quality").

91. Wallace, *supra* note 86; *see* Mike Butcher, *SearchInk—Unlocking the Handwritten Past, and Present, with Machine Learning*, TECHCRUNCH (Nov. 17, 2016), https://techcrunch.com/2016/11/17/searchink-unlocking-the-handwritten-past-and-present-with-machine-learning [https://perma.cc/H9X5-4EKU] (discussing SearchInk's machine learning technology); Nick Wallace, *5 Q's for Harald Gölles, CTO and Co-Founder of SearchInk*, CTR. FOR DATA INNOVATION (Nov. 25, 2016), https://datainnovation.org/2016/11/5-qs-for-harald-golles-cto-of-searchink [https://perma.cc/VDY8-E8GU] (providing information about SearchInk's technology).

92. Wallace, *supra* note 91.

93. *Id.*

94. Wallace, *supra* note 86.

95. *See, e.g.*, Jarek Gryz & Marcin Rojszczak, *Black Box Algorithms and the Rights of Individuals: No Easy Solution to the "Explainability" Problem*, 10 INTERNET POL'Y REV. 1, 10 (2021) (citing one issue with the right to explainability as "the average individual's lack of knowledge and expertise in analysing and evaluating the very complex results of operations carried out by advanced [machine learning] algorithms, where highly specialized knowledge is needed").

Further, a right to explanation would likely implicate concerns related to the protection of trade secrets.[96] In calibrating the law's weight on consumer data privacy interests, affording an expansive transparency requirement may hinder a company's protection of its trade secrets.[97] Doshi-Velez et al. suggest that requiring a sweeping right to explanation of AI systems "would stifle innovation" because "explanations might force trade secrets to be revealed."[98] However, if incorporated in California's data privacy framework, the right to explanation could be fulfilled by "legally-operative explanations" that provide sufficient explanations for consumers without revealing trade secrets related to the contents of the AI.[99]

B. Scope of the Term "Solely Automated"

Determining the scope of the term "solely automated" adds a layer of complexity in defining the right against automated decision-making. The CPPA must indicate how far it will extend the definition of "automated" as it relates to automated decision-making systems. By comparison, Article 22 of the GDPR restricts the right against automated decision-making systems to cases that are solely automated and have legal or similarly significant effects, referring to the automated decision-making systems that use inputted data to make a decision without any interference from a human.[100] The CPPA could limit the CPRA's right against automated decision-making to situations where the system is "solely automated," but on its own, this likely will not assist consumer protection measures because many decision-making systems incorporate human involvement at least to some degree.

The European Data Protection Board (EDPB) has raised concerns with the "solely automated" approach in the European Union, noting that it opens the door to the "token

96. *See* Katarina Foss-Solbrekk, *Three Routes to Protecting AI Systems and Their Algorithms Under I.P. Law: the Good, the Bad, and the Ugly*, 16 J. INTELL. PROP. L. & PRAC. 247, 247 (2021) ("Because trade secret protection subsists for as long as the information remains confidential and requires actors to take steps to ensure confidentiality, trade secret protection facilitates algorithmic opacity."); Ryan N. Phelan, *Artificial Intelligence & the Intellectual Property Landscape*, MARSHALL, GERSTEIN & BORUN LLP (Sept. 2019), https://www.marshallip.com/insights/artificial-intelligence-the-intellectual-property-landscape/ [https://perma.cc/9SRY-ZZEW] ("AI algorithms and data are entitled to state and federal protection as trade secrets."); Niovi Plemmenou, *Protecting Algorithms as Trade Secrets. Time for Change?*, LEGAL COMPASS (Feb. 2, 2022), https://www.thelegalcompass.co.uk/post/protecting-algorithms-as-trade-secrets-time-for-change [https://perma.cc/XY4V-XUHC] (discussing the competing interests between a right to explanation and the protection of algorithms as trade secrets).

97. *See* sources cited *supra* note 96 and accompanying text (discussing the tension between transparency requirements and trade secret protections).

98. Finale Doshi-Velez et al., *Accountability of AI Under the Law: The Role of Explanation* 3 (Berkman Klein Ctr. Working Grp. on AI Interpretability, Working Paper, 2017).

99. *Id.* at 12–14.

100. Regulation (EU) 2016/679, *supra* note 22, at art. 22 (stating that consumers "shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her"); *see generally* Reuben Binns & Michael Veale, *Is That Your Final Decision? Multi-Stage Profiling, Selective Effects, and Article 22 of the GDPR*, 11 INT'L DATA PRIV. L. 319 (2021) (detailing how "[l]ittle attention has been paid to Article 22 in light of decision-making processes with multiple stages," and providing examples of "complications relating to interpreting Article 22 in the context of such multi-stage profiling systems").

human" problem.[101] If companies want to avoid the "solely automated" limitations while remaining maximally cost-effective, they may implement a human in merely a small step of a predominantly automated decision-making process. If that human does not interact meaningfully in the decision-making process, then they act merely as a "token," providing little benefit for consumer protection while allowing the company to circumvent GDPR obligations.[102] The EDPB suggests that when businesses incorporate a human step to these systems, the person should "be in a position to independently evaluate the case and assess the outputs of the system" if the company plans to avoid categorization of its AI as a "solely automated" system.[103] For example, a person involved in this process should have authority in the decision-making process, which could include having the ability to overturn outputs or to consider additional information or mitigating factors that may change the outcome of the decision.[104] Most European Union member states have adopted this approach.[105] If the CPPA models its regulations off of the GDPR, the CPPA should structure the scope of the term "solely automated" so that it prevents businesses from enacting "token human" systems.

C. Multi-Stage Decision-Making Systems

AI often uses multi-stage decision-making systems.[106] Rather than inputting a single piece of data to receive a single output, AI systems generally function with steps involving both AI and humans making decisions, which can blur the definition of "solely automated" AI.[107]

There are three main models for multi-stage decision-making systems: supporting, triaging, and automatic summarization.[108] In the supporting model, AI provides information to a human decision-maker, who then determines the output.[109] An example is the Correctional Offender Management Profiling for Alternative Sanctions (COMPAS) system used by judges to assess bail and parole conditions. Through COMPAS, cases are assigned a recidivism-risk score, and this information is relayed to a human, who

101. *See* Binns & Veale, *supra* note 100, at 320–21 (discussing the degree of human oversight that could render automated decisions not "solely automated").

102. *Id.*

103. *Id.* at 320.

104. *See id.* (noting ways that a human can meaningfully be involved in the decision-making process to avoid a mere "token human" situation in a system that, in effect, is "solely automated").

105. *Id.*

106. *See, e.g.*, Wenjun Kou et al., *A Multi-Stage Machine Learning Model for Diagnosis of Esophageal Manometry*, 124 A.I. MED. 1 (2022) (discussing the use of multi-stage algorithms for medical diagnosis); Jochen Baier et al., *A Multi-Stage AI-Based Approach for Automatic Analyzation of Bike Paths: Stage 1 – Road Surface Detection*, 682 IFIPAICT 70, 70 (2023) (explaining how a three-stage AI system detects surface conditions of bicycle paths); Andy Markus, *Harnessing Data and AI for Business Value*, AT&T BLOG (Aug. 9, 2022), https://about.att.com/innovationblog/2022/data-ai-part-1.html [https://perma.cc/3M75-NFNN] (noting that AT&T uses a "multi-stage AI-based fraud management tool" to examine transactions).

107. *See, e.g.*, Joe McKendrick & Andy Thurai, *AI Isn't Ready to Make Unsupervised Decisions*, HARV. BUS. REV. (Sept. 15, 2022), https://hbr.org/2022/09/ai-isnt-ready-to-make-unsupervised-decisions [https://perma.cc/9MHD-BL38] (mentioning circumstances where decision-making systems use both algorithms and human decision-makers).

108. *See* Binns & Veale, *supra* note 100, at 322–23.

109. *Id.*

determines which sentencing criteria each score warrants.[110] In the triaging model, the AI sorts which cases go to a human for decision-making and which move to additional automated processes.[111] The TSA's Secondary Security Screening Selection process is an example. The AI processes information about airline passengers, triaging whether each person receives a typical boarding pass or whether the case is passed to a human, who may in turn decide whether the person receives a typical boarding pass or one subject to enhanced security screening measures.[112] Automated summarization aggregates multiple decisions that a human inputs.[113] The optical scanning process used at polling stations to count votes is an example. In these systems, a scanner detects the inputted votes from each ballot and assigns votes to the corresponding candidates.[114]

Multi-stage systems complicate rulemaking regarding automated decision-making. First, it may be difficult to locate where a decision occurs. For example, in a triaging model, it may be unclear whether to assign the bulk of responsibility for the decision to the AI (which made the first determination in the system), or whether to attribute the decision to the human involved (who received the information from the AI and made a subsequent decision). In other words, one could reasonably argue that the human made the final decision in the process; at the same time, one could reasonably argue that but for the AI's initial determination to triage an individual case, the second decision—the decision made by the human—would not have occurred.[115] Because of this, when assigning accountability to a decision-maker for biased or inaccurate decisions *ex post*, multi-stage systems cloud the determination of whether the AI or a human should bear responsibility for the result.

When an error occurs in a multi-step decision-making system, accountability often lands largely on the person involved in the decision-making process—regardless of whether they had a significant influence on the outcome. Madeleine Clare Elish penned this the dilemma of the "moral crumple zone," in which human operators become "'liability sponges' . . . to fill the gaps in accountability that may arise in the context of new and complex systems."[116] Cars protect drivers by incorporating a controlled portion in the vehicle known as a crumple zone to absorb the majority of an impact. A "moral crumple zone" in the automated decision-making context similarly arises when "responsibility for an action [is] misattributed to a human actor who had limited control over the behavior of an automated or autonomous system."[117] Elish explains that "accountability appears to be

110. *See* Andrew Lee Park, *Injustice Ex Machina: Predictive Algorithms in Criminal Sentencing*, UCLA L. REV.: LAW MEETS WORLD (Feb. 19, 2019), https://www.uclalawreview.org/injustice-ex-machina-predictive-algorithms-in-criminal-sentencing/ [https://perma.cc/QYD9-RWEM] (explaining the mechanics of the COMPAS system).

111. Binns & Veale, *supra* note 100, at 322–23.

112. *Id.* at 322. TSA does not publish specific information about how the SSSS algorithm functions or what criteria it weights in decision-making; however, Binns and Veale indicate that its AI uses triaging methods. *Id.*

113. *Id.* at 322–24.

114. *See Elections and Technology*, ACE PROJECT, https://aceproject.org/ace-en/topics/et/eth/eth02/eth02b/eth02b2 [https://perma.cc/U469-FLQC] (describing how optical scanning systems function).

115. Binns & Veale, *supra* note 100, at 325–26.

116. Madeleine Clare Elish, *Moral Crumple Zones: Cautionary Tales in Human-Robot Interaction*, 5 ENGAGING SCI. TECH. & SOC'Y 40, 41 (2019).

117. *Id.* at 40.

deflected off of the automated parts of the system . . . and focused on the immediate human operators, who possess only limited knowledge, capacity, or control."[118] The "moral crumple zone" highlights how "users and operators of such systems may be held responsible for failures in ways that obscure other human actors who may possess equal if not greater control over the behavior of a purportedly 'autonomous' system," and demonstrates that it "is not only the misattribution of responsibility but also the ways in which new forms of consumer and worker harm may develop in new automated technologies."[119]

Even when designed with a step involving a human decision-maker to mitigate the automated system's errors, the system still may produce incorrect outcomes. When a harmful or inaccurate outcome occurs, apportioning responsibility becomes more difficult, and may result in the human decision-maker absorbing the brunt of the fault regardless of whether the mistake was truly in that person's control.[120] Because of the complexity of these systems, the CPPA should structure its regulations to protect both consumer data as well as the humans involved in multi-stage decision-making.

D. Automated Decisions in High-Risk Activities

The use of automated decision-making systems often implicates serious legal and ethical concerns. Organizations in the United States use automated decision-making systems across many industries, including banking and finance, law enforcement, healthcare, and emergency services.[121] Other high-risk uses of AI include determining whether to grant parole and diagnosing patients with medical conditions.[122] The use of AI in these matters raises the challenge of ensuring that the decisions come out fairly and accurately, and that, in case the decision involves an error, some degree of accountability exists for businesses implementing this technology. Because of this, the CPPA should

---

118. *Id.* at 42.

119. *Id.*

120. *Id.* at 41.

121. *See* Penny Crosman, *Can AI Help When a Scam Is Invisible to the Bank?*, AM. BANKER (Feb. 25, 2024), https://www.americanbanker.com/news/can-ai-help-when-a-scam-is-invisible-to-the-bank [https://perma.cc/T62R-S7NP] (explaining that banks use AI to uncover fraudulent activity by "identify[ing] physical behavior, such as typing or tapping patterns, that deviate from the customer's usual activity" and "to spot anomalous transactions"); *AI-Powered Decision Management Key for Global Credit Card Security*, MASTERCARD, https://b2b.mastercard.com/news-and-insights/blog/ai-powered-decision-management-key-for-global-credit-card-security/ [https://perma.cc/AEW4-TZ2M] ("With hundreds of thousands of decisions to make every second of every day, Mastercard depends on its AI-powered Decision Management Platform to detect fraud and other irregularities."); *see also* INDUS. COUNCIL FOR EMERGENCY RESPONSE TECH., HISTORY OF 911 AND WHAT IT MEANS FOR THE FUTURE OF EMERGENCY COMMUNICATIONS 7–8, https://www.911.gov/assets/History-of-911-And-What-It-Means-for-the-Future-of-Emergency-Communications.pdf [https://perma.cc/SA4U-KK7X] (describing how enhanced 911 calls use automatic location data to route emergency services to a caller's location with increased speed and accuracy); MOTOROLA SOL., LOCATION-BASED ROUTING 101 6–7 (2023), https://www.motorolasolutions.com/content/dam/msi/docs/motorola-solutions-connectivity/location_based_-routing_educational_whitepaper-11-23-v5.pdf [https://perma.cc/XW72-6HWN] (describing location-based 911 routing technology and providing examples of how the technology can be used in practice); *see generally* Corinne Cath, *Governing Artificial Intelligence: Ethical, Legal, and Technical Opportunities and Challenges*, PHIL. TRANSACTIONS ROYAL SOC'Y A. (Oct. 15, 2018), https://royalsocietypublishing.org/doi/10.1098/rsta.2018.0080 [https://perma.cc/6NPZ-WZ98] (listing industries that commonly use automated decision-making systems).

122. *See generally* Cath, *supra* note 121.

consider consumers' interests in overseeing companies' use of automated decision-making in high-risk activities.

If the CPPA follows the GDPR, the agency may limit the scope of automated decision-making to "legal . . . or similarly significant [e]ffects."[123] The GDPR recognizes that certain activities with high-risk outcomes should not be subject to automated systems.[124] Recital 71 of the GDPR, which addresses profiling in automated decision-making systems, lists examples of decisions that create significant legal effects for consumers, such as an "automatic refusal of an online credit application or e-recruiting practices without any human intervention."[125] Taking this approach may help California balance the efficiency interests of businesses with consumer privacy interests because companies can use this technology to boost efficiency in their operations.[126] These systems increase consistency in decision-making results and reduce a business' operational costs overall.[127]

For example, if the CPPA limits the right to opt-out of automated decision-making systems to circumstances where a consumer may face legal or other significantly similar effects, then consumers have additional protection in high-risk situations, such as decisions about obtaining parole, a medical diagnosis, or financial resources. Businesses may have increased compliance and administrative costs in these areas, but the CPPA can justify this by the need for greater consumer protection. Conversely, in situations where a decision carries lower stakes for consumers—such as a clothing retailer's use of profiling to make decisions about which of its products to promote to customers—this approach allows businesses to continue their use of automated decision-making systems largely unaffected.

E. Bias in Automated Decision-Making

While legislation exists to address bias in decisions made by humans, potential bias in AI decision-making has generally gone unaddressed. Some proponents of automated decision-making systems posit that these systems reduce biased results.[128] Because an algorithm determines the outcome without viewing race, gender, or other protected categories, the argument ensues, the system's outputs prevent biased results.[129] However,

123. Regulation (EU) 2016/679, *supra* note 22, at art. 22 § (1).

124. *Id.*

125. Regulation (EU) 2016/679, *supra* note 22, at recital (71).

126. If regulation requires companies to implement heightened protections for high-risk decisions but allows for lower standards when stakes are not as significant for consumers, this will likely reduce compliance costs. Many small decisions could still predominantly use automated systems, and high-risk decisions—the settings where consumers would most likely be harmed by an erroneous decision—could remain the focus of more meticulous decision-making.

127. *See* Mariarosaria Taddeo & Luciano Floridi, *How AI Can Be a Force for Good*, 361 SCIENCE 751, 751–52 (2018) (discussing the benefits of automated decision-making technology in the business context).

128. *See, e.g.*, Jon Kleinberg et al., *Human Decisions and Machine Predictions*, 133 Q.J. ECON. 237 (2018) (suggesting that automated decision-making could help reduce racial disparities in the criminal justice system); Jake Silberg & James Manyika, *Tackling Bias in AI (and in Humans)*, MCKINSEY GLOB. INST., June 2019, at 2, https://www.mckinsey.com/~/media/mckinsey/featured%20insights/artificial%20intelligence/tackling%20bias%20in%20artificial%20intelligence%20and%20in%20humans/mgi-tackling-bias-in-ai-june-2019.pdf [https://perma.cc/7XCS-S6LH] (indicating that algorithms may reduce disparities caused by human biases, but also recognizing that "it can . . . bake in and scale bias").

129. *See* Silberg & Manyika, *supra* note 128, at 2–3.

this does not accurately capture the machine learning aspect of automated decision-making systems.

Algorithms are vulnerable to similar biases that face human decision-makers due to the machine learning process.[130] While the algorithm itself cannot discriminate against a person in the same manner that a human could, it nonetheless carries similar biases and errors based on the information it uses to train.[131] In the process of machine learning, algorithms can perpetuate bias because they train using data with built-in human bias.[132] For example, Amazon used an AI recruiting tool that discriminated against women who applied for jobs.[133] The AI trained on data from "applicants by observing patterns in resumes submitted to the company over a 10-year period."[134] Because most of Amazon's resumes historically came from men, Amazon's algorithm taught itself to rank male candidates higher.[135]

In addition to the direct discriminatory decision-making found in Amazon's automated systems, other algorithms may engage in biased decision-making that humans cannot easily detect. This is accomplished through proxy discrimination, in which an automated system analyzes data that appears neutral on its face, but in fact correlates with discriminatory decision-making practices.[136] Proxy discrimination can occur when an

130. Melissa Hall et al., *A Systematic Study of Bias Amplification* (working paper associated with arXiv.org and last updated Oct. 19, 2022), https://arxiv.org/abs/2201.11706 [https://perma.cc/D7EM-52KS] ("Recent research suggests that predictions made by machine-learning models can amplify biases present in the training data."); Isabelle Bousquette, *Rise of AI Puts Spotlight on Bias in Algorithms*, WALL ST. J. (Mar. 9, 2023), https://www.wsj.com/articles/rise-of-ai-puts-spotlight-on-bias-in-algorithms-26ee6cc9 (on file with the *Journal of Corporation Law*) ("AI systems have been found to be less accurate at identifying the faces of dark-skinned people, particularly women; to give women lower credit-card limits than their husbands; and to be more likely to incorrectly predict that black defendants will commit future crimes than whites. Part of the problem is that companies haven't built controls for AI bias into their software-development life cycles."); *Algorithms That Adjust for Worker Race, Gender Still Show Biases*, UNIV. TEX. AUSTIN NEWS (Feb. 8, 2023), https://news.utexas.edu/2023/02/08/algorithms-that-adjust-for-worker-race-gender-still-show-biases [https://perma.cc/F523-GLGX] ("Even after algorithms are adjusted for overt hiring discrimination, they may show a subtler kind: preferring workers who mirror dominant groups . . . .").

131. *See, e.g.*, PETRA MOLNAR & LEX GILL, BOTS AT THE GATE: A HUMAN RIGHTS ANALYSIS OF AUTOMATED DECISION-MAKING IN CANADA'S IMMIGRATION AND REFUGEE SYSTEM 31–32 (Citizen Lab & Int'l Hum. Rts. Program eds., 2018), https://tspace.library.utoronto.ca/bitstream/1807/94802/1/IHRP-Automated-Systems-Report-Web-V2.pdf [https://perma.cc/Z4NS-FL7A] (explaining the presence of biases in algorithms).

132. *See Automated Decision Making Systems Are Making Some of the Most Important Life Decisions for You, but You Might Not Even Know It*, ACLU OF WASH. (Sept. 22, 2021), https://www.aclu-wa.org/story/automated-decision-making-systems-are-making-some-most-important-life-decisions-you-you-might [https://perma.cc/3F59-SSAM] (explaining that data carrying human biases creates biased outputs from AI that uses machine learning).

133. Jeffrey Dastin, *Amazon Scraps Secret AI Recruiting Tool That Showed Bias Against Women*, THOMSON REUTERS (Oct. 11, 2018), https://www.reuters.com/article/us-amazon-com-jobs-automation-insight/amazon-scraps-secret-ai-recruiting-tool-that-showed-bias-against-women-idUSKCN1MK08G [https://web.archive.org/web/20230718052944/https://www.reuters.com/article/us-amazon-com-jobs-automation-insight/amazon-scraps-secret-ai-recruiting-tool-that-showed-bias-against-women-idUSKCN1MK08G] (captured using Wayback machine).

134. *Id.*

135. *See id.* (stating that the extent of discriminatory decisions in Amazon's AI reached so far as to even "penalize[] resumes that included the word 'women's,' as in 'women's chess club captain" and to "downgrade[] graduates of two all-women's colleges").

136. *See* MOLNAR & GILL, *supra* note 131, at 10 (describing proxy discrimination).

automated system examines postal codes. Due to the history of redlining in the United States, the "use of apparently 'neutral' factors such as postal code[s] may in practice serve as a proxy for race, exacerbating racial biases [and] affording false legitimacy to patterns of racial profiling."[137] A lack of data may also increase bias in automated decisions. For people who do not maintain a strong online presence, and therefore have less data amassed for controllers to collect and analyze, results from algorithms may be inaccurately skewed.[138]

AI retains many of the same issues in biased decision-making that human decision-making presents. Additionally, algorithms allow for proxy discrimination, and may create greater room for error in decisions about consumers who lack a strong data presence.

F. Inherent Tension Points Between AI and Law

The intersection of automated decision-making and law contains unavoidable tension points. The practice of law involves balancing rules and discretion. This requires the ability to consider cases with contradictory norms and various contextual factors, and to then use that judgment in determining outcomes.[139] Attorneys and judges often face unpredictable variables in cases they handle, such as inconsistent human behavior, conflicting or ambiguous rules, and novel cases that do not follow analogously from prior cases. By contrast, AI models function based on training data and are capable only of abiding by the rules inherent in their predisposed data set. An algorithm, by definition, cannot exercise discretion with changing or novel variables if those variables are not present in the available data set.[140] This innate discrepancy between AI and law indicates that human intervention, at least to some degree, must remain in the decision-making process. Reuben Binns, Associate Professor of Human Centered Computing at the University of Oxford, describes this as a need for individual justice. He explains this as "the notion that each case needs to be assessed on its own merits, without comparison to, or generalization from, previous cases."[141] Indeed, while some decisions involve recurring patterns, the law must, at its core, maintain the ability to individually analyze each case. Law involves situations

137. *Id.* at 32.

138. For example, Janet Vertesi, Associate Professor of Sociology at Princeton University, attempted in 2014 to minimize her data footprint online. She experimented by attempting to hide her pregnancy from companies that market products to pregnant women. While avoiding internet searches or activity that could allow data controllers to infer information about her, going so far as to route her searches through a Tor browser and withdraw cash to make purchases that would otherwise be traceable. As a result, automated decision-making systems erroneously flagged Vertesi as suspected of engaging in fraudulent criminal activity. Janet Vertesi, Opinion, *My Experiment Opting Out of Big Data Made Me Look Like a Criminal*, TIME (May 1, 2014), https://time.com/83200/privacy-internet-big-data-opt-out [https://perma.cc/SBU9-HTXT]; *see also* Anya E. R. Prince, *I Tried to Keep My Pregnancy Secret*, THE ATLANTIC (Oct. 10, 2022), https://www.theatlantic.com/ideas/archive/2022/10/can-you-hide-your-pregnancy-era-big-data/671692/ [https://perma.cc/APG3-SX4H] (describing how the article's author similarly attempted to hide personal details from online targeted advertising).

139. *See* Reuben Binns, *Human Judgment in Algorithmic Loops: Individual Justice and Automated Decision-Making*, 16 REGUL. & GOVERNANCE 197, 198 (2022) (discussing the rules-versus-discretion debate related to automated decision-making systems).

140. *See id.* (noting that "algorithmic decision-making is usually regarded as incapable of exercising this kind of discretion" and that humans "are unable to pre-specify [in an algorithm] how to reason appropriately about new cases without human intervention").

141. *Id.* at 197.

where "the possibility of future vagueness is always inherent, even for [circumstances] which are currently entirely clear but may later need to be adapted in the face of unknown examples."[142] Adaptation in the face of vagueness is a feature of independent analysis that AI simply cannot replicate. Rulemaking about automated decision-making at large must, therefore, consider the concept of individual justice in determining how consumers may exercise meaningful rights to human intervention in the decision-making process.

IV. RECOMMENDATIONS FOR CPPA RULEMAKING

When conducting rulemaking for rights against automated decision-making under the CPRA, the CPPA should: (1) avoid a broad right to explanation; (2) scale the use of automated systems to the risk of consumer activity; (3) incorporate meaningful human oversight; and (4) exempt certain activities.

A. Avoid a Broad Right to Explanation

A broad right to explanation will likely prove difficult to administer and may not offer the data protection consumers seek.[143] The GDPR has explored the right to transparency, with the idea that disclosing a given algorithm will allow consumers to determine whether the decision it produces ultimately has unfairly prejudiced the consumer.[144] Nonetheless, algorithms constantly evolve and make the accuracy of disclosure administratively difficult.[145] Disclosing a company's algorithm may also raise concerns of exposing trade secrets and infringing on intellectual property rights.[146] Further, if the CPPA enacted a right of transparency, this still would not provide consumers with significant protection from bias, because "even transparent algorithms and automated systems can cause harm by perpetuating and exacerbating biases."[147] Therefore, the CPPA should avoid a broad right to explanation as a means of regulating automated decision-making systems.

While the CPPA should not rely heavily on a right to explanation for the previously mentioned reasons, the CPPA may be able to find a middle ground with proponents of AI explainability. One possibility is the use of event logging subsystems, which provide a reasonable degree of explainability that gives insight into how a system came to its eventual decision.[148] Event logging subsystems have been used to trace decision-making in the context of flight recorders, which determine the course of flight events in aviation accident investigations.[149] Airplanes are equipped with "black boxes." Black boxes contain a flight data recorder (FDR) and a cockpit voice recorder (CVR), and are placed in locations least likely to be destroyed on impact.[150] In the event of an aviation accident, a recovered black

142. *Id.* at 201.

143. *See supra* Part III.A (assessing the difficulty of explainability).

144. *Id.*

145. *Id.*

146. *Id.*

147. ACLU OF WASH., *supra* note 132.

148. *See* Gryz & Rojszczak, *supra* note 95, at 3 (introducing event logging subsystems as a potential solution to the explainability issue).

149. *Id.*

150. John Staughton, *How Do Airplane Black Boxes Work?*, SCI. ABC (July 27, 2022), https://www.scienceabc.com/innovation/how-do-airplane-black-boxes-work.html [https://perma.cc/44C9-3TUU].

box provides pinpoints of data to help investigators reconstruct the incident.[151] In this sense—while no fully transparent method of recounting the events exists, such as a full video recording—there are data points that serve as "memory banks" of the flight, maintaining enough data to "reveal the secrets of an aircraft's functions and pilot actions" for purposes of discovering how the accident occurred.[152]

The benefits of implementing systems similar to the event logging subsystems on aircraft are that, on one hand, it provides data to explain how decisions were made. On the other hand, it "is relatively simple to implement, does not increase the costs of deploying and maintaining the system, and does not require time-consuming validation procedures."[153] Perhaps a method of explanation under California law could require businesses to provide certain data touch points that would allow consumers some insight into how automated decisions using their data are made without reasonably compromising algorithms protected as trade secrets. Under this model, regulations could require a business to provide relevant data touchpoints for consumers (for example, stating which categories of consumer data the AI uses when making decisions). This could allow consumers to understand a general idea of how the decision-making process occurred without requiring that the company disclose significantly detailed information about its algorithms. If the CPPA required an explanation for automated decision-making systems, then tailoring this requirement to resemble a process like an event logging subsystem would both give consumers a degree of information about the decision while also easing the burden on businesses who must provide the explanations to consumers.

B. Scale the Use of Automated Systems to the Risk of Consumer Activity

In its rulemaking, the CPPA should balance the ability to use automated decision-making with the risk of consumer activity involved. AI used for low-risk situations may call for greater flexibility under the CPRA, while situations prone to higher risk for consumers should require greater constraints.

AI in targeted advertising provides an example of a low-risk situation. Under California's existing data privacy legislation, consumers can opt-out of their data being used for marketing purposes, and this will continue under the CPRA.[154] For consumers who have not opted out, companies may use automated decision-making systems to determine how to best market their products. These situations generally present low risks for consumers—a person who has not opted out of their data's use for marketing would be unlikely to experience hardship or serious legal consequences from seeing personalized advertisements based on automated decision-making. Thus, low-risk circumstances where AI is involved may present an opportunity for the CPRA to allow more lenient use of automated decision-making for purposes of reasonably balancing compliance costs for data controllers.

---

151. *Id.*

152. *Id.*

153. Gryz & Rojszczak, *supra* note 95, at 13.

154. *See supra* note 65 and accompanying text (referring to the right to opt-out of the sale or sharing of personal data in California).

Other situations where businesses use automated decision-making systems pose significant risks to consumers.[155] The CPPA should target its automated decision-making restrictions towards these scenarios. Automated decision-making is currently used in high-risk circumstances involving, *inter alia*, bail and sentencing determinations,[156] job and educational assessments, loan application processes,[157] and police monitoring.[158] These situations pose significant risks for consumers. In the judicial system, a criminal defendant has a strong interest in knowing how the determination for their sentencing or bail is made. Individuals in job and educational settings have a reasonable expectation to know how their performance is measured. A consumer who applies for a loan relies on AI to determine whether the lending institution will grant the loan, and the public at large has an interest in understanding how decisions by law enforcement to monitor specific areas might disproportionately affect certain communities. In these high-risk scenarios, where the possibility of an automated system wrongfully reaching a decision would place greater burdens on consumers, the CPPA should require easier opt-out mechanisms to support consumer protection interests. The balance in the use of automated decision-making systems often depends on the benefit to businesses in creating greater efficiency in their operations; however, where the risk to consumers is great, the CPPA should conclude that the potential legal and financial risks to consumers weigh heavier than business interests. The CPPA, therefore, should tailor the scope of its greatest protection for opting out of automated decision-making to circumstances posing heightened risks to consumers.

C. Incorporate Meaningful Human Oversight

Rulemaking for the CPRA's right against automated decision-making should require meaningful human oversight. In multi-stage automated decision-making systems, controllers can incorporate humans in the decision-making process, but that alone is unlikely to provide effective intervention.[159] To prevent businesses from merely adding humans in ways that do not significantly aid the decision-making process, the CPPA should draft its regulations to require meaningful human involvement in otherwise automated systems.

The United States housing market provides an example of how this could function. In the last decade, the housing market has increasingly used algorithms such as Yield Star and RealPage, which make automated decisions about pricing that landlords set for an

155. *See supra* Part III.D (discussing high-stakes scenarios such as financial determinations and medical diagnoses).

156. *See* Ben Winters, *AI in the Criminal Justice System*, ELEC. PRIV. INFO. CTR., https://epic.org/issues/ai/ai-in-the-criminal-justice-system/ [https://perma.cc/L53Y-T6LW] (explaining the role of automated decision-making in bail and sentencing determinations); *see also* Tim Wu, *Will Artificial Intelligence Eat the Law? The Rise of Hybrid Social-Ordering Systems*, 119 COLUM. L. REV. 2001, 2002 (2019) (noting that the criminal justice system uses automated decision-making technology for bail and sentencing purposes).

157. Binns & Veale, *supra* note 100, at 321.

158. *See* ACLU OF WASH., *supra* note 132 ("In Tacoma, police have used PredPol software, which uses a secret algorithm to predict the exact blocks where future crimes will occur, and recommends that police spend extra time patrolling those blocks.").

159. *See, e.g.*, *supra* Part III.B (discussing the "token human" issue that arises when humans are not meaningfully incorporated in the decision-making process).

apartment unit's rent.[160] It bases this determination on data from pricing of similar apartment units in the surrounding area.[161] Here, while the algorithm is used as the primary method of determining pricing, the systems seem to allow for meaningful human intervention; "[t]here is still an opportunity [that] if a landlord wanted to challenge the recommendations that the software makes, they can potentially overrule a suggestion [set by the algorithm]."[162] It is unclear to what extent many of these rental properties allow for human intervention in and oversight of the automated decision-making system, but this structure at least suggests that AI can be compatible with meaningful human judgment. The CPPA should include provisions in its regulations that require meaningful human oversight, which would allow a person to exercise discretion in monitoring and overriding an algorithm's decision. Combining the benefits of human judgment with automated decision-making technology will help balance consumer data protection and business efficiency interests.

As another tool to incorporate meaningful human oversight in automated decision-making, the CPPA could require an appeal process. Allowing businesses to use automated decision-making at the front end could ease the initial compliance burden, and should erroneous decisions occur, consumers would then have the protection of a human-based appeal to review the decision.

D. Exempt Certain Activities

The CPPA should exempt certain business activities from the requirement to give consumers an opt-out from automated decision-making. The regulations should limit this to cases where benefits to the consumer of automated decisions substantially outweigh the potential harms of using this technology. 911 call centers often use automated decision-making to route emergency services to a caller's location quickly and accurately.[163] Financial institutions similarly use automated decision-making systems to efficiently detect potential fraud among the millions of transactions they process daily.[164] In these situations, benefits to the consumer of receiving life-saving services and stopping fraudulent transactions substantially outweigh the possible risks associated with automated decision-making. Accordingly, the CPPA should calibrate its regulations to provide a carve-out from the right against automated decision-making for these activities.

V. CONCLUSION

The data privacy landscape in the United States is still in its early stages, and California has pioneered efforts to enhance consumer data privacy measures. As the public learns more about how personal data is used, many people prefer more comprehensive data protection. The CPPA can establish rulemaking that aids data privacy efforts, especially

160. *When an Algorithm Raises Your Rent*, SLATE (Oct. 21, 2022), https://slate.com/transcripts/N3lWMXNLQjdHL1ZpK0YzRk04THN5UUNjdm1GUXF0Uy9GZFZhN2dQK0xOTT0= [https://perma.cc/98K9-46LJ].

161. *See id.* (explaining typical mechanics of rent-setting algorithms).

162. *Id.*

163. *See supra* note 121 and accompanying text.

164. *Id.*

with respect to the right against automated decision-making, while also furthering the interests of businesses employing this technology.