A NEW WAVE OF PRIVACY AND CONSUMER LAWS: SHOULD THE CALIFORNIA CONSUMER PRIVACY ACT BE IMPLEMENTED IN NORTH DAKOTA?

ABSTRACT

The California Consumer Privacy Act was recently passed by the California State Legislature on June 28, 2018 and it became law on January 1, 2020. The Act was introduced in order to enhance privacy rights and consumer protection of personal information. The Act introduces many changes relating to consumer privacy and how companies collect, store, share, and use personal consumer data. It is the first step towards limiting companies use of personal data without consent by the state. At present, North Dakota does have privacy laws concerning certain situations, but it does not have privacy laws as substantial and as enforceable as the California Consumer Privacy Act. An overview of the Act itself, as well as the new approaches taken by certain states to protect private consumer information, will clarify the paths currently accessible to protect the privacy consumer information of North Dakotans. Looking toward the future of consumer privacy laws, North Dakota legislation should strongly consider implementing many, if not all, the policies contained in the California Consumer Privacy Act.

I. BACKGROUND

Individual privacy is becoming more important in today's world. Since the introduction of mainstream social media, commencing with Facebook in 2004,[1] personal data is shareable across many platforms and a person's information is susceptible to be sold to third parties or the highest bidder, many times as advertisers.[2] When a person creates a Facebook profile and inputs certain information about product preferences, advertisements relating to those preferences are displayed as a result of the sharing of their information. Even though the person shared this information, they are unaware their preferences would be used for this purpose. For example, if someone were to state on their Facebook profile that they were a fan of Star Wars and "liked" several Star Wars posts on Facebook, they would most assuredly see advertisements for an upcoming Star Wars movie or television series in their Facebook feed.[3] What they may not know is behind the scenes, Facebook has sent their information to advertisers in order to advertise those specific product placements and Facebook has also tracked their activity on other third-party websites.[4]

Recently, Facebook has received criticism for the practice of selling information concerning its users to advertisers without the user's knowledge. Facebook is a free service for its users; therefore, it depends on advertisements to obtain revenue for its services.[5] Facebook's advertising practices came into focus in what is now known as the 2018 Cambridge Scandal,[6] where Cambridge Analytica, a British political consulting firm, harvested the personal data of millions of Facebook users without their consent.[7] They used this data for political advertising purposes.[8] In 2018, Facebook's creator, Mark Zuckerberg, testified for two days before a joint Senate Commercial and Judicial committee, where he answered questions about the company's data gathering practices.[9] In one notable exchange, Zuckerberg was asked by Senator Orrin Hatch, "So, how do you sustain a business model in which

---

1. Yasamine Hashemi, *Facebook's Privacy Policy and Its Third-Party Partnerships: Lucrativity and Liability*, 15 B.U. J. SCI. & TECH. L. 140, 142 (2009).

2. *Id.* at 141.

3. Michelle Castillo, *Why Facebook Ads Follow You*, CNBC (Nov. 30, 2017, 2:53 PM), https://www.cnbc.com/2017/11/30/why-facebook-ads-follow-you.html.

4. *Id.*

5. Matthew Johnson, *How Facebook Makes Money*, INVESTOPEDIA (Jan 12, 2020), https://www.investopedia.com/ask/answers/120114/how-does-facebook-fb-make-money.asp.

6. Nikhill Rajesh, *Cambridge Analytica Scandal Explained*, SIMPLE SNIPPETS (Mar. 27, 2018, 5:24 PM), https://simplesnippets.tech/cambridge-analytica-scandal-explained/.

7. *Id.*

8. *Id.*

9. 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, 71 (2018).

users don't pay for your service?" Zuckerberg replied, "Senator, we run ads."[10] The Cambridge Scandal revealed to governments and the general public how giant technology companies, such as Facebook, collect personal information from their users.[11] This opened Facebook up to scrutiny on its sharing of personal information and how the data is shared today, including an investigation by the United States Federal Trade Committee (FTC).[12]

The FTC concluded its investigation of the Cambridge Scandal with Facebook agreeing to a $5 billion-dollar settlement for the company's user privacy violations.[13] As part of the settlement, Facebook committed to a massive overhaul of its consumer privacy practices.[14]

As consumer privacy became more of a concern, certain states began to implement stricter consumer privacy protection laws. In 2018, the State of California took steps toward protecting the privacy of the consumer and signed into law the California Consumer Privacy Act (CCPA) on June 28, 2018.[15] The law went into effect on January 1, 2020.[16] The details of the law are explained below, however, the broad basic rights set out in the Act are as follows:

> (1) [The bill] gives consumers "the right to know what personal information a business has collected about them and how it is being used; (2) the right to 'opt out' of a business selling their personal information; (3) the right to have a business delete their personal information; and (4) the right to receive equal service and pricing from a business, even if they exercise their privacy rights under the CCPA.[17]

These four rights are to be enforced primarily by the California Attorney General, with a narrow private right of action for the user for data breaches.[18] If there is an unintentional violation of the new law, a company could be fined up to $2,500 per unintentional violation and $7,500 for an intentional

---

10. *Id.*

11. Nikhill Rajesh, *Cambridge Analytica Scandal Explained*, SIMPLE SNIPPETS (Mar. 27, 2018, 5:24 PM), https://simplesnippets.tech/cambridge-analytica-scandal-explained/.

12. *Id.*

13. Julia Carrie Wong, *Facebook to be fined $5bn for Cambridge Analytica privacy violations-reports*, GUARDIAN (July 12, 2019, 6:12 PM), https://www.theguardian.com/technology/2019/jul/12/facebook-fine-ftc-privacy-violations.

14. Natalie Gagliordi, *FTC Hits Facebook with Record $5 Billion Fine for User Privacy Violations*, ZDNET: BETWEEN THE LINES (July 24, 2019, 2:22 PM), https://www.zdnet.com/article/ftc-hits-facebook-with-record-5-billion-fine-for-user-privacy-violations/.

15. Pardau, *supra* note 9, at 72.

16. *Id.*

17. *Id.*

18. *Id.*

violation.[19] The Act has been nicknamed "America's GDPR"[20] in comparison to the General Data Protection Regulations (GDPR) set by the European Union, published in May 2016 and enacted into law in all European Union member states on May 24, 2018.[21] Facebook stated they made the necessary updates in order to comply with the CCPA,[22] as they had with the GDPR.[23] For example, Facebook asked users if they wanted to continue sharing certain types of information on their Facebook profile.[24] Facebook also updated their terms of service and data policy to comply with the GDPR.[25] Nevertheless, more steps will likely have to be undertaken to comply with the CCPA.[26]

We are nearing a new digital age with regard to accessing personal information,[27] where lawmakers will need to update privacy laws in order to reflect the times we live in.[28] Privacy laws concerning the sharing of personal information have not caught up to today's advances in technology. The CCPA is a much-needed step to bring privacy laws in line with protecting personal information and returning control of one's personal information back into the hands of the consumer. Other states have since begun to draft and implement their own consumer privacy laws as a result of the CCPA.[29]

---

19. CAL. CIV. CODE § 1798.155(b) (West 2020); *see also* Mark Diamond, *Quick Overview: Understanding the California Consumer Privacy Act*, ASS'N OF CORP. COUNSEL (July 26, 2019), https://www.acc.com/resource-library/quick-overview-understanding-california-consumer-privacy-act-ccpa.

20. Joel-Noël Barneron, *Get Ready for America's GDPR: CCPA*, STREETFIGHT MAG. (Oct. 21, 2019), https://streetfightmag.com/2019/10/21/get-ready-for-americas-gdpr-ccpa/.

21. Pardau, *supra* note 9, at 85.

22. Daphne Leprince-Ringuet, *We are Ready, Says Facebook as California Prepares for New Privacy Law*, ZDNET (Dec. 16, 2019, 3:04 PM), https://www.zdnet.com/article/we-are-ready-says-facebook-as-california-prepares-for-new-privacy-law/.

23. *Id.*

24. Arjun Kharpal, *Facebook Lays Out Changes to Comply with a Strict New European Privacy Law*, CNBC (Apr. 18, 2018, 2:39 AM), https://www.cnbc.com/2018/04/18/facebook-makes-changes-to-comply-with-eu-privacy-law-gdpr.html.

25. *Id.*

26. Daphne Leprince-Ringuet, *We are Ready, Says Facebook as California Prepares for New Privacy Law*, ZDNET (Dec. 16, 2019, 3:04 PM), https://www.zdnet.com/article/we-are-ready-says-facebook-as-california-prepares-for-new-privacy-law/.

27. Alyssa M. Brumis, *The Right to Privacy in a Digital Age: Reinterpreting the Concept of Personal Privacy*, 8 INQUIRIES J. 1, 1-2 (2016).

28. *Id.*

29. The states of Hawaii, Maryland, Massachusetts, Mississippi, Nevada, New Mexico, New York, North Dakota, and Rhode Island have all introduced bills pertaining to consumer privacy protection since the passing of the CCPA. *See* Emily Tabatabai, et al., *State Legislators Joining the Consumer Privacy Protection Party: Introduced CCPA-Like Bills*, ORRICK: TRUST ANCHOR (Mar. 18, 2019), https://blogs.orrick.com/trustanchor/2019/03/18/state-legislators-joining-the-consumer-privacy-protection-party-introduced-ccpa-like-bills/.

II. PRIVACY LAWS BEFORE THE CALIFORNIA CONSUMER PRIVACY ACT

The CCPA is the latest step in laws protecting the right to privacy for an individual, notably concerning a user's personal data and information. As this section demonstrates, an individual's right to privacy is entrenched in the United States Constitution under the Fourth Amendment.[30] Privacy rights are also included in the First Amendment as well as the Fourteenth Amendment.[31] A right to privacy according to the courts is a "basic human right, and as such is protected by virtue of the [Ninth] Amendment."[32] However, while case law has brought significant changes to the right to privacy, there is limited protection for an individual against non-governmental persons and companies, only federal and state governments.

The right to privacy in the United States has undergone significant evolution through case law, including the right of married couples to access contraception in *Griswold v. Connecticut*,[33] where the United States Supreme Court held married couples have the right to access contraception.[34] The right to privacy was furthered eight years later by the United States Supreme Court holding a woman had the right to privacy to protect her right to an abortion in *Roe v. Wade*.[35] The court held that "the Court has recognized that a right of personal privacy, or a guarantee of certain areas or zones of privacy, does exist under the Constituion."[36] Further the court held "This right of [personal] privacy . . . is broad enough to encompass a woman's decision whether or not to terminate her pregnancy."[37] Thirty years later, the United States Supreme Court upheld the right to privacy regarding sexual practices of same-sex couples in *Lawrence v. Texas*.[38] While these three cases changed the scope of an individual's right to privacy, they were limited to non-governmental actors. Thus, they did not extend these constitutional rights to privacy and to non-governmental related companies or persons.

Federal privacy laws are in need of reform to reflect the current technological environment of American society. An individual's personal

---

30. U.S. CONST. amend. IV.

31. U.S. CONST. amends. I, XIV.

32. Steve Mount, *Things That are Not in the Constitution: The Right to Privacy*, USCONSTITUTION.NET (Dec. 18, 2010), https://usconstitution.net/constnot.html#privacy.

33. 381 U.S. 479 (1965).

34. *Griswold*, 381 U.S. at 485.

35. 410 U.S. 113 (1973).

36. *Roe*, 410 U.S. at 152.

37. *Id.* at 153.

38. 539 U.S. 558 (2003).

information can be shared amongst a variety of websites.[39] These websites are largely unregulated concerning the information and companies are set up to extrapolate the information, known as data brokers.[40] These data brokers may then use the information in a manner not necessarily reflective of the consumer's intents or interests.[41] Following the initiative of the GDPR of the European Union, several states such as California commenced implementing state privacy laws to emulate the GDPR, while also advancing their respective state data privacy laws.[42]

A. UNITED STATES FEDERAL PRIVACY LAWS

While the word "privacy" does not appear in the text of the Constitution, there are constitutional limits to intrusion by the government into the privacy of an individual.[43] The Fourth Amendment states:

> [T]he right of the people to be secure in their person, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.[44]

However, the United States does not have a single, comprehensive federal law concerning data privacy.[45]

The FTC is in charge of the security and safety of consumers in the United States.[46] Nonetheless, many FTC regulations are outdated and should be updated.[47] Federal privacy laws have only been updated sparingly since

---

39. Brian Naylor, *Firms are Buying, Sharing Your Online Info. What Can You Do About It?*, NPR (July 11, 2016, 4:51 PM), https://www.npr.org/sections/alltechconsidered/2016/07/11/485571291/firms-are-buying-sharing-your-online-info-what-can-you-do-about-it.

40. *Id.*

41. *Id.*; *see also* Nuala O'Connor, *Reforming the U.S. Approach to Data Protection and Privacy*, COUNCIL ON FOREIGN REL.: DIG. AND CYBERSPACE POL'Y PROGRAM (Jan. 30, 2018), https://www.cfr.org/report/reforming-us-approach-data-protection.

42. Rachel R. Marmor, et al., "*Copycat CCPA" Bills Introduced in States Across County*, DAVIS WRIGHT TREMAINE LLP: PRIVACY & SECURITY L. BLOG (Feb. 8, 2019), https://www.dwt.com/blogs/privacy—security-law-blog/2019/02/copycat-ccpa-bills-introduced-in-states-across-cou.

43. Steve Mount, *Things That are Not in the Constitution: The Right to Privacy*, USCONSTITUTION.NET (Dec. 18, 2010), https://usconstitution.net/constnot.html#privacy.

44. U.S. CONST. amend. IV.

45. Nuala O'Connor, *Reforming the U.S. Approach to Data Protection and Privacy*, COUNCIL ON FOREIGN REL.: DIG. AND CYBERSPACE POL'Y PROGRAM (Jan. 30, 2018), https://www.cfr.org/report/reforming-us-approach-data-protection.

46. *About the FTC*, FED. TRADE COMM'N, https://www.ftc.gov/about-ftc (last visited Dec. 10, 2019).

47. *Internet Law – Privacy*, USLEGAL, https://internetlaw.uslegal.com/privacy/ (last visited Dec. 17, 2019).

1990.[48] There were attempts to pass new legislation as a result of the Equifax data breach in 2017-18, where the personal information of more than 145 million Americans was exposed to hackers.[49] There, hackers seized information and gained access to the names, social security numbers, birth dates, and addresses of millions of individuals.[50] Nonetheless, attempts to pass new legislation failed to pass through Congress.[51] Lawmakers, often split down party lines, could not agree on the appropriate scope or how to properly implement these laws.[52] Therefore, it was left to the states to implement data privacy laws in regard to the use of personal information. To date, there is no uniform Federal Privacy Law comparable to the CCPA or the GDPR.[53]

B. FACEBOOK AND ITS USAGE OF PERSONAL DATA

The internet has changed the way personal data is shared among companies and advertisers today in the digital age. Facebook has expanded the amount of data it accumulates from its users over the years. Facebook's practices on how it divulged its users information was highlighted in the Cambridge Scandal.[54] Cambridge Analytica developed and then provided an application called "thisisyourdigitallife."[55] Cambridge Analytica arranged a process where several hundred thousand Facebook users agreed to complete a survey, which was stated to be only for academic use.[56] However, the app also collected the personal information of each of the survey takers friends on Facebook, leading to the accumulation of a data pool of tens of millions of users.[57] This data harvesting violated Facebook's "platform policy," which only allowed the collection of friends' data "to improve user experience in the app" and prohibited the information from being sold or used for

48. *Id*.

49. David Lazarus, *Months After Equifax Data Breach, We're Still No Closer to Privacy Protections*, L.A. TIMES (Jan. 5, 2018, 3:00 AM), https://www.latimes.com/business/lazarus/la-fi-lazarus-cybersecurity-data-breaches-20180102-story.html.

50. *Id*.

51. *Id*.

52. *Id*.

53. Nuala O'Connor, *Reforming the U.S. Approach to Data Protection and Privacy*, COUNCIL ON FOREIGN REL.: DIG. AND CYBERSPACE POL'Y PROGRAM (Jan. 30, 2018), https://www.cfr.org/report/reforming-us-approach-data-protection.

54. Carole Cadwalladr & Emma Graham-Harrison, *Revealed: 50 million Facebook Profiles Harvested for Cambridge Analytica in Major Data Breach*, THE GUARDIAN (Mar. 17, 2018, 6:03 P.M), https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election.

55. *Id*.

56. *Id*.

57. *Id*.

advertising.[58] Facebook later admitted the information of up to 87 million Facebook users was improperly shared.[59]

Mark Zuckerberg, during his testimony in front of a joint Senate Judicial and Commerce Committee, stated that Facebook does not sell data to advertisers or anyone.[60] However, user data is used without their knowledge.[61] Zuckerberg then went on to explain the process:

> What we allow is for advertisers to tell us who they want to reach, and then we do the placement. So, if an advertiser comes to use and says, "All right, I am a ski shop and I want to sell skis to women," then we might have some sense, because people shared skiing-related content, or said they were interested in that, they shared whether they're a woman, and then we can show the ads to the right people without that data ever changing hands and going to the advertiser.[62]

Even if no personal data is shared with the advertiser, Facebook is still using data harvested from its platform's users for advertisement purposes.[63]

Even more alarming, USA Today reported Facebook could also track and create a running log of the webpages each of its users visited during the previous ninety days.[64] Facebook would also keep track of where non-members would go on the web after they visited a Facebook web page.[65] Also, when a user would "like" a page on Facebook, this data would be sent to Facebook's servers.[66] Personal information of its users, including a user's friends list, interests and likes, was also exchanged when a user would use

58. *Id.*

59. Hanna Kozlowska, *The Cambridge Analytica Scandal Affected Nearly 40 million More People Than We Thought*, QUARTZ (Apr. 4, 2018), https://qz.com/1245049/the-cambridge-analytica-scandal-affected-87-million-people-facebook-says/.

60. Ben Gilbert, *How Facebook Makes Money From Your Data, in Mark Zuckerberg's Words*, BUS. INSIDER (Apr. 11, 2018, 9:25 AM), https://www.businessinsider.com/how-facebook-makes-money-according-to-mark-zuckerberg-2018-4.

61. *Id.*

62. *Id.*

63. *Id.*

64. Byron Acohido, *Facebook Tracking is Under Scrutiny*, U.S.A. TODAY (Nov. 16, 2011, 9:03 AM), https://usatoday30.usatoday.com/tech/news/story/2011-11-15/facebook-privacy-tracking-data/51225112/1?csp=34money.

65. *Id.*

66. *Id.*

applications on Facebook.[67] In 2015, Facebook restricted this access to third-parties to only information about a user's friends.[68]

The Cambridge Scandal brought to light the data collection practices of Facebook, which up to that point, were not widely known to its users and the general public.[69] Beginning with the implementation of the GDPR in 2018, governments began to realize stricter enforcements regarding personal information are needed for privacy protection.

C. IMPLEMENTATION OF THE GENERAL DATA PROTECTION REGULATION

Since the introduction of Facebook and data collection by companies, the European Union was the first to put forward and then enact its own regulation regarding broad consumer privacy data laws.[70] As explained by Stuart L. Pardau:

> For decades, European privacy law has offered a stark contrast to the content-, modality-, and subject-focused data regime in the United States. This contrast is rooted in underlying norms and conflicting values about the importance of free enterprise and flow of information on one hand and the individual's privacy on the other. Whereas legislators in the U.S. "tend to emphasize the free flow of information and minimal government regulation," European focus has traditionally been "first and foremost on individual privacy protection as a basic human right."[71]

The European Union first published the GDPR in May 2016, with the legislation going into effect in all European Union Member states by May 25, 2018.[72] There are eight basic rights given to individuals under the GDPA: (1) the right to be informed about how their data is used; (2) the right of access (a company must usually provide access to an individual's data free of charge); (3) the right to rectification, where individuals are entitled to have their personal data rectified if it is inaccurate or incomplete; (4) the right to erasure, where companies must have procedures in place for removing or deleting personal data easily and securely if the individual withdraws consent

---

67. Jessica Guynn, *Can Facebook Be Trusted with Your Personal Info? Voter Harvesting Scheme Shows Perils for Users*, U.S.A. TODAY (Mar. 19, 2018, 5:26 PM.), https://www.usatoday.com/story/tech/2018/03/19/can-facebook-trusted-your-personal-info-voter-harvesting-scheme-shows-perils-users/438464002/.

68. *Id*.

69. *Id*.

70. Pardau, *supra* note 9, at 71.

71. *Id*. at 83.

72. *Id*. at 85.

to the usage of the data; (5) the right to restrict processing, where individuals can "block" or restrict processing of their personal data if they contest its accuracy or objected to the processing; (6) the right to data portability, which allows individuals to obtain and reuse their personal data across different platforms; (7) the right to object, where individuals can object to having their data used for direct marketing and purposes of scientific/historical research and statistics; and (8) the right related to automated decision making and profiling (if any of the processors constitute profiling with their automatic decision making, individuals now have the right to object and obtain human intervention, unless it is a contractual necessity).[73]

The GDPR applies in three circumstances: (1) if an organization collects data from European Union residents, regardless of whether the processing takes place in the Union (data controller); (2) if an organization processes data of Union citizens on behalf of a data controller (processor); or (3) the person is based in the European Union.[74] The scope of the regulation is broad enough to include countries outside Europe and applies to organizations outside the European Union that collect or possess personal data on individuals who are located outside the European Union.[75] Personal data according to the European Commission is: "[I]nformation that relates to an identified or identifiable individual."[76] As Associate Professor Stuart L. Pardau states in his law review article *The California Consumer Privacy Act: Towards a European-Style Privacy Regime in the United States*, "[The] GDPR has nothing to do with citizenship or protecting rights of Europeans, per se . . . the law aims to protect anyone in Europe, even tourists."[77]

The GDPR also has stronger enforcement mechanisms compared to previous data privacy laws.[78] Fines imposed for breaches could be up to 4% of a company's global revenue.[79] Further, the GDPR gives "broad 'investigative' and 'corrective' powers to European supervisory authorities."[80] This makes it much easier for a subject to bring a claim against data collectors and

---

73. *Individual Rights – Guide to the General Data Protection Regulation,* INFO. COMM'R'S OFF., https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/ (last visited Dec. 15, 2019).

74. *General Data Protection Regulation Article 3 - Territorial Scope*, INTERSOFT CONSULTING, https://gdpr-info.eu/art-3-gdpr/ (last visited Dec. 14, 2019).

75. *Id*.

76. *What is Personal Data?*, EUR. COMM'N, https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_en. (last visited Dec. 10, 2019).

77. Pardau, *supra* note 9, at 86.

78. *Id*. at 87.

79. *Id*.

80. *Id*.

data processors.[81] U.S. companies can seek compliance with the GDPR.[82] In order to do so, U.S. companies must "develop a conforming privacy policy, identify an independent recourse mechanism, and self-certify through the Department of Commerce website."[83]

The day after the GDPR was enacted into law, companies served Facebook and Google with multiple lawsuits for violating GDPR law, totaling $8.8 billion.[84] Facebook received a "flood" of lawsuits after the passing of the GDPR.[85] It is too early to determine the effects of the GDPR on companies. Nevertheless, because there are numerous lawsuits against the giant technological companies as a result of the regulation, the impact of the GDPR will most likely be substantial on giant technological companies. The GDPR also paved the way for numerous states to enact their own privacy laws to emulate it, such as the CCPA.

III. THE CALIFORNIA CONSUMER PRIVACY ACT

California is one of ten states to enshrine privacy as a specified right in its state constitution.[86] Article 1, Section 1 of the California Constitution states: "[a]ll peoples are by nature free and independent and have inalienable rights . . . enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and *privacy*."[87] Even before the CCPA, California was known for its elaborate and strict privacy laws.[88] Prior to the CCPA, California enacted the California Online Privacy Protection Act (CalOPPA) in 2004.[89] When it was enacted, it was regarded as one of the broadest internet privacy laws in the United States.[90] Most notably, it required commercial websites and online services to post a privacy policy.[91] Not only did the policy have to be "conspicuously" stated, it also had to clearly state what information was collected and who it

81. *Id.*
82. *Id.*
83. *Id.* at 88.
84. Russell Brandom, *Facebook and Google Hit with $8.8 Billion in Lawsuits on Day One of GDPR*, VERGE (May 25, 2018, 10:21 AM), https://www.theverge.com/2018/5/25/17393766/facebook-google-gdpr-lawsuit-max-schrems-europe.
85. Rob Price, *Facebook is About to be Hit With a 'Flood of Lawsuits' in the EU – But There's a Bigger Threat on the Horizon*, BUS. INSIDER (May 16, 2018, 3:02 PM), https://www.businessinsider.com/facebook-flood-of-lawsuits-eu-post-gdpr-deutsche-bank-2018-5.
86. Pardau, *supra* note 9, at 88.
87. CAL. CONST. art. I, § 1 (emphasis added).
88. Pardau, *supra* note 9, at 89.
89. *Id.*
90. *Id.*
91. *Id.*

was shared with.[92] Knowing the advances California made with internet privacy when it enacted CalOPPA in 2004, it is not surprising California is trying to make the same steps in regard to consumer data collection and personal privacy information with the CCPA.

A. ORIGINS AND PASSING

The CCPA began initially as an initiated measure process.[93] Under California law, one way for an initiated measure is to be included for a popular vote. As stated under the Californian Constitution, "[T]he initiative is the power of the electors to propose statutes and amendments to the Constitution and to adopt or reject them."[94] In order to qualify as an initiative in 2018, the citizen(s) proposing the initiative needed to secure 365,880 votes.[95] Alastair Mactaggart, a real estate magnate, along with Rick Arney, a finance executive, and Mary Stone Ross, who had been legal counsel for the House of Representatives Intelligence Committee brought the initiative forward.[96] They brought over 600,000 votes forward for the initiative, even though, not surprisingly, many tech companies publicly opposed it.[97]

When it was originally drafted, the initiative granted consumers residing only in California three main rights:

> (1) the right to know what data companies have collected about them; where it is sourced from; and how it is being used, sold, or disclosed; (2) the right to 'opt out' of the sale or sharing of their data for business purposes, or the right for consumer under 16 year old not to have their information sold absent their or their parents' 'opt in'; and (3) the right to sue companies that violate the law.[98]

The drafters of the initiative set a deadline of June 28, 2018 for the legislature to either pass privacy legislation that was comparable, or else the initiative would appear on the ballot in November.[99] If the initiative was passed, lawmakers would have little ability to amend the law as ballot initiatives cannot

---

92. *Id.*

93. *Id.*

94. CAL. CONST. art. 2, § 8(a); *see also State Initiative Guide*, CAL. SEC'Y OF STATE, https://elections.cdn.sos.ca.gov/ballot-measures/pdf/statewide-initiative-guide.pdf (last visited May 5, 2020).

95. *Signature Requirements for Ballot Measures in California,* BALLOTPEDIA.ORG, https://ballotpedia.org/Signature_requirements_for_ballot_measures_in_California (last visited May 5, 2020). The number of votes needed to qualify as an initiative was changed in 2019 to 623,212 votes. *Id.*

96. Pardau, *supra* note 9, at 90.

97. *Id.*

98. *Id.* at 91.

99. *Id.*

be amended by the legislature.[100] To avoid this, the legislature quickly introduced Assembly Bill 375, which was substantially similar to the initiative.[101] It was then passed by the legislature on the same day as the deadline.[102] The bill was renamed as the California Consumer Privacy Act.[103]

B. CONTENTS

The CCPA retained the three core rights of the initiative and added a fourth right, namely the right to have a business delete a consumer's personal information.[104] However, certain exceptions would apply.[105]

Generally, the CCPA applies to businesses, rather than individuals.[106] Under the CCPA, a business is defined as:

> [A]ny for-profit entity 'that collects consumers' personal information, or on the behalf of which such information is collected and that alone, or jointly with others, determines the purposes and means of the processing of consumers' personal information, that does business in the State of California.[107]

Further, under the CCPA, a business also needs to satisfy one of the following requirements: the business brings in annual gross revenue "in excess of $25,000,000" it buys, sells, receives or shares the personal information of 50,000 or more "consumers, households, or devices" for commercial purposes or it derives 50% or more of its annual revenues from selling the personal information of its consumers.[108] A business is also defined under the CCPA as "[a]ny entity that controls or is controlled by a business, as defined in [the definition of business under the CCPA], and that shares common branding with the business."[109] Under the CCPA, the definition of a consumer is a "natural person who is a California resident."[110] Personal information is defined as "information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household."[111] There are

100. *Id*.
101. *Id*.
102. *Id*.
103. *Id*.
104. *Id*. at 91-92.
105. *Id*. at 92.
106. *Id*.
107. *Id*.; *see also* CAL. CIV. CODE § 1798.140(c)(1) (West 2020).
108. CAL. CIV. CODE § 1798.140(c)(1)(A)-(C) (West 2020).
109. CAL. CIV. CODE § 1798.140(c)(2) (West 2020).
110. CAL. CIV. CODE § 1798.140(g) (West 2020).
111. CAL. CIV. CODE § 1798.140(o)(1) (West 2020).

numerous examples of personal information included in the CCPA, including names, postal addresses, IP addresses, and social security numbers.[112]

The CCPA gives a number of rights to consumers, notably in sections 1798.100-1798.125.[113] First, consumers can request the business that collected their personal information disclose to them the categories and specific pieces of information the business collected free of charge.[114] Second, under Section 1798.105(a), consumers have the right to ask the business to delete the collected personal information.[115] After the request, the business is required to delete the information from its own records.[116]

Third, under Section 1798.110, consumers also have the right to make other requests from the businesses that collect their information.[117] They have the right to request:

> (1) [The] categories of personal information [it has] collected [about that consumer;] (2) The categories of sources from which the personal information is collected[;] (3) The business or commercial purpose for collecting or selling personal information[;] (4) The categories of third parties with whom the business shares personal information[; and] (5) The specific pieces of personal information [the business] has collected about that consumer.[118]

Fourth, under section 1798.115 of the CCPA,[119] consumers can make the same request from business that sell the consumer's information, where the categories of information are different, such as:

> (1) The categories of personal information that the business collected about the consumer; (2) The categories of personal information that the business sold about the consumer and the categories of third parties to whom the personal information was sold . . . ; (3) The categories of personal information that the business disclosed about the consumer for a business purpose.[120]

Lastly, a business cannot discriminate against a consumer as a result of the consumer exercising any of their rights under the CCPA.[121] The CCPA gives certain examples of discrimination such as denying goods or services

---

112. Pardau, *supra* note 9, at 92.
113. *Id*. at 94.
114. CAL. CIV. CODE § 1798.100(a) (West 2020).
115. CAL. CIV. CODE § 1798.105(a) (West 2020).
116. CAL. CIV. CODE § 1798.105(c) (West 2020).
117. Pardau, *supra* note 9, at 95.
118. *Id*. at 95-96.
119. CAL. CIV. CODE § 1798.115 (West 2020).
120. *Id*.
121. CAL. CIV. CODE § 1798.125 (West 2020).

or providing a different level or quality of goods or services to the consumer.[122]

Along with the rights given to consumers, businesses have certain requirements pertaining to disclosures in their privacy policies.[123] Also, the businesses must inform the consumer which categories of personal information are being collected and inform them of the purpose for which those categories will be used.[124] Businesses also have to allow the consumer to opt-out.[125] Businesses are required to have a conspicuous link on their webpage that is titled "Do Not Sell My Personal Information."[126] They are also required to provide details of the opt-out rights of the consumer.[127]

Under the act, a consumer is granted remedies.[128] Section 1798.150 of the CCPA states:

> [a]ny consumer whose nonencrypted or nonredacted personal information . . . is subject to an unauthorized access and exfiltration, theft, or disclosure as a result 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 may institute a civil action . . . .[129]

The consumer can bring a civil action for statutory damages from $100 to $750 per consumer per incident, or actual damages, whichever is greater of the two.[130] They can also bring an action for injunctive or declaratory relief,[131] or for "[a]ny other relief the court deems proper."[132]

The consumer must satisfy certain requirements before initiating a civil action, if the action is not solely for actual pecuniary damages.[133] They first have to provide the business with 30 days written notice of the CCPA provisions that were violated.[134] The business then has 30 days to cure the breach.[135] If the business fails to cure any alleged violation within 30 days after notification, they are "subject to an injunction and liable for a civil

---

122. Pardau, *supra* note 9, at 97; *see also* CAL. CIV. CODE § 1798.125(a)(1) (West 2020).
123. CAL. CIV. CODE § 1798.130(a)(5) (West 2020).
124. CAL. CIV. CODE § 1798.100(b) (West 2020).
125. CAL. CIV. CODE § 1798.135(a)(1) (West 2020).
126. *Id.*
127. CAL. CIV. CODE § 1798.135(a)(2) (West 2020).
128. CAL. CIV. CODE § 1798.150 (West 2020).
129. *Id.*
130. CAL. CIV. CODE § 1798.150(a)(1)(A) (West 2020).
131. CAL. CIV. CODE § 1798.150(a)(1)(B) (West 2020).
132. CAL. CIV. CODE § 1798.150(a)(1)(C) (West 2020).
133. CAL. CIV. CODE § 1798.150(b) (West 2020).
134. *Id.*
135. *Id.*

penalty of not more than . . . ($2,500) for each violation or . . . ($7,500) for each intentional violation . . . ."[136] The penalties would then be "assessed and recovered in a civil action brought in the name of the people of the State of California by the Attorney General."[137]The CCPA provides for significant penalties for collectors if they violate its provisions.[138] Technological companies, such as Google and Facebook, can be penalized up to $7500 per intentional infraction.[139] If there were multiple infractions involving a large group of individuals, the penalties to these companies could be costly.

The CCPA gives consumers data privacy rights that are unprecedented in American privacy legislation.[140] The provisions of the CCPA return to the consumer control of their personal information, minus exceptions.[141] The consumer, unless it involves an exception, must consent before their personal information is used by the collector.[142] They are also entitled to request and be advised of the purpose for which their information is to be used.[143] The consumer can also request the deletion of the information if they do not agree to its usage.[144]

C. EXCEPTIONS

The CCPA does have exceptions to personal information as it excludes certain types of personal information that are covered by federal privacy laws, such as protected health information that is collected by a covered entity under Health Insurance Portability and Accountability Act (HIPPA).[145] Where the CCPA overlaps with HIPPA, the CCPA "shall not apply to protected or health information that is collected by a covered entity" since both "'protected health information' and 'covered entity' are defined in the HIPPA Privacy Rule."[146]

There are also exceptions which allow a business to refuse a request from the consumer to delete the collected personal information under Section 1798.105(a). If the personal information is necessary to be retained due to

---

136. CAL. CIV. CODE § 1798.155(b) (West 2020).

137. *Id.*

138. *See* CAL. CIV. CODE § 1798.155(b) (West 2020); *see also* CAL. CIV. CODE § 1798.150(a)(1) (West 2020).

139. CAL. CIV. CODE § 1798.155(b) (West 2020).

140. Sara Morrison, *California's New Privacy Law, Explained*, VOX: RECODE (Dec. 30, 2019, 6:50 PM), https://www.vox.com/recode/2019/12/30/21030754/ccpa-2020-california-privacy-law-rights-explained.

141. *Id.*

142. CAL. CIV. CODE § 1798.105 (West 2020).

143. CAL. CIV. CODE § 1798.100 (West 2020).

144. CAL. CIV. CODE § 1798.105 (West 2020).

145. *Id.* at 93.

146. *Id.*

fraud protection, or a legal obligation, then it is exempted from the deletion requirement.[147] The Act also gives an exemption for research, where the business is engaged in "public or peer-reviewed scientific, historical, or statistical research . . . when the businesses' deletion of the information is likely to render impossible or seriously impair the achievement of such research . . . ."[148]

D. POTENTIAL IMPACT AND CONCERNS

The potential impact of the CCPA on the future of privacy law is significant. Before the CCPA, there was limited protection for consumers and their rights to privacy over their personal information in the United States.[149] Lawmakers have failed to update these laws to reflect the challenges to privacy flowing from the current age of technology.[150] Privacy laws are quickly becoming outdated when it comes to the subject of consumer privacy.[151] Many of the federal laws currently in place do not adequately address the challenges relating to the new technological advancements during the past twenty years.[152] The sharing and the efficiency of transfer of data has evolved quickly in society overtaking the pace of our existing laws.

There are concerns by critics of the CCPA that the Act itself can be overly harsh in its penalties and the Act goes beyond what is required for transparency.[153] Currently a coalition of large internet companies, wireless providers, and banks are spearheading bills such as Assembly Bill 1416, seeking to exempt themselves from the scope of the CCPA.[154] However, their lobbying efforts are unlikely to be successful.[155] While the CCPA was enacted quickly to avoid the initial initiative voted on in November and is in need of amendments, the bill is open to amendments even after its enactment.[156] Companies that are subject to the legislation must for the first time, comply with the CCPA and modify the way they collect data.[157] Critics of

147. CAL. CIV. CODE § 1798.105(d) (West 2020).

148. Pardau, *supra* note 9, at 94; *see also* CAL. CIV. CODE § 1798.105(d)(6) (West 2020).

149. Sara Morrison, *California's New Privacy Law, Explained*, VOX: RECODE (Dec. 30, 2019, 6:50 PM), https://www.vox.com/recode/2019/12/30/21030754/ccpa-2020-california-privacy-law-rights-explained.

150. *Id.*

151. *Id.*

152. *Id.*

153. Michael Hitltzik, *Big Business is Trying to Gut California's Landmark Privacy Law*, L.A. TIMES (Apr. 19, 2019, 6:30 AM), https://www.latimes.com/business/hiltzik/la-fi-hiltzik-cal-privacy-act-20190419-story.html.

154. *Id.*

155. *Id.*

156. Pardau, *supra* note 9, at 103.

157. Ivan Guzenko, *How CCPA Will Impact the World's Digital Economy*, FORBES (Oct. 31, 2019, 9:00AM), https://www.forbes.com/sites/forbestechcouncil/2019/10/31/how-ccpa-will-impact-the-worlds-digital-economy/#4294bfc56922.

the CCPA have simply not shown why the entire Act should be voided. However, the CCPA is in need of amendments and the California legislature may modify some of its current provisions. The bill was hastily put together in order to avoid a referendum vote on the initiative.[158] There are improvements that can be made on the powers of the Attorney General, the overall cure period for collectors and clarity on certain definitions under the CCPA. These improvements are discussed later in this note.

The CCPA is the first step in the United States to return the control of one's personal information to the consumer and not to a collector of that information. Without federal laws in place to regulate the collection of data and control of the usage of personal information, the CCPA and state-wide regulations are the next best step to update consumer privacy laws. The CCPA and state-wide regulations are necessary in order to address the impact of numerous technological advances and facilitation of current data sharing practices.

IV. PRIVACY LAWS ACROSS THE UNITED STATES

Since the enactment of the CCPA, ten other states have introduced similar legislation: Hawaii, Maryland, Massachusetts, Mississippi, Nevada, North Dakota, New Mexico, New York, Rhode Island, and Washington.[159] Many of the proposed bills were modeled after the structure of the CCPA but there were areas of variation as well.[160] There are notable differences from the CCPA in these proposed bills.[161] For example, Rhode Island's proposed bill does not have a role for the state Attorney General, either in enforcing

158. Pardau, *supra* note 9, at 91.

159. Rachel R. Marmor, et al., *"Copycat CCPA" Bills Introduced in States Across County*, DAVIS WRIGHT TREMAINE LLP: PRIVACY & SECURITY L. BLOG (Feb. 8, 2019), https://www.dwt.com/blogs/privacy—security-law-blog/2019/02/copycat-ccpa-bills-introduced-in-states-across-cou; *see also* Emily Tabatabai, et al., *State Legislators Joining the Consumer Privacy Protection Party: Introduced CCPA-Like Bills*, ORRICK: TRUST ANCHOR (Mar. 18, 2019), https://blogs.orrick.com/trustanchor/2019/03/18/state-legislators-joining-the-consumer-privacy-protection-party-introduced-ccpa-like-bills/.

160. Rachel R. Marmor, et al., *"Copycat CCPA" Bills Introduced in States Across County*, DAVIS WRIGHT TREMAINE LLP: PRIVACY & SECURITY L. BLOG (Feb. 8, 2019), https://www.dwt.com/blogs/privacy—security-law-blog/2019/02/copycat-ccpa-bills-introduced-in-states-across-cou; *see also* Emily Tabatabai, et al., *State Legislators Joining the Consumer Privacy Protection Party: Introduced CCPA-Like Bills*, ORRICK: TRUST ANCHOR (Mar. 18, 2019), https://blogs.orrick.com/trustanchor/2019/03/18/state-legislators-joining-the-consumer-privacy-protection-party-introduced-ccpa-like-bills/.

161. Rachel R. Marmor, et al., *"Copycat CCPA" Bills Introduced in States Across County*, DAVIS WRIGHT TREMAINE LLP: PRIVACY & SECURITY L. BLOG (Feb. 8, 2019), https://www.dwt.com/blogs/privacy—security-law-blog/2019/02/copycat-ccpa-bills-introduced-in-states-across-cou; *see also* Emily Tabatabai, et al., *State Legislators Joining the Consumer Privacy Protection Party: Introduced CCPA-Like Bills*, ORRICK: TRUST ANCHOR (Mar. 18, 2019), https://blogs.orrick.com/trustanchor/2019/03/18/state-legislators-joining-the-consumer-privacy-protection-party-introduced-ccpa-like-bills/.

the legislation or the formulation of the bill.[162] Further, in Hawaii's proposed bill, a business is not defined and therefore the bill would apply to all businesses that are operating in Hawaii.[163] In Massachusetts' proposed bill, private lawsuits may be brought for any violation of the law, not merely data breaches.[164] Washington's proposed bill also is largely modeled after the GDPR and not the CCPA.[165]

Further, the degree of enforcement differs among the states. While many have copied the $7500 per intentional infraction under the CCPA, New Mexico's legislation enforcement is $10,000 per violation.[166] The disclosures regarding the collection of data also differ, as only Hawaii and New Mexico require the disclosures among the legislation of the ten states mentioned.[167] Hawaii even has the same opt-out link requirement as in the CCPA, with slightly different wordings such as "Do Not Sell My Identifying Information."[168]

These proposed privacy bills have undergone various legislative changes and are at different stages of legislative enactment.[169] The proposed legislation in Mississippi died in committee.[170] The legislation in Washington, Senate Bill 5376, has passed the Washington Senate and is now before the Washington House.[171] The legislation from the other seven states are now in the respective state senates.[172] The proposed legislation in Hawaii, Mississippi, New Mexico, New York, and Rhode Island all have a higher probability of passing and being enacted in the coming years with both chambers of the legislature and the governor's office under the control of the same political

---

162. Rachel R. Marmor, et al., *"Copycat CCPA" Bills Introduced in States Across County*, DAVIS WRIGHT TREMAINE LLP: PRIVACY & SECURITY L. BLOG (Feb. 8, 2019), https://www.dwt.com/blogs/privacy—security-law-blog/2019/02/copycat-ccpa-bills-introduced-in-states-across-cou

163. *Id.*

164. *Id.*

165. *Id.*

166. Emily Tabatabai, et al., *State Legislators Joining the Consumer Privacy Protection Party: Introduced CCPA-Like Bills*, ORRICK: TRUST ANCHOR (Mar. 18, 2019), https://blogs.orrick.com/trustanchor/2019/03/18/state-legislators-joining-the-consumer-privacy-protection-party-introduced-ccpa-like-bills/.

167. Rachel R. Marmor, et al., *"Copycat CCPA" Bills Introduced in States Across County*, DAVIS WRIGHT TREMAINE LLP: PRIVACY & SECURITY L. BLOG (Feb. 8, 2019), https://www.dwt.com/blogs/privacy—security-law-blog/2019/02/copycat-ccpa-bills-introduced-in-states-across-cou.

168. *Id.*

169. *Id.*

170. *Id.*

171. Emily Tabatabai, et al., *State Legislators Joining the Consumer Privacy Protection Party: Introduced CCPA-Like Bills*, ORRICK: TRUST ANCHOR (Mar. 18, 2019), https://blogs.orrick.com/trustanchor/2019/03/18/state-legislators-joining-the-consumer-privacy-protection-party-introduced-ccpa-like-bills/.

172. *Id.*

party.[173] The legislators in North Dakota replaced their proposed law, House Bill (H.B.) 1485, with a Legislative Management Study.[174]

A. CURRENT CONSUMER PRIVACY LAWS IN NORTH DAKOTA AND H.B. 1485

North Dakota has consumer privacy regulations in place, but they are not comparable to the CCPA. Most of the consumer privacy regulations in place are related to financial institutions and health information.[175] However, these laws are contained in the administrative code, not statute.[176] North Dakota Administrative Code Chapter 13-02-21 regulates the disclosure of customer information by financial institutions, while Chapter 45-14-01 contains laws pertaining to privacy of consumer financial and health information.[177] However, North Dakota does not currently have any consumer privacy laws under statutory law.[178]

The state legislature introduced a bill somewhat modeled on the CCPA.[179] H.B. 1485 was introduced on January 14, 2019. The bill was introduced as "A Bill for an Act to create and enact chapter 51-37 of the North Dakota Century Code, relating to protection against the disclosure of personal information; and to provide a penalty."[180]

The overall approach of the bill as stated under the proposed legislation was to "prohibit disclosure of personal information except upon express written consent from the data subject."[181] Further, it states that in order to obtain the individual's express written consent, the entity "shall send by mail or electronic mail a brief, one to two page summary of the terms and conditions of using the covered entity's services."[182] The summary would need to include a "description of how, when, and to and from the covered entity buys, receives, sells and shares an individual's personal information."[183]

---

173. Rachel R. Marmor, et al., *"Copycat CCPA" Bills Introduced in States Across County*, DAVIS WRIGHT TREMAINE LLP: PRIVACY & SECURITY L. BLOG (Feb. 8, 2019), https://www.dwt.com/blogs/privacy—security-law-blog/2019/02/copycat-ccpa-bills-introduced-in-states-across-cou (last visited Dec 16, 2019).

174. *Id*.

175. N.D. ADMIN. CODE ch. 13-02-21, 45-14-01 (2020).

176. N.D. ADMIN. CODE ch. 13-02-21, 45-14-01 (2020).

177. N.D. ADMIN. CODE ch. 13-02-21, 45-14-01 (2020).

178. *See* H.B. 1485, 66th Legis. Assemb., Reg. Sess. (N.D. 2019).

179. H.B. 1485, 66th Legis. Assemb., Reg. Sess. (N.D. 2019) (introduced version).

180. *Id*.

181. *Id*.

182. *Id*.

183. *Id*.

Afterwards, the entity has to receive an affirmative response from the individual, or a parent or legal guardian if the individual is under 18 years old.[184]

Further, a covered entity under the proposed legislation was defined as a "partnership, limited liability company, corporation, or other legal entity that collects consumers' personal information," and conducts business in the state.[185] Additionally, the covered entity must have one or more of the following: "annual gross revenues in excess of twenty-five million dollars; annually buys, receives, sells, or shares personal information of at least fifty thousand consumers, households, or devices; or "[d]erives at least fifty percent of its annual revenues from selling personal information," in order to qualify as a "covered entity" under H.B. 1485.[186] It is similar, but not identical when comparing it to the definition of a "business" under the CCPA.[187]

Next, "personal information" is defined under H.B. 1485 as "information that identifies, describes, or could reasonably be linked with a particular individual."[188] As under the CCPA, publicly available information is not included.[189] The examples of personal information are nearly identical in relation to an individual's personal identifiers.[190] Also, an individual's biometric information[191] and geolocational data[192] are included.[193] H.B. 1485 also included "[i]nternet or other electronic network activity information, including browsing history, search history, and information regarding an individual's interaction with an internet website, application, or advertisement."[194]

---

184. *Id*.

185. *Id*.

186. *Id*.

187. *See* CAL. CIV. CODE § 1798.140(c) (West 2020).

188. H.B. 1485, 66th Legis. Assemb., Reg. Sess. (N.D. 2019) (introduced version).

189. *Id*.; CAL. CIV. CODE § 1798.140(o)(K)(2) (West 2020).

190. H.B. 1485, 66th Legis. Assemb., Reg. Sess. (N.D. 2019) (introduced version); CAL. CIV. CODE § 1798.140(o)(1) (West 2020).

191. Biometric information is defined under the CCPA as "an individual's physiological, biological, or behavioral characteristics, including an individual's deoxyribonucleic (DNA), that can be used, singly or in combination with each other or with other identifying data, to establish individual identity." CAL. CIV. CODE § 1798.140(b) (West 2020). Examples of biometric information are fingerprints or voice recordings. *Id*. The CCPA also cites "sleep, health, or exercise data that contains identifying information" as biometric information. *Id*.

192. Geolocational data is not defined under the CCPA. CAL. CIV. CODE § 1798.140. However, Collins English Dictionary defines geolocation as "the use of technology to find the location of an internet or mobile phone user." *Geolocation*, COLLINS ENGLISH DICTIONARY, https://www.collinsdictionary.com/dictionary/english/geolocation (last visited May 8, 2020). For example, geolocational data can be collected when a person uses their phone so that their internet service provider is able to determine their location through the Global Positioning System (GPS). Daniel Ionescu, *Geolocation 101: How It Works, the Apps, and Your Privacy*, PCWorld (Mar. 29, 2010, 6:45PM), https://www.pcworld.com/article/192803/geolo.html.

193. H.B. 1485, 66th Legis. Assemb., Reg. Sess. (N.D. 2019) (introduced version); CAL. CIV. CODE § 1798.140(o)(1) (West 2020).

194. H.B. 1485, 66th Legis. Assemb., Reg. Sess. (N.D. 2019) (introduced version).

One substantial difference between the CCPA and H.B. 1485 is the word "consumer" was not defined under H.B. 1485, arguably a definition that is needed in a proposed bill that relates to consumer privacy.[195] In future versions of the bill, the term "consumer" must be defined.

Further, an individual's private right of action was different under H.B. 1485 then in the CCPA.[196] Under H.B. 1485, a civil lawsuit was allowed if the individual's personal information was "purchased, received, sold, or shared by a covered entity in violation of this chapter."[197] There was no 30-day waiting period needed before bringing an action or an opportunity for the entity/business to cure under H.B. 1485.[198] There was also no mention of bringing a civil action as a result of the entity being unable to "implement and maintain reasonable security procedures."[199] The individual may then bring the civil action in a court of North Dakota which has jurisdiction over the entity.[200] There, the individual can recover "damages, costs, and fees, including reasonable attorney's fees."[201] There was no stated amount of statutory damages as under the CCPA.[202] Similar to the CCPA, the individual can also obtain injunctive or declaratory relief or "any other relief the court deems proper."[203]

H.B. 1485 was read for the first time and referred to the Industry, Business and Labor Committee.[204] The Committee reported back on February 15, 2019.[205] North Dakota Representative Lefor clarified in the North Dakota House of Representatives, the Committee did not believe there was enough time to fully vet the pros and cons of the bill.[206] However, the Committee believed the discussion to protect consumer privacy was important enough to

---

195. H.B. 1485, 66th Legis. Assemb., Reg. Sess. (N.D. 2019) (introduced version); CAL. CIV. CODE § 1798.140(g) (West 2020).

196. H.B. 1485, 66th Legis. Assemb., Reg. Sess. (N.D. 2019) (introduced version); CAL. CIV. CODE § 1798.150 (West 2020).

197. H.B. 1485, 66th Legis. Assemb., Reg. Sess. (N.D. 2019) (introduced version).

198. H.B. 1485, 66th Legis. Assemb., Reg. Sess. (N.D. 2019) (introduced version); CAL. CIV. CODE § 1798.155(b) (West 2020).

199. H.B. 1485, 66th Legis. Assemb., Reg. Sess. (N.D. 2019) (introduced version); CAL. CIV. CODE § 1798.150(a)(1) (West 2020).

200. H.B. 1485, 66th Legis. Assemb., Reg. Sess. (N.D. 2019) (introduced version).

201. *Id.*

202. H.B. 1485, 66th Legis. Assemb., Reg. Sess. (N.D. 2019) (introduced version); CAL. CIV. CODE § 1798.155(b) (West 2020).

203. H.B. 1485, 66th Legis. Assemb., Reg. Sess. (N.D. 2019) (introduced version); CAL. CIV. CODE § 1798.150(a)(1)(C) (West 2020).

204. N.D. HOUSE, H. JOURNAL, 66th Legis. Assemb., Reg. Sess., at 264 (2019).

205. N.D. HOUSE, H. JOURNAL, 66th Legis. Assemb., Reg. Sess., at 884 (2019).

206. Representative Lefor, Bill Videos for H.B. 1485, 66th Legis. Assemb. Reg. Sess. (February 19, 2019, 2:03PM) (N.D. 2019), https://www.legis.nd.gov/assembly/66-2019/bill-video/bv1485.html

have a study on the issue.[207] Therefore, the Committee recommended the House of Representatives vote in favor of the amended H.B. 1485.[208] Their report stated for the bill to be sent to a Legislative Management Study for Consumer Personal Data Disclosures.[209] As the committee stated in their report:

> During the 2019-20 interim, the legislative management shall study protections, enforcement, and remedies regarding the disclosure of consumers' personal data. The study must include a review of privacy laws of other states and applicable federal law. The legislative management shall report its finding and recommendations, together with any legislation required to implement the recommendations, to the sixty-seventh legislative assembly.[210]

The Sixty-Seventh North Dakota Legislative Assembly is due to begin its session in 2021-22.[211] Until that time, it is uncertain as to if and when a version of the bill will be enacted in North Dakota and what protections, enforcement, and remedies regarding the disclosure of consumers personal data the bill will contain.

B. FUTURE AND NEXT STEPS OF CONSUMER PRIVACY LAW IN NORTH DAKOTA

At this point, the future of consumer privacy law is uncertain in North Dakota. Legislative Management will conduct its study and then report to the Sixty-Seventh North Dakota Legislative Assembly in 2021.[212] Until such time, it is unknown as to how much of the previous text of H.B. 1485 will remain in a new bill, or even if one will be brought forward in the legislative assembly. There are many similarities to the CCPA in H.B. 1485. However, as previously mentioned, H.B. 1485 does not define the term "consumer," nor is the bill as detailed as the CCPA in terms of remedies and its construction.[213] There are notable improvements under H.B. 1485 which should be included under future amendments to the CCPA and future versions of the bill in North Dakota.

The CCPA is not a perfect piece of legislation. The Act was drafted quickly in order to avoid a referendum vote on the initial proposed

---

207. *Id.*
208. *Id.*
209. *Id.*
210. H.B. 1485, 66th Legis. Assemb., Reg. Sess. (N.D. 2019) (amended version).
211. N.D. LEGIS. COUNCIL, 2021 LEGISLATIVE DEADLINES, 21.9019.03000, 67th Legis. Assemb. (2020).
212. *Id.*
213. H.B. 1485, 66th Legis. Assemb., Reg. Sess. (N.D. 2019) (introduced version).

initiative.[214] While it is significant legislation and a worthy first step toward the development of a uniform federal consumer privacy act, there are improvements and amendments that should be made to the legislation and to other state consumer privacy laws as well.

One improvement would be to allow private lawsuits by consumers and taking some of that action out of the hands of the state attorney general. Under the CCPA, a consumer can bring a lawsuit only for data breaches.[215] The consumer should be allowed to bring a lawsuit for other actions other than data breaches. The amount of damages would need to be reasonable, but it would promote better policing of the private sector and promote efficiency by removing the need to involve the office of the attorney general for every action. Involving the attorney general in all actions other than data breaches would tax the already limited resources available to their office. Even if the attorney general were given more resources, it would likely not be enough to police the large number of businesses in this emerging sector California.[216] In allowing these private actions, as Pardau states, "[it] could also help provide more clarity for the business community" concerning certain areas of the CCPA.[217] Allowing greater opportunities for a consumer to bring a lawsuit against a collector other than for a data breach, so long as it is reasonable, would help police the business community.

Second, there should be a longer cure period for collectors under the CCPA or other CCPA modeled legislation. Thirty days is not sufficient to allow the collector to cure a breach in all circumstances.[218] In the case of small violations, 30 days is doable, yet there are larger violations which would require a longer period. There should be the possibility of a flexible curative period for collectors depending on the circumstances. Measures would need to be taken to ensure a collector would not abuse this system and gain a longer curative period for an instance which could reasonably be cured in 30 days.

Third, the definition of "publicly available information" requires a more detailed explanation than what is defined under the CCPA.[219] The statute is vague. Under the CCPA, "publicly available information" is not defined as "publicly available" if the data is "biometric information collected by a business about a consumer without the consumer's knowledge.".[220] Future

214. Pardau, *supra* note 9, at 91.
215. *Id*. at 72-73.
216. *See id*. at 104.
217. *See id*. at 105.
218. *See* CAL. CIVIL CODE § 1798.150(b) (West 2020).
219. *See* CAL. CIVIL CODE § 1798.140(o)(2) (West 2020).
220. *See id*.

amendments may be needed in order to clarify the limits and the types of biometric information included under the definition.

North Dakota made great steps in becoming one of the first ten states to introduce a consumer privacy bill comparable to the CCPA.[221] Instead of taking further steps to enact the bill in its original form, the committee chose instead to have H.B. 1485 sent to Legislative Management for a study with plans to report the findings to the Sixty-Seventh North Dakota Legislative Assembly in 2021.[222] For the future of consumer privacy laws in North Dakota, the report should state a new version of the bill is warranted.. In today's society, where data is constantly shared among individuals, there is more importance than ever to a consumer's privacy and how their information is shared and used by others.

While North Dakota does not need to implement every aspect of the CCPA, more is needed. For example, there must be additions to the definition of a "consumer," "publicly available information" must be more clearly defined, and there should also include a period of 30 days or more where the collector can cure their violation of the statute. However, similar to the CCPA, the legislation can be amended after it becomes law.[223] The Legislative Management report will be given to the North Dakota Legislative Assembly in 2021.[224] After this, it is of particular importance that a bill similar to the original version of H.B. 1485 is passed and implemented.[225] As could likely be the case, similar bills in Hawaii, Mississippi, New Mexico, New York, and Rhode Island could all be enacted or set for enactment by that point in 2021.[226] If the legislature would enact a privacy protection law modeled on the CCPA, it would be a great service to North Dakotan consumers.

V. CONCLUSION

Privacy is extremely important in today's world. There must be a balance between the data being shared with others and one's privacy interest.

---

221. Rachel R. Marmor, et al., *"Copycat CCPA" Bills Introduced in States Across County*, DAVIS WRIGHT TREMAINE LLP: PRIVACY & SECURITY L. BLOG (Feb. 8, 2019), https://www.dwt.com/blogs/privacy—security-law-blog/2019/02/copycat-ccpa-bills-introduced-in-states-across-cou.

222. N.D. HOUSE, H. JOURNAL, 66th Legis. Assemb., Reg. Sess., at 884 (2019).

223. Pardau, *supra* note 9, at 103.

224. H.B. 1485, 66th Legis. Assemb., Reg. Sess. (N.D. 2019) (amended version).

225. *See* Kyle Schryver, *The Future of Data Privacy in the United States*, CPO MAG. (Aug. 1, 2019), https://www.cpomagazine.com/data-protection/the-future-of-data-privacy-in-the-united-states/.

226. Rachel R. Marmor, et al., *"Copycat CCPA" Bills Introduced in States Across County*, DAVIS WRIGHT TREMAINE LLP: PRIVACY & SECURITY L. BLOG (Feb. 8, 2019), https://www.dwt.com/blogs/privacy—security-law-blog/2019/02/copycat-ccpa-bills-introduced-in-states-across-cou.

However, with information being shared, it is imperative that consumers have control over how their data is used and the right to refuse the usage if they do not consent to the purpose. Further, a business or collector of that personal information should need to advise the consumer how they will utilize the data. Consumers should be aware and be in control of how their personal information is shared to the world.

The Cambridge Scandal opened the world's eyes to large technological companies utilizing personal information of its users without their consent.[227] The CCPA is the first step to rein in a collector's usage of a consumer's data and revert control and consent back to the consumer. While not perfect legislation, it is the logical first step toward limiting and protecting the usage of a consumer's data. Since there is no uniform federal consumer privacy law, the CCPA has inspired other state legislation, with ten states so far introducing legislation similar to the CCPA.[228]

North Dakota is in the enviable situation where a bill similar to the CCPA was brought forward and it is now in a Legislative Management study, with a report expected to be ready by 2021[229] Legislators of North Dakota now have a chance to bring a consumer privacy law in the next few years to include other provisions that were not in H.B. 1485. They also can bring improvements to the bill as well as provisions that are not included in the CCPA. While re-enacting the entire CCPA is unnecessary, North Dakota should have a consumer privacy law passed. This law should echo many provisions of the CCPA and contain aspects of H.B. 1485's original text included in the legislation. A hybrid of those two pieces of legislation will be the most beneficial to North Dakotans.

*Paul Monnin**

---

227. Nikhill Rajesh, *Cambridge Analytica Scandal Explained*. SIMPLE SNIPPETS (Mar. 27, 2018, 5:24 PM), https://simplesnippets.tech/cambridge-analytica-scandal-explained/.

228. Rachel R. Marmor, et al., *"Copycat CCPA" Bills Introduced in States Across County*, DAVIS WRIGHT TREMAINE LLP: PRIVACY & SECURITY L. BLOG (Feb. 8, 2019), https://www.dwt.com/blogs/privacy—security-law-blog/2019/02/copycat-ccpa-bills-introduced-in-states-across-cou.

229. N.D. HOUSE, H. JOURNAL, 66th Legis. Assemb., Reg. Sess., at 884 (2019).

*2020 J.D. Graduate from the University of North Dakota School of Law. Thank you to my parents, Marc and Donna, for their love and support. A very special thank you to Professor Emeritus Patti Alleva for her mentorship and guidance. Also, thank you to Dean Michael McGinniss and Associate Dean for Academic and Student Affairs and Associate Professor Julia Ernst for their advice and encouragement throughout my three years at the University of North Dakota School of Law. I also thank the North Dakota Law Review Board of Editors and my fellow North Dakota Law Review members for their helpful comments and their improvements to this note.