AB 2182 and Chapter 55: Enacting Privacy Regulations in the Face of Legislative Complacency

*Thomas Gerhart**

Code Sections Affected

Civil Code § 1798.82 (amended); Title 1.81.5 (commencing with §1798.100) to Part 4 of Division 3 of the Civil Code (new).
AB 2182 (Levine); AB 375 (Chau, Hertzberg); 2018 Stat. Ch. 55.

TABLE OF CONTENTS

* J.D. Candidate, University of the Pacific, McGeorge School of Law, to be conferred May 2021; B.A. Medieval and Early Modern Studies, University of California, Davis, 2005. I would have never achieved this dream without the support of my loving wife Jennifer and my Border Collie Lyra. Your love and fetch keep me going. A thousand thanks to my mother-in-law Carolee and the Austria A-Team. I shall always persevere with you in my corner. "With law our land shall rise, but it will perish with lawlessness." -Njáll Þorgeirsson

I. INTRODUCTION

On March 17, 2018, the tip of the data protection iceberg became public when news broke that Cambridge Analytica harvested the personally identifiable information ("PII") of 50 million Facebook users without consent.[1] The world learned that Cambridge Analytica, a political consulting firm,[2] had obtained PII from up to 87 million Facebook users.[3] Many of these users had not consented to the consulting firm accessing their PII.[4] Facebook, a business that collects its users' PII and generates personalized advertisements based on that data,[5] conceded that Cambridge Analytica had improperly accessed many Facebook users' information.[6]

Cambridge Analytica conducted a survey within Facebook and accessed PII from both consenting and non-consenting users.[7] Approximately 270,000 consenting users voluntarily took Cambridge Analytica's survey, downloaded a computer application ("app"), and gave Cambridge Analytica permission to collect their PII through the app.[8] Unfortunately, the app also accessed

1. Sam Meredith, *Facebook-Cambridge Analytica: A Timeline of the Data Hijacking Scandal*, CNBC (Apr. 10, 2018, 9:21 AM), https://www.cnbc.com/2018/04/10/facebook-cambridge-analytica-a-timeline-of-the-data-hijacking-scandal.html (on file with *The University of the Pacific Law Review*).

2. *About Us*, CAMBRIDGE ANALYTICA, https://ca-political.com/ca-advantage (last visited May 23, 2018) (on file with *The University of the Pacific Law Review*).

3. Natasha Singer, *What You Don't Know About How Facebook Uses Your Data*, N.Y. TIMES (Apr. 11, 2018), https://www.nytimes.com/2018/04/11/technology/facebook-privacy-hearings.html (on file with *The University of the Pacific Law Review*).

4. Matthew Rosenberg, Nicholas Confessore & Carole Cadwalladr, *How Trump Consultants Exploited the Facebook Data of Millions*, N.Y. TIMES (Mar. 17, 2018), https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html [hereinafter Rosenberg, Confessore & Cadwalladr] (on file with *The University of the Pacific Law Review*).

5. *All Things Considered: What Facebook is Changing About its Data-Sharing Practices*, NPR (Apr. 5, 2018), https://www.npr.org/2018/04/05/599895248/what-facebook-is-changing-about-its-data-sharing-practices [hereinafter *All Things Considered: What Facebook is Changing About its Data-Sharing Practices*] (on file with *The University of the Pacific Law Review*); *Data Policy*, FACEBOOK, https://www.facebook.com/full_data_use_policy (last updated Apr. 19, 2018) (on file with *The University of the Pacific Law Review*).

6. *All Things Considered: What Facebook is Changing About its Data-Sharing Practices*, *supra* note 5.

7. Rosenberg, Confessore & Cadwalladr, *supra* note 4.

8. *Id.*

information from individuals connected to those consenting users.[9] At the time of the breach, Facebook permitted businesses to access non-consenting users' information.[10] Non-consenting users did not take the survey, download the app, or give Cambridge Analytica permission to access their PII.[11] In short, Cambridge Analytica failed to obtain consent from a vast majority of the Facebook users whose PII it accessed.[12]

Marc Levine, Assemblymember for California's Tenth District,[13] proposed AB 2182 to "catch up with [technology]" and eliminate ways that businesses misuse and abuse Californians' PII.[14] He wanted to hold "Big Tech" accountable by creating a regulatory body to ensure privacy regulations evolve with the inevitable advancements in data collection.[15] Pressured by the Big Tech lobby, both the Assembly and the Senate revised AB 2182 and removed its ability to create regulations.[16] As modified, AB 2182 will not generate new data protection regulations and will do nothing to further protect Californians' privacy.[17]

While Big Tech lobbyists dismembered AB 2182, a real estate developer from San Francisco qualified a ballot measure for the November election.[18] Years of planning, research, and hard work from Alastair Mactaggart and Rick Arney culminated in the creation of Chapter 55.[19] Mactaggart and Arney are the embodiment of former President Obama's 2013 challenge: "[If] you don't like a particular policy . . . Then argue for your position. Go out there and win an election. Push to change it."[20] The pair submitted nearly double the amount of signatures required to qualify a ballot measure,[21] leveraged their measure to force

---

9. *Id.*

10. *Id.*

11. *Id.*

12. *Id.*

13. Marc Levine, *California Must Regulate How Big Tech Uses Our Data*, S.F. CHRON. (Mar. 23, 2018), https://www.sfchronicle.com/opinion/openforum/article/California-must-regulate-how-Big-Tech-uses-our-12777734.php (on file with *The University of the Pacific Law Review*).

14. Telephone Interview with Marc Levine, Assemblymember, Cal. Assembly (June 20, 2018) (notes on file with *The University of the Pacific Law Review*).

15. ASSEMBLY COMMITTEE ON PRIVACY & CONSUMER PROTECTION, COMMITTEE ANALYSIS OF AB 2182, at 2 (May 25, 2018); *see also* Will Oremus, *Big Tobacco. Big Pharma. Big Tech?*, SLATE (Nov. 17, 2017), http://www.slate.com/articles/technology/technology/2017/11/how_silicon_valley_became_big_tech.html (on file with *The University of the Pacific Law Review*) (defining "Big Tech" as "Google, Facebook, Amazon, Microsoft, and Apple").

16. AB 2182, 2018 Leg., 2017–2018 Sess. (Cal. 2018) (as amended on May 25, 2018, but not enacted).

17. Telephone Interview with Marc Levine, *supra* note 14.

18. Levi Sumagaysay, *Privacy in California: Ballot Measure Qualifies, Bill Advances*, MERCURY NEWS (June 26, 2018, 5:15 PM), https://www.mercurynews.com/2018/06/26/privacy-in-california-ballot-measure-qualifies-bill-advances/ (on file with *The University of the Pacific Law Review*).

19. *About Us*, CAL. CONSUMER PRIVACY ACT, https://www.caprivacy.org/about-us (last visited Aug. 9, 2018) (on file with *The University of the Pacific Law Review*).

20. Chris Cillizza, *President Obama to Republicans: I won. Deal with it*, WASH. POST (Oct. 17, 2013), https://www.washingtonpost.com/news/the-fix/wp/2013/10/17/president-obama-to-republicans-i-won-deal-with-it/ (on file with *The University of the Pacific Law Review*).

21. *About Us*, CAL. CONSUMER PRIVACY ACT, *supra* note 19.

legislators to act, and defeated the tech lobby with the passage of Chapter 55.[22] In a world where money and lobbying have immense influence over legislative decisions, Mactaggart and Arney provided a blueprint for Californians to overcome wealthy lobbies and enact common-sense privacy legislation.[23]

II. LEGAL BACKGROUND

Historically, legislation has lagged behind technological developments.[24] For example, the United States Patent and Trademark Office granted Alexander Graham Bell a patent for the telephone on March 7, 1876.[25] It was not until 1994 that Congress passed the Telemarketing and Consumer Fraud and Abuse Prevention Act, which focused on protecting consumers from "telemarketing deception and abuse."[26] Today, technology is developing exponentially faster than before,[27] and the telephone/telemarketer paradigm resurfaced with PII and Big Tech.[28] States are beginning to realize that Big Tech collects information from individuals that are on and offline.[29]

Although the Supreme Court discussed the right to privacy, and other countries enacted legislation to protect their citizens' privacy, this right never materialized anywhere in the United States.[30] Section A of this part presents the

22. Ben Adler, *California Passes Strict Internet Privacy Law with Implications for the Country*, NPR (June 29, 2018, 5:05 AM), https://www.npr.org/2018/06/29/624336039/california-passes-strict-internet-privacy-law-with-implications-for-the-country (on file with *The University of the Pacific Law Review*).

23. *See id.* (conquering "a trillion-dollar goliath" with $3.5 million).

24. Vivek Wadhwa, *Laws and Ethics Can't Keep Pace with Technology*, MIT TECH. REV. (Apr. 15, 2014), https://www.technologyreview.com/s/526401/laws-and-ethics-cant-keep-pace-with-technology/ (on file with *The University of the Pacific Law Review*).

25. U.S. Patent No. 117,465 (filed Feb. 14, 1876).

26. 15 U.S.C.A. § 6101 (Westlaw through Pub. L. No. 115-231).

27. Wadhwa, *supra* note 24.

28. *See* Will Oremus, *Big Tobacco. Big Pharma. Big Tech?*, SLATE (Nov. 17, 2017), http://www.slate.com/articles/technology/technology/2017/11/how_silicon_valley_became_big_tech.html (on file with *The University of the Pacific Law Review*) (pointing to Big Tech's agenda of self-regulation and moving slowly toward achieving that goal); *see also* Jason Morris & Ed Lavandera, *Why Big Companies Buy, Sell Your Data*, CNN (Aug. 23, 2012), https://www.cnn.com/2012/08/23/tech/web/big-data-acxiom/index.html (on file with *The University of the Pacific Law Review*) (indicating that cyberspace is outpacing legislation).

29. Telephone Interview with Marc Levine, *supra* note 14.

30. *See* 15 U.S.C.A. § 6801 (Westlaw through Pub. L. No. 115-231) (pertaining only to financial institutions); *see also* 5 U.S.C.A. § 552(a) (Westlaw through Pub. L. No. 115-231) (defining records as "information about an individual maintained by a [government] agency"); Time, Inc. v. Hill, 385 U.S. 374, 415 (1967) ("Privacy, then, is a basic right."); Griswold v. Conn., 381 U.S. 479, 483 (1965) ("[T]he First Amendment has a penumbra where privacy is protected from governmental intrusion"); Mapp v. Ohio, 367 U.S. 643, 656 (1961) ("The right to privacy, no less important than any other right carefully and particularly reserved to the people, would stand in marked contrast to all other rights declared as 'basic to a free society.'"); *see generally* Regulation 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) 1 [hereinafter GDPR] (regulating PII in the EU).

federal government's lack of privacy regulations.[31] Section B discusses the European Union's ("EU") recent privacy regulation.[32] Section C reflects upon California's early attempts at privacy regulations.[33] Section D explores California's current privacy regulations.[34]

A. The Federal Government and Data Protection

Article I, Section 8 of the Constitution lists the powers delegated to Congress,[35] and the Tenth Amendment limits those powers by reserving non-delegated powers to the states.[36] In short, the Framers empowered the states to regulate areas where no law existed.[37] The United States Constitution makes no mention of privacy, and the Supreme Court has offered minimal guidance on the subject.[38] In the 1960s, the Supreme Court declared that "the right of privacy is a fundamental personal right,"[39] and yet the federal government has remained virtually silent when it comes to protecting the privacy of United States citizens on the Internet.[40]

The Supreme Court recognized a right to privacy on three separate occasions.[41] First, in 1961, the Court stated that "the right to privacy . . . [is] no less important than any other right" and it is "basic to a free society."[42] Then, in 1965, the Supreme Court cited the Ninth Amendment to justify the right to privacy.[43] The Ninth Amendment states, the rights enumerated in "the Constitution . . . shall not be construed to deny . . . [other rights] retained by the people."[44] Finally, in 1967, the right to privacy reemerged in a dissent where Justice Fortas asserted that "Privacy . . . is a basic right" and "the states may . . . enact laws to vindicate that right."[45]

The legislature responded to the Supreme Court's acknowledgement of the

---

31. *Infra* Part II.A.

32. *Infra* Part II.B.

33. *Infra* Part II.C.

34. *Infra* Part II.D.

35. U.S. CONST. art. I, § 8.

36. U.S. CONST. amend. X.

37. *See id.* (reserving undelegated powers to the states).

38. *See generally* U.S. CONST. (making no mention of the word "privacy"); *see also* Time, Inc. v. Hill, 385 U.S. 374, 415 (1967) ("Privacy, then, is a basic right.").

39. Griswold v. Conn., 381 U.S. 479, 494 (1965).

40. *See Protecting Consumers Privacy*, FED. TRADE COMM'N, https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy (last visited June 23, 2018) (on file with *The University of the Pacific Law Review*) (regulating financial and children's privacy but not individual privacy).

41. *Time, Inc.*, 385 U.S. at 415; *Griswold*, 381 U.S. at 483; Mapp v. Ohio, 367 U.S. 643, 656 (1961).

42. *Mapp*, 367 U.S. at 656.

43. *Griswold*, 381 U.S. at 490.

44. U.S. CONST. amend. IX.

45. *Time, Inc.*, 385 U.S. at 415.

right to privacy by passing a series of privacy laws between 1970 and 1999.[46] Congress enacted the Fair Credit Reporting Act ("FCRA") in 1970, which focused on consumer privacy in credit reporting agencies.[47] Congress expanded privacy regulations by passing the Privacy Act of 1974, which only applies to government records.[48] Then, in 1999, Congress passed the Gramm-Leach-Bliley Act, which codified a list of mandatory privacy rules for financial institutions.[49] Though all three pieces of legislation implemented privacy protections, no modern regulations protect privacy from commercial abuses on the Internet.[50]

B. The European Union and Data Protection

The Facebook/Cambridge Analytica data breach alerted the public to commercial abuses of PII and the need for an official right to privacy on the Internet.[51] Both companies have since come under heavy international scrutiny.[52] Prior to the breach, the EU was well aware of the need to regulate information privacy.[53] In fact, the EU had already affirmed its citizens' right to Internet privacy in court and adopted legislation to protect its citizens from commercial data abuses.[54]

The Council of Europe signed the European Convention on Human Rights ("ECHR") in 1950.[55] The ECHR is an international treaty that proclaims essential human rights and freedoms,[56] many of which run parallel to the United States' Bill of Rights.[57] For example, Section 1 of the ECHR guarantees citizens the

46. 15 U.S.C.A. § 1681(a) (Westlaw through Pub. L. No. 115-231); 15 U.S.C.A. § 6801 (Westlaw through Pub. L. No. 115-231); 15 U.S.C.A. § 6101 (Westlaw through Pub. L. No. 115-231); 5 U.S.C.A. § 552(a) (Westlaw through Pub. L. No. 115-231).

47. 15 U.S.C.A. § 1681.

48. 5 U.S.C.A. §§ 551–552(a).

49. 15 U.S.C.A. § 6801.

50. 15 U.S.C.A. § 1681; 15 U.S.C.A. § 6801; 5 U.S.C.A. §§ 551–552(a).

51. Meredith, *supra* note 1.

52. Matthew Rosenberg & Sheera Frenkel, *Facebook's Role in Data Misuse Sets Off Storms on Two Continents*, N.Y. TIMES (Mar. 18, 2018), https://www.nytimes.com/2018/03/18/us/cambridge-analytica-facebook-privacy-data.html (on file with *The University of the Pacific Law Review*).

53. *See* GDPR, *supra* note 30, at 1 (drafting the GDPR two years before the Facebook/Cambridge Analytica data breach); *see also* Seung Lee, *California Legislator Introduces Bill to Regulate How Silicon Valley Uses Your Data*, MERCURY NEWS (Feb. 13, 2018, 4:41 AM), https://www.mercurynews.com/2018/02/12/182uropa182nia-assemblymember-introduces-bill-to-regulate-silicon-valleys-data/ (on file with *The University of the Pacific Law Review*) (proposing the privacy legislation one day before the news article was published).

54. Case C-131/12, Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos, Mario Costeja González, 2014 E.C.R. I-317; *Make Me Smart: It's a GDParty*, MINN. PUB. RADIO (May 24, 2018), https://www.marketplace.org/2018/05/24/tech/make-me-smart-kai-and-molly/66-its-gdparty (on file with *The University of the Pacific Law Review*).

55. European Convention on Human Rights, June 1, 2010, C.E.T.S. No. 194, art. 8 [hereinafter ECHR].

56. Charter of Fundamental Rights of the European Union, Oct. 26, 2012, 2012 O.J. (326/391), pmbl. [hereinafter ECFR].

57. *Compare* ECHR, *supra* note 55, at arts. 6, 9–11 (declaring freedoms of expression, religion, press, assembly, and the right to a fair trial), *with* U.S. CONST. amends. I, VI (guaranteeing freedoms of speech,

right to a fair trial, freedom of expression, freedom of religion, and freedom of assembly.[58] Further, the ECHR guarantees many rights that have emerged in the United States since the ratification of the Bill of Rights, including the right to marry, and prohibitions on slavery and discrimination.[59]

In 2007, the EU ratified the Treaty of Lisbon, which amended and enacted the European Charter of Fundamental Rights ("ECFR").[60] The ECFR, not to be confused with the ECHR, is the EU's modern declaration of fundamental rights.[61] Article 7 of the ECFR guarantees the right to respect for a person's private life.[62] Article 8 of the ECFR states, "everyone has the right to the protection of personal data concerning him or her" and discusses topics such as consent and data use.[63]

In a 2014 case, the EU Court of Justice cited Articles 7 and 8 of the ECFR in a judgment against Big Tech.[64] The court ruled that an individual may request the removal of his or her information from an Internet search engine's search results.[65] In its holding, the court discussed the balance between a legitimate Internet user's interest in the PII and the "data subject's fundamental rights" to privacy and the protection of his or her personal data.[66]

In April 2016, the EU approved the General Data Protection Regulation ("GDPR"),[67] which took effect on May 25, 2018.[68] The GDPR gave every citizen of an EU member state complete control over his or her PII.[69] It also placed many restrictions on PII, including limitations on what businesses may do with Europeans' PII.[70] The GDPR is the most expansive privacy regulation addressing data protection on the Internet, and experts anticipate that the regulation will cause a lasting impact in the privacy community.[71]

---

religion, press, assembly, and the right to a fair trial).

58. ECHR, *supra* note 55, at arts. 6, 9–11.

59. *Id.* at arts. 4, 12, 14.

60. Treaty of Lisbon Amending the Treaty on European Union and the Treaty Establishing the European Community, Dec. 13, 2007, 2007 O.J. (C 306) 1.

61. ECFR, *supra* note 56, at pmbl.

62. *Id.* at art. 7.

63. *Id.* at art. 8.

64. Case C-131/12, Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos, Mario Costeja González, 2014 E.C.R. I-317.

65. *Id.*

66. Court of Justice of the European Union, Judgment in Case C-131/12, Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González, (2014), https://curia.europa.eu/jcms/upload /docs/application/pdf/2014-05/cp140070en.pdf (on file with *The University of the Pacific Law Review).*

67. Andrew Rossow, *The Birth of GDPR: What Is It and What You Need to Know*, FORBES (May 25, 2018, 7:32 AM), https://www.forbes.com/sites/andrewrossow/2018/05/25/the-birth-of-gdpr-what-is-it-and-what-you-need-to-know/ (on file with *The University of the Pacific Law Review*).

68. *Id.*

69. GDPR, *supra* note 30, at 2–3.

70. *Id.* at 7.

71. *The Future of U.S. Data Privacy After the GDPR*, COUNCIL ON FOREIGN REL., https://www.cfr.org /event/future-us-data-privacy-after-gdpr (last visited Aug. 11, 2018) (on file with *The University of the Pacific Law Review*).

C. California's Initial Attempts to Regulate Data Protection

California has traditionally been at the forefront of privacy law.[72] In fact, California is one of only ten states guaranteeing the right to privacy in its constitution.[73] The California Constitution guarantees its citizens "the right to pursue and obtain privacy,"[74] but recent advances in technology have enabled Big Tech to encroach upon these rights in new and creative ways.[75] Therefore, California is looking to regulate data protection once again.[76]

In 2010, California created the Office of Privacy Protection ("OPP") "to protect the privacy of individuals' personal information in a manner consistent with the California Constitution."[77] The California Legislature tasked the OPP with making "recommendations to organizations for privacy policies and practices that promote and protect the interests of [California consumers]."[78] However, in early 2011, California Governor Jerry Brown announced a budget cut that slashed government spending by 12.5 billion dollars in an effort to increase government efficiency while reducing its cost.[79] Unfortunately, the OPP was a casualty of those budget cuts, and although it still exists statutorily, it ceased operations in 2012.[80] After the OPP disbanded, its director transitioned to the Office of the Attorney General ("OAG") and assumed control of the newly created Privacy Enforcement and Protection Unit.[81]

D. The Scope of the Privacy Enforcement and Protection Unit

The OAG established the Privacy Enforcement and Protection Unit to "enforce state and federal privacy laws" regulating the "collection . . . of

---

72. Jan Willem Knibbe, *From California with Love, The Latest Privacy Law*, RW CONNECT (Aug. 24, 2018), https://rwconnect.esomar.org/from-california-with-love-the-latest-privacy-law/ (on file with *The University of the Pacific Law Review*).

73. *Privacy Protections in State Constitutions*, NAT'L CONF. OF ST. LEGS. (May 5, 2017), http://www.ncsl.org/research/telecommunications-and-information-technology/privacy-protections-in-state-constitutions.aspx (on file with *The University of the Pacific Law Review*).

74. CAL. CONST. art. I, § 1.

75. Jemima Kiss, *Does Technology Pose a Threat to Our Private Life?*, THE GUARDIAN (Aug. 20, 2010, 7:06 PM), https://www.theguardian.com/technology/2010/aug/21/facebook-places-google (on file with *The University of the Pacific Law Review*).

76. *See* AB 2182, 2018 Leg., 2017–2018 Sess. (Cal. 2018) (as amended on Mar. 15, 2018, but not enacted) (proposing regulations that may limit data collection).

77. CAL. GOV'T. CODE § 11549.5 (West 2018).

78. *Id.*

79. *Governor Brown's Budget Slashes State Spending by $12.5 Billion*, OFF. OF GOVERNOR EDMUND G. BROWN JR. (Jan. 10, 2010), https://www.gov.ca.gov/2011/01/10/news16872/ (on file with *The University of the Pacific Law Review*).

80. ASSEMBLY COMMITTEE ON PRIVACY & CONSUMER PROTECTION, COMMITTEE ANALYSIS OF AB 2182, at 2 (May 25, 2018).

81. *Id.*

information by individuals, organizations, and the government."[82] Data collection regulations diverge into two distinct categories: one category is applicable to government agencies, and the other to businesses.[83] Subsection 1 examines the regulations applicable to government agencies,[84] while Subsection 2 explains the regulations applicable to businesses.[85]

1. Data Collection Regulations Applicable to Government Agencies

The California Information Practices Act ("IPA") acknowledges the sophistication of technology and privacy risks that result from data collection.[86] The IPA reaffirms Californians' constitutional right to privacy and indicates that "the lack of effective laws" threaten that right.[87] Embracing the principle that less is more, the IPA limits the amount and type of information a government agency may collect.[88] A government entity may only collect information "necessary to accomplish [its] purpose."[89] Also, the IPA requires state agencies to collect information directly from individuals, "to the greatest extent practicable," instead of collecting it from third parties.[90] When collecting information electronically, government agencies must provide individuals with various notices.[91] Finally, agencies must obtain consent prior to sharing an individual's information with a third party.[92]

2. Data Collection Regulations Applicable to Businesses

The California Online Privacy Protection Act requires the operator of a commercial website that collects PII to publish its privacy policy in a conspicuous location on its website.[93] A privacy policy must contain the information that the business collects and indicate the categories of third parties that receive the information the business shares.[94] California law also prohibits

82. *Id.*

83. *Compare* CAL. CIV. CODE §§ 1798.14–1798.22 (West 2018) (regulating how government agencies may collect PII), *with* CAL. BUS. & PROF. CODE § 22575 (West 2018) (mandating that businesses publish privacy policies on their websites), *and* CAL. BUS. & PROF. CODE § 22580 (West 2018) (prohibiting businesses from marketing products to minors who cannot legally purchase those goods).

84. *Infra* Part II.D.1.

85. *Infra* Part II.D.2.

86. CAL. CIV. CODE § 1798.1 (West 2018).

87. *Id.*

88. CAL. CIV. CODE § 1798.14 (West 2018).

89. *Id.*

90. CAL. CIV. CODE § 1798.15 (West 2018).

91. CAL. GOV'T CODE § 11015.5 (West 2018).

92. *Id.*

93. CAL. BUS. & PROF. CODE § 22575 (West 2018).

94. *Id.*

specific, targeted marketing on websites designed for minors.[95] These websites may not market goods or services to minors who cannot legally purchase the advertised goods or services.[96]

Additionally, a website's privacy policy must disclose how the business responds to a web browser's "do not track" ("DNT") signal.[97] Most major websites track their visitors' browsing behaviors, but some web browsers allow consumers to enable a DNT signal.[98] This signal communicates to websites that the consumer does not want his or her activity recorded.[99] California law requires that a commercial website disclose how the business responds to a DNT signal, but the law does not require the website to comply with the request.[100]

III. AB 2182 AND CHAPTER 55

Like the EU and its adoption of the GDPR, the California Legislature did not draft AB 2182 in response to the Facebook/Cambridge Analytica data breach.[101] In fact, the California Assembly had read AB 2182 twice, and amended it once, before news of Cambridge Analytica's improprieties became public.[102] Section A discusses the regulatory body that AB 2182 would have created.[103] Section B describes the substantial changes that the Assembly made to AB 2182.[104] Section C briefly analyzes the minor changes that the Senate made to AB 2182 before Chapter 55 came into existence.[105] Finally, Section D explains various provisions of Chapter 55—the first Internet privacy law in the United States focused on protecting individuals' PII.[106]

---

95. CAL. BUS. & PROF. CODE § 22580 (West 2018).

96. *Id.*

97. CAL. BUS. & PROF. CODE § 22575; ASSEMBLY COMMITTEE ON PRIVACY & CONSUMER PROTECTION, COMMITTEE ANALYSIS OF AB 2182, at 2 (Apr. 17, 2018); CAL. DEP'T. OF JUST., MAKING YOUR PRIVACY PRACTICES PUBLIC 7 (May 2014), *available at* https://www.oag.ca.gov/sites/all/files/agweb/pdfs/cybersecurity/making_your_privacy_practices_public.pdf? (on file with *The University of the Pacific Law Review*).

98. *How Do I Turn On the Do Not Track Feature*, FIREFOX, https://support.mozilla.org/en-US/kb/how-do-i-turn-do-not-track-feature (last visited June 23, 2018) (on file with *The University of the Pacific Law Review*).

99. *Id.*

100. CAL. BUS. & PROF. CODE § 22575; ASSEMBLY COMMITTEE ON PRIVACY & CONSUMER PROTECTION, COMMITTEE ANALYSIS OF AB 2182, at 2 (Apr. 17, 2018); CAL. DEP'T. OF JUST. MAKING YOUR PRIVACY PRACTICES PUBLIC 7 (2014), *available at* https://www.oag.ca.gov/sites/all/files/agweb/pdfs/cybersecurity/ making_your_privacy_practices_public.pdf? (on file with *The University of the Pacific Law Review*).

101. AB 2182, *supra* note 16.

102. *Id.*

103. *Infra* Part III.A.

104. *Infra* Part III.B.

105. *Infra* Part III.C.

106. *Infra* Part III.D.

A. AB 2182 and the California Data Protection Authority

AB 2182, as proposed by Assemblymember Levine, intended to protect Californians' PII by establishing the California Data Protection Authority ("CDPA").[107] Assemblymember Levine designed the CDPA to propose new regulations that would evolve with Big Tech's rapid development.[108] Further, AB 2182 required businesses to delete a customer's PII when their business relationship ends.[109] Finally, the CDPA would evaluate whether "state and federal personal information protection laws" were adequate when juxtaposed with California's data breach laws.[110] Due to potentially high costs,[111] the Committee on Privacy and Consumer Protection placed AB 2182 on the suspense file for reevaluation.[112]

B. The California Assembly's Modifications to AB 2182

The Department of Consumer Affairs' (DCA) mission statement is to "protect California consumers by providing a safe and fair marketplace through oversight, enforcement, and licensure of professions."[113] The Assembly modified AB 2182, it required the DCA to create a centralized directory where consumers could access the privacy policies of commercial Internet platforms.[114] This change reduced the overall cost of the proposed bill,[115] but it also stripped AB 2182 of its ability to generate privacy regulations.[116] When AB 2182 moved from the Assembly to the Senate, legislators refocused the bill to inform consumers about the existence of privacy policies rather than protect consumer privacy.[117]

---

107. ASSEMBLY COMMITTEE ON PRIVACY & CONSUMER PROTECTION, COMMITTEE ANALYSIS OF AB 2182, at 3 (Apr. 17, 2018).

108. Telephone Interview with Marc Levine, *supra* note 14.

109. ASSEMBLY COMMITTEE ON PRIVACY & CONSUMER PROTECTION, COMMITTEE ANALYSIS OF AB 2182, at 1 (Apr. 17, 2018).

110. *Id.*

111. ASSEMBLY COMMITTEE ON PRIVACY & CONSUMER PROTECTION, COMMITTEE ANALYSIS OF AB 2182, at 1 (May 9, 2018).

112. Complete Bill History of AB 2182, http://leginfo.legislature.ca.gov/faces/billHistoryClient.xhtml? bill_id=201720180AB2182 (last visited Aug. 12, 2018) (on file with *The University of the Pacific Law Review*).

113. CAL. DEP'T. OF CONSUMER AFF., WHO WE ARE AND WHAT WE DO 5 (2014), *available at* http://www.dca.ca.gov/publications/dca_booklet.pdf (on file with *The University of the Pacific Law Review*).

114. AB 2182, *supra* note 16.

115. *Compare* ASSEMBLY COMMITTEE ON PRIVACY & CONSUMER PROTECTION, COMMITTEE ANALYSIS OF AB 2182, at 1 (May 9, 2018) (projecting significant annual costs as a result of the legislation), *with* ASSEMBLY COMMITTEE ON PRIVACY & CONSUMER PROTECTION, COMMITTEE ANALYSIS OF AB 2182, at 2 (May 25, 2018) (anticipating minor costs to operate the website).

116. Telephone Interview with Marc Levine, *supra* note 14.

117. *See* AB 2182, *supra* note 16 (containing no regulatory powers but mandating a website for consumers).

C. The California Senate's Modifications to AB 2182

When AB 2182 arrived at the Senate, it contained provisions requiring the DCA to provide California consumers with a centralized repository of privacy policies.[118] Mirroring the OAG's 2012 absorption of the DCA's privacy enforcement duties,[119] the Senate amended the bill and shifted web portal operation from the DCA to the OAG.[120] Following the Senate's amendments to AB 2182, the OAG would have been responsible for the creation and maintenance of a web portal containing commercial privacy policies.[121] AB 2182 placed additional responsibilities on the OAG to protect Californians' PII by requiring the creation of an Internet web portal containing links to the privacy policies of online platforms.[122] Further, AB 2182 required online platforms to inform the OAG of required updates and revisions to the web portal.[123]

Despite expanding the OAG's role with respect to data privacy enforcement, AB 2182 would not have changed the amount or type of information that commercial Internet platforms are legally obligated to disclose.[124] Additionally, AB 2182 classified social media websites as online platforms, making social media subject to the provisions of this legislation.[125] Before the California Legislature could approve these changes, the legislature rushed Chapter 55 through the legislative process, which the governor signed it into law.[126] The legislature had not approved AB 2182 when the Governor signed Chapter 55 into law; rather, the legislature modified AB 2182 again, causing it to no longer relate to privacy.[127]

D. Chapter 55: The California Consumer Privacy Act of 2018

Like AB 2182, Mactaggart and Arney conceptualized the California Consumer Privacy Act of 2018 long before the Facebook/Cambridge Analytica scandal.[128] Chapter 55 guarantees many consumer rights, including the right to

---

118. *Id.*

119. ASSEMBLY COMMITTEE ON PRIVACY & CONSUMER PROTECTION, COMMITTEE ANALYSIS OF AB 2182, at 2 (May 25, 2018).

120. AB 2182, 2018 Leg., 2017–2018 Sess. (Cal. 2018) (as amended on June 18, 2018, but not enacted).

121. *Id.*

122. *Id.*

123. *Id.*

124. *Id.*

125. *Id.*

126. *Compare* Complete Bill History of AB 2182, *supra* note 112, *with* Complete Bill History of AB 375, http://leginfo.legislature.ca.gov/faces/billHistoryClient.xhtml?bill_id=201720180AB375 (last visited Aug. 12, 2018) (on file with *The University of the Pacific Law Review*) (becoming law after Governor Brown signed it within seven days of its creation).

127. *See* Complete Bill History of AB 2182, *supra* note 112 (as of Aug. 12, 2018, bill was not enacted); AB 2182, 2018 Leg., 2017–2018 Sess. (Cal. 2018) (as amended on Aug. 13, 2018, but not enacted).

128. *Compare About Us*, CAL. CONSUMER PRIVACY ACT, *supra* note 19 (initiating the process of

know what PII a business collects, whether a business sells that information, the consumer's right to prohibit that sale, and the freedom from discrimination for exercising these rights.[129]

Beginning on January 1, 2020, California consumers will be able to request that a business disclose the information it collected about the requestor.[130] Moving forward, a business that collects PII must disclose what information it collects at or before the collection begins.[131] The consumer has the right to request copies of collected information, free of charge, and request that the business delete the collected PII.[132] The California Consumer Privacy Act requires businesses to comply with these requests unless an exception applies.[133] The most notable exception exists when a business must maintain a customer's information because of an ongoing relationship.[134]

Chapter 55 requires businesses to provide notice to consumers about their sharing practices and inform consumers of their "right to opt out."[135] The right to opt out means that consumers may direct a business to discontinue selling their PII, and the law prohibits businesses from discriminating against consumers who opt out.[136] Namely, businesses cannot charge higher rates to customers who opt out, but they can offer financial incentives to encourage customers to opt in to the selling of their PII.[137] To provide consumers an adequate means of opting out, businesses must offer consumers at least two ways to opt out of data collection.[138] Businesses must now provide a "clear and conspicuous link" on their website(s), titled "Do Not Sell My Personal Information," and they cannot require consumers to create an account in order to opt out.[139]

One final provision of Chapter 55 permits consumers to seek damages against a business when the consumers' PII is the subject of a data breach.[140] In the event that unencrypted or nonredacted PII is the subject of a data breach, affected consumers can choose to seek damages between $100-$750 "per

drafting privacy legislation in 2015), *with* Meredith, *supra* note 1 (breaking news of the Facebook/Cambridge Analytica scandal in 2018).

129. CAL. CIV. CODE §§ 1798.100, 1798.120 1798.125 (enacted by Chapter 55).

130. CAL. CIV. CODE § 1798.198 (enacted by Chapter 55).

131. CAL. CIV. CODE § 1798.100 (enacted by Chapter 55).

132. *Id.*

133. *See* CAL. CIV. CODE § 1798.105(d)(2)–(9) (enacted by Chapter 55) (exempting businesses from complying with a request when there are fraudulent activities, problems with their systems, questions of free speech, compliance issues with the California Electronic Communications Privacy Act, ongoing studies, or other legal obligations).

134. CAL. CIV. CODE § 1798.105(d)(1) (enacted by Chapter 55).

135. CAL. CIV. CODE § 1798.120 (enacted by Chapter 55).

136. CAL. CIV. CODE §§ 1798.105, 1798.125 (enacted by Chapter 55).

137. CAL. CIV. CODE § 1798.125 (enacted by Chapter 55).

138. CAL. CIV. CODE § 1798.130 (enacted by Chapter 55).

139. CAL. CIV. CODE § 1798.135 (enacted by Chapter 55).

140. CAL. CIV. CODE § 1798.150 (enacted by Chapter 55).

customer per incident or actual damages, whichever is greater."[141] In assessing damages, the courts may consider factors such as the "seriousness of the misconduct, the number of violations, . . . and the defendant's assets, liabilities, and net worth."[142]

IV. ANALYSIS

With over two billion active monthly users,[143] Facebook possesses data on approximately thirty percent of the world's population.[144] Every day, millions of Facebook users post information about their lives, and there are no limitations on what Facebook can do with that information.[145] Facebook's unfettered access to PII is an example of the control that a single member of Big Tech has over information.[146] Considering that Google, Amazon, Microsoft, and Apple are also a part of Big Tech, and that thousands of other companies in the world collect PII, the volume of unregulated PII is astounding.[147] As a result, the need for commercial data protection regulations is growing, and the Legislature's refusal to regulate commercial data use left Californians vulnerable.[148]

While some legislators may criticize the EU's attempt at data regulation as overly prescriptive,[149] it was a step toward protecting PII in a time when privacy regulations were uncommon.[150] Despite the fact that the United States shares many values with the EU, American legislators have remained stagnant while their European counterpart has been protecting citizens' privacy from commercial abuses.[151] In the wake of federal complacency, California began

141. *Id.*

142. *Id.*

143. *Company Info*, FACEBOOK, https://newsroom.fb.com/company-info/ (last visited July 14, 2018) (on file with *The University of the Pacific Law Review*).

144. *World Population Projected to Reach 9.7 Billion by 2050*, UNITED NATIONS, http://www.un.org/en/development/desa/news/population/2015-report.html (last visited July 11, 2018) (on file with *The University of the Pacific Law Review*).

145. Cara Pring, *100 Social Media Statistics for 2012*, THE SOCIAL SKINNY (Jan. 11, 2012), http://thesocialskinny.com/100-social-media-statistics-for-2012/ (on file with *The University of the Pacific Law Review*).

146. *Id.*

147. Will Oremus, *Big Tobacco. Big Pharma. Big Tech?*, SLATE (Nov. 17, 2017), http://www.slate.com/articles/technology/technology/2017/11/how_silicon_valley_became_big_tech.html (on file with *The University of the Pacific Law Review*); Steve Kroft, *The Data Brokers: Selling Your Personal Information*, CBS (Mar. 9, 2014), https://www.cbsnews.com/news/the-data-brokers-selling-your-personal-information/ (on file with *The University of the Pacific Law Review*).

148. *Compare* CAL. CIV. CODE §§ 1798.14–1798.15 (placing strict regulations on the information that government agencies may collect), *with* CAL. BUS. & PROF. CODE § 22575 (requiring a business to simply publish a privacy policy to its website).

149. Telephone Interview with Marc Levine, *supra* note 14.

150. *See generally* ECHR, *supra* note 55 (adding newly acknowledged human rights to the convention on June 1, 2010), *and* ECFR, *supra* note 56 (acknowledging new fundamental rights to the charter on Oct. 26, 2012); Adler, *supra* note 22.

151. *Compare* 15 U.S.C.A. § 1681(a) (implementing non-commercial privacy regulations as of July 21,

exploring privacy protections for its citizens.[152] The question of how to protect Californians' privacy was unresolved until Alastair Mactaggart, Rick Arney, and Assemblymember Levine, broached the topic.[153]

Section A juxtaposes the sluggish approach to privacy legislation in the United States with the EU's dynamic approach to fundamental rights.[154] Section B explains why existing privacy laws will not protect Californians' PII.[155] Section C explores how the California Legislature failed its constituents by failing to legislate.[156] Section D details Big Tech's excitement over AB 2182.[157] Section E chronicles how Chapter 55 transitioned from a ballot measure to a law,[158] and Section F discusses how citizens can use Chapter 55 as a model to defeat powerful interest groups.[159]

A. American Reluctance Versus European Proactivity

There is a stark contrast between the recent uptick in European cases pitting the right to privacy against corporate interests and the absence of such cases in the United States.[160] Although the concept of privacy is not new in the United States,[161] legislation protecting privacy from commercial entities has never surfaced.[162] In 1890, *Harvard Law Review* published an article titled "The Right to Privacy," in which Samuel Warren and Justice Brandeis concluded that common law should grow "to meet the demands of society."[163] The article asserted that the "development of the law was inevitable" as the legal community identified new rights.[164] Nearly 130 years later, the issue of privacy was unresolved in the United States, which raises the question: For a country founded on protecting individual liberties, why did it taking so long to protect the right to

2011), *with* ECHR, *supra* note 55, at 3 (expanding recognized rights on June 1, 2010), *and* ECFR, *supra* note 56, at 391 (including new rights as of Oct. 26, 2012).

152. *See* AB 2182, *supra* note 76 (attempting to protect Californians' privacy through regulations).

153. Adler, *supra* note 22.

154. *Infra* Part IV.A.

155. *Infra* Part IV.B.

156. *Infra* Part IV.C.

157. *Infra* Part IV.D.

158. *Infra* Part IV.E.

159. *Infra* Part IV.F.

160. *See generally* Case C-131/12, Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos, Mario Costeja González, 2014 E.C.R. I-317 (ruling in favor of an individual's right to privacy on the Internet), *and* Delfi AS v. Estonia, 2015 Eur. Ct. H.R. 5 (2015) (holding a business accountable for speech posted on its website by an anonymous third party).

161. *See* Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 193 (1890) (discussing the right to privacy in the year 1890).

162. *See* 15 U.S.C.A. § 6801 (regulating privacy with regard to the financial industry); CAL. BUS. & PROF. CODE § 22580 (restricting marketing for businesses that advertise to minors).

163. Warren & Brandeis, *supra* note 161, at 193.

164. *Id.* at 193–95.

privacy?[165]

Although the rights guaranteed in the ECHR and ECFR do not completely mirror the freedoms that Americans enjoy, Europe takes human rights and fundamental rights very seriously.[166] Neither the EU nor the Council of Europe acknowledge every freedom from the Bill of Rights, but that is a testament to the different values between the governing bodies.[167] The oldest rights guaranteed by the ECHR and ECFR are less than 100 years old, and the respective governing bodies updated both the ECHR and ECFR within the last ten years.[168] In fact, the EU and the Council of Europe are continuously amending the ECHR and ECFR to reflect values and protections required in a modern society.[169]

Why are American legislators hesitant to restrict the ways that businesses abuse PII, let alone modernize the rights of Americans?[170] While Europe strives to continually modernize its ECHR and ECFR, the United States government is leaving Americans out in the cold.[171] Part of the reason politicians avoid attempts to regulate privacy is because the tech lobby is too powerful.[172] Nevertheless, legislators should steel their nerves on controversial topics like data breaches because these issues impact millions of people, and Californians feel passionate about consumer privacy.[173] The issue is whether legislators will produce common sense regulations to protect their constituents.[174] If people are disenchanted with the way that Big Tech sells consumer PII but legislators are failing to act, then the tech lobby must be winning over the legislators.[175]

---

165. *See generally* U.S. CONST. amends. I–X (establishing the Bill of Rights that, without its existence, the Constitutional Convention would not have ratified the Constitution); CAL. CIV. CODE § 1798.100 (enacted by Chapter 55) (creating the first privacy regulation impacting private industry since Warren and Brandeis theorized the right to privacy in 1890).

166. *See generally* ECHR, *supra* note 55 (adding newly acknowledged human rights to the convention on June 1, 2010), *and* ECFR, *supra* note 56 (acknowledging new fundamental rights to the charter on Oct. 26, 2012).

167. *Compare generally* U.S. CONST. amend. II (protecting the right to bear arms), *with* ECHR, *supra* note 55 (remaining silent on the possession of firearms) *and* ECFR, *supra* note 56 (declining to address the topic of firearms).

168. *See* ECHR, *supra* note 55, at 3 (adding new rights on June 1, 2010), *and* ECFR, *supra* note 56, at 391 (updating the listed rights on Oct. 26, 2012).

169. *See generally* ECHR, *supra* note 55 (including the right to privacy as a protected right), *and* ECFR, *supra* note 56 (safeguarding an individual's right to protect his or her data on the Internet).

170. *See* Telephone Interview with Marc Levine, *supra* note 14 (suggesting legislators do not want to "take on the wealthiest, most profitable special interest in the world").

171. *See supra* Part IV.A (juxtaposing European proactivity with American complacency as it applies to modernizing rights).

172. *See* Telephone Interview with Marc Levine, *supra* note 14 (emphasizing the broad power and vast wealth that Big Tech possesses).

173. *See About Us*, CAL. CONSUMER PRIVACY ACT, *supra* note 19 (discovering how angry and trapped Californians feel regarding Internet privacy).

174. *See* Adler, *supra* note 22 (expressing skepticism whether lawmakers would be open to regulating Internet privacy).

175. *See About Us*, CAL. CONSUMER PRIVACY ACT, *supra* note 19 (taking matters into his own hands and proposing privacy regulations on a ballot measure).

B. Why Existing Laws are Failing California Consumers

In *Time, Inc. v. Hill*,[176] the Supreme Court noted that states are free to create their own privacy laws.[177] California took advantage of this opportunity by including the right to privacy in its constitution.[178] Now, California has three main laws to regulate privacy, but none of these laws protect Californians from commercial data abuse.[179] The first law applies to personal data that the government possesses and is therefore irrelevant to consumer protection from commercial abuses.[180] The second law concerns California's privacy policy disclosure, but this law does nothing to protect consumers.[181] These first two regulations impose no restrictions on what a business may do with PII, how long it can retain PII, or whether a Californian can request that a business delete his or her PII.[182]

California's third privacy law created the OPP in 2010 and was a preliminary step toward regulating data protection.[183] The state appeared to follow Warren and Brandeis' guidance from 1890 by requiring the OPP to recommend policies to address consumer privacy.[184] Unfortunately, the government removed funding from the OPP, and the agency ceased operations before the law could fulfill its primary function.[185] In essence, the OPP still exists, yet it is completely meaningless without funding and staff.[186]

When the OPP became defunct, its enforcement responsibilities shifted to the OAG's Privacy Enforcement and Protection Unit.[187] One of the main responsibilities this unit absorbed was the enforcement of state and federal privacy laws.[188] In the absence of privacy regulations, the only real duties that this unit has are to enforce the IPA and ensure that businesses are posting their privacy policies online.[189] The Privacy Enforcement and Protection Unit is an

176. 385 U.S. 374 (1967).

177. *Id.* at 415.

178. *Compare generally id.* (discussing the right to privacy in 1967), *with* J. Clark Kelso, *California's Constitutional Right to Privacy*, 19 PEPP. L. REV. 327, 328 (1992) (noting that California added "privacy" to its Constitution in 1972).

179. CAL. BUS. & PROF. CODE § 22575; CAL. BUS. & PROF. CODE § 22580; CAL. CIV. CODE § 1798.14.

180. CAL. CIV. CODE § 1798.14.

181. CAL. BUS. & PROF. CODE § 22575.

182. *Id.*; CAL. CIV. CODE § 1798.14.

183. CAL. GOV'T. CODE § 11549.5.

184. *Id.*

185. ASSEMBLY COMMITTEE ON PRIVACY & CONSUMER PROTECTION, COMMITTEE ANALYSIS OF AB 2182, at 2 (May 25, 2018); *Governor Brown's Budget Slashes State Spending by $12.5 Billion*, OFF. OF GOVERNOR EDMUND G. BROWN JR., *supra* note 79.

186. ASSEMBLY COMMITTEE ON PRIVACY & CONSUMER PROTECTION, COMMITTEE ANALYSIS OF AB 2182, at 2 (May 25, 2018).

187. *Id.*

188. *Id.*; *Privacy Enforcement and Protection*, CAL. DEP'T. OF JUST., https://oag.ca.gov/privacy/ (last visited July 14, 2018) (on file with *The University of the Pacific Law Review*).

189. *Compare Privacy Enforcement and Protection*, CAL. DEP'T. OF JUST., https://oag.ca.gov/privacy/

enforcement agency that has neither regulatory authority nor support from a regulatory body.[190] This regulatory gap is precisely what Assemblymember Levine hoped to close when he proposed AB 2182.[191]

C. How the California Legislature Let Californians Down

Coincidentally, Assemblymember Levine proposed AB 2182 to do precisely what Warren and Brandeis postulated in 1890; it would have created a regulatory body to propose regulations matching modern innovation.[192] Like Warren and Brandeis, Assemblymember Levine foresaw that modernizations generate the need for legislation, that technological advancement impinges on the right to privacy, and that legislation should develop alongside technology.[193] Assemblymember Levine's proposed regulatory agency, the CDPA, would have periodically recommended privacy regulations that would both account for technological advancements and protect Californians' privacy.[194] The CDPA's recommended regulations would have provided the Privacy Enforcement and Protection Unit actual, meaningful authority because the unit would be enforcing regulations that genuinely protect Californians' privacy.[195]

The Assembly held a legislative hearing for AB 2182 on April 17, 2018, roughly one month before the Assembly removed the regulatory powers of the bill.[196] Mike Shapiro, Chief Privacy Officer for Santa Clara County, attended the hearing for AB 2182 as the only witness present in support of the legislation.[197] In his testimony, he discussed an "uptick in data breaches," namely from Facebook, Cambridge Analytica, and Experian.[198] Mr. Shapiro explained that AB 2182 is a reasonable step toward data protection and that government must

(last visited July 14, 2018) (on file with *The University of the Pacific Law Review*) (stating that the Privacy Enforcement and Privacy Unit enforces state and federal laws), *with supra* Part II.D (pointing to an absence of state privacy laws), *and supra* Part II.D (explaining that federal privacy regulations do not apply to private industry).

190. *See* ASSEMBLY COMMITTEE ON PRIVACY & CONSUMER PROTECTION, COMMITTEE ANALYSIS OF AB 2182, at 6 (Apr. 17, 2018) (explaining that the regulatory body—the OPP—disbanded and enforcement responsibilities shifted to the OAG).

191. Telephone Interview with Marc Levine, *supra* note 14.

192. ASSEMBLY COMMITTEE ON PRIVACY & CONSUMER PROTECTION, COMMITTEE ANALYSIS OF AB 2182, at 3 (Apr. 17, 2018).

193. *Id.*

194. *See* Levine, *supra* note 14 (stating that the CDPA would have answered to the legislature for the creation of regulations).

195. ASSEMBLY COMMITTEE ON PRIVACY & CONSUMER PROTECTION, COMMITTEE ANALYSIS OF AB 2182, at 1 (Apr. 17, 2018).

196. *Compare id.* at 8 (noting the date of the hearing as Apr. 17, 2018), *with supra* Part III.B (discussing the California Assembly's May 25, 2018 modifications).

197. *Hearing on AB 2182 Before the Assembly Committee on Privacy & Consumer Prot.*, 2017 Leg., 2017–2018 Sess. (Cal. 2018) (on file with *The University of the Pacific Law Review*).

198. *Id.*

"balance business interests with the privacy interests of the public."[199] He charged government leaders with taking action and said that officials "cannot say we understand, we know about these breaches, we have met, we have discussed it, and yet we've decided to do nothing."[200] After Mr. Shapiro finished speaking, five witnesses representing various tech groups testified against AB 2182.[201] In total, fourteen different business interest groups officially opposed AB 2182.[202]

An enforcement agency should have support from a regulatory body, yet both the California Assembly and Senate stripped AB 2182 of its ability to generate regulations.[203] Influenced by the tech lobby, the Assembly and the Senate rendered the law harmless.[204] In discussing privacy regulations, Assemblymember Levine said, "You have a choice: you can do nothing, or you can do something. Let's advance the conversation."[205] By removing regulatory power from AB 2182, the California Legislature chose to do nothing.[206]

D. Why AB 2182 Became a Win for Big Tech

Today, the OAG's Privacy Enforcement and Protection Unit is responsible for enforcing privacy regulations, but the lack of regulations leaves Californians vulnerable to abuses by Big Tech.[207] Initially, AB 2182 would have addressed this vulnerability; however, the legislature modified the law and required the OAG to publish a website containing links to privacy policies that businesses already publish on their own websites.[208] Currently, the OAG maintains a similar repository on its website which provides Californians with links to state and federal regulations.[209] It is evident that the OAG does not take its privacy responsibilities seriously because, as of July 14, 2018, most of the links on its website to federal privacy laws do not work.[210]

Given the OAG's nonchalant approach to its privacy enforcement responsibilities, the gutted version of AB 2182 was a huge win for Big Tech.[211] If the OAG cannot properly maintain the hyperlinks on one of its existing websites,

---

199. *Id.*

200. *Id.*

201. *Id.*

202. ASSEMBLY COMMITTEE ON PRIVACY & CONSUMER PROTECTION, COMMITTEE ANALYSIS OF AB 2182, at 8 (Apr. 17, 2018).

203. Telephone Interview with Marc Levine, *supra* note 14.

204. *Id.*

205. *Id.*

206. *See id.* (implying the failure to regulate is "doing nothing").

207. *Privacy Enforcement and Protection*, *supra* note 188.

208. AB 2182, *supra* note 120.

209. *Privacy Laws*, CAL. DEP'T. OF JUST., https://oag.ca.gov/privacy/privacy-laws (last visited July 14, 2018) (on file with *The University of the Pacific Law Review*).

210. *See id.* (failing to update its links to federal privacy laws).

211. *See* Telephone Interview with Marc Levine, *supra* note 14 (discussing the changes to AB 2182 and how it no longer applies to privacy).

what evidence exists that its approach to this new repository would be any different?[212] AB 2182 reinforced the idea that, without actual regulations, Californians must rely on the OAG's website for information detailing how businesses may sell their data.[213] It is hard to see how California can protect its citizens' PII from commercial data abuses without implementing meaningful data protection regulations.[214] Big Tech would have been free to continue its abuses of consumer data given that the legislators failed to create a regulatory body supported by a proactive enforcement agency.[215]

E. The Story Behind Chapter 55

Inspired by a 2015 conversation with a Google engineer, Alastair Mactaggart began researching the best way to enact privacy regulations.[216] The Google engineer told Mactaggart, "If people just understood how much we knew about them, they'd be really worried."[217] This comment prompted Mactaggart, aided by his friend Rick Arney, to embark on a two-year journey where the pair researched Internet privacy, conducted focus groups, and drafted their ideal privacy regulation.[218] Finally, they realized that the best route to enact change would involve putting the matter in the hands of the people via a ballot initiative.[219]

As Mactaggart's plan unfolded, Big Tech caught wind of the potential privacy regulations and began contributing money to oppose the initiative.[220] Initially, Facebook, Google, Comcast, AT&T, Verizon, Microsoft, and Uber had contributed nearly 2 million dollars to a political action committee in opposition to the measure.[221] Californians' concerns over what businesses can do with their PII won the day, and Mactaggart submitted his ballot initiative with 629,000 signatures.[222]

Two California legislators contacted McTaggart and asked if he would

212. *See Privacy Laws*, *supra* note 209 (anticipating the OAG will take a hands-off approach to its new website much like it does with its current repository).

213. *See supra* Part III.C (explaining how the California Senate stripped AB 2182 of its regulatory authority and rewrote the bill to create an Internet repository).

214. *See supra* Part IV.C (describing how the California Legislature actively avoided regulating Internet privacy by killing AB 2182).

215. *Compare* GDPR, *supra* note 30, at 7 (implementing privacy protections), *with* ASSEMBLY COMMITTEE ON PRIVACY & CONSUMER PROTECTION, COMMITTEE ANALYSIS OF AB 2182, at 4 (Apr. 17, 2018) (noting the amount of data breaches in California), *and Privacy Laws*, CAL. DEP'T. OF JUST., https://oag.ca.gov/privacy/privacy-laws (last visited July 14, 2018) (on file with *The University of the Pacific Law Review*) (containing non-operational links to federal privacy laws).

216. *About Us*, CAL. CONSUMER PRIVACY ACT, *supra* note 19.

217. *Id.*

218. *Id.*

219. *Id.*

220. *Id.*

221. *Id.*

222. *Id.*

withdraw the ballot initiative if the "California Legislature passed a law" addressing his concerns.[223] Skeptical, Mactaggart agreed on two conditions: first, the law must replicate all of the measure's critical components; second, the legislature must pass the law before June 28, 2018.[224] Mactaggart found the legislators' first draft unacceptable because it gave the giant companies "a free pass" by failing to require enforcement.[225] Then, the day after the ballot measure qualified for the November election, Chapter 55 passed its first committee.[226]

Rumors swirled about the tech, automotive, and communications industries mounting a 100-million-dollar opposition to the ballot measure in November.[227] The stage was set with public opinion favoring the ballot measure, the election looming in November, and the California Legislature advancing a bill that mirrored the ballot measure.[228] Once Chapter 55 satisfied his criteria, Mactaggart offered the tech industry a choice: proceed with an expensive, unpopular campaign in November, or accept Chapter 55.[229] The tech industry admitted defeat, Mactaggart withdrew his ballot measure, and Governor Brown signed Chapter 55 into law.[230]

F. Chapter 55: A Model for Californians to Defeat Wealthy Lobbies

Big Tech is clearly thriving in today's economy.[231] It built the perfect business model: provide free services where users volunteer information that the service provider monetizes.[232] On the most basic level, Big Tech created a system of human capital where many people do not realize they are the product.[233] As Mactaggart noted, "if you're not paying for the product, you are the product."[234] Big Tech is the "wealthiest, most powerful special interest in the world,"[235] and every time a Facebook user adds information to his or her profile, the lobby grows stronger and wealthier.[236] Who will protect the people when lawmakers

223. *Id.*

224. *Id.*

225. *Id.*

226. Sumagaysay, *supra* note 18.

227. *About Us*, CAL. CONSUMER PRIVACY ACT, *supra* note 19; Adler, *supra* note 22; *Proposed Calif. Ballot Measure Takes on Tech Companies*, CBS NEWS, https://www.cbsnews.com/video/proposed-ballot-measure-california-consumer-privacy-act-personal-information/ (last visited Aug. 9, 2018) (on file with *The University of the Pacific Law Review*).

228. *About Us*, CAL. CONSUMER PRIVACY ACT, *supra* note 19; Adler, *supra* note 22.

229. Adler, *supra* note 22.

230. *About Us*, CAL. CONSUMER PRIVACY ACT, *supra* note 19; Adler, *supra* note 22.

231. Telephone Interview with Marc Levine, *supra* note 14.

232. *See id.* (indicating that Big Tech's model of selling personal information has made it the wealthiest and most profitable special interest in the world).

233. *Id.*

234. *About Us*, CAL. CONSUMER PRIVACY ACT, *supra* note 19.

235. Telephone Interview with Marc Levine, *supra* note 14.

236. *See* Pring, *supra* note 145 (noting over 510,000 posts per minute); Telephone Interview with Marc Levine, *supra* note 15 (implying Big Tech grows stronger and wealthier when data is added).

refuse to regulate the richest special interest in the world?[237]

Fortunately, as Mactaggart and Arney learned from the focus groups they conducted, Californians have a deep-seated disdain for the "privacy bargain" that Big Tech forces upon consumers.[238] Using Internet services is a take it-or-leave-it scenario, where using the service means permitting the sale of your information.[239] Mactaggart and Arney leveraged Big Tech's own product against itself when the two discovered overwhelming support for their ballot measure.[240]

Mactaggart's approach to enacting change became novel when he decided to enact legislation without the legislature.[241] As Mactaggart said, for the past twenty-five years legislators have "been able to take up privacy," but "[n]o one ever has, because the big tech companies make sure it never gets anywhere."[242] Instead of matching the complicity of the Legislature, Mactaggart leveraged the public's support for his ballot measure to force lawmakers to do their jobs.[243] Although there are lawmakers interested in regulating privacy like Assemblymember Levine, the California Legislature demonstrated their unwillingness to stand up to Big Tech by gutting AB 2182.[244] Mactaggart revealed Californian's concerns to the legislators, provided them with a model on how to legislate privacy, gave them an ultimatum to enact change, and persisted until Chapter 55 accomplished what he set out to do.[245] The story behind Chapter 55 illustrates the idea that, when the Legislature refuses to enact common-sense legislation, Californians have a workaround via the ballot measure system.[246]

V. CONCLUSION

There is an apparent disconnect between a person's right to privacy, as identified by the legal community, and the privacy regulations implemented by the federal government.[247] Early on, Samuel Warren and Justice Brandeis pointed

237. *See supra* Part III.C (inferring that by refusing to enact privacy regulations the California Legislature will not cross Big Tech).

238. *About Us*, CAL. CONSUMER PRIVACY ACT, *supra* note 19.

239. *Id.*

240. *Id.*

241. *See id.* (pursuing privacy regulations through a ballot measure).

242. Adler, *supra* note 22.

243. *See About Us*, CAL. CONSUMER PRIVACY ACT, *supra* note 19 (noting that public opinion was on the side of regulating privacy when legislators reached out to him).

244. *See* Telephone Interview with Marc Levine, *supra* note 14 (implying he would pursue privacy legislation once he figures out how to overcome the opposition), *supra* Part III.B (explaining how the Assembly removed AB 2182's regulatory powers), *and supra* Part III.C (describing how the Senate planned to give control of AB 2182's Internet repository to an agency that is already failing to maintain a website).

245. *About Us*, CAL. CONSUMER PRIVACY ACT, *supra* note 19.

246. *See supra* Part III.B (indicating that by stripping AB 2182 of its regulatory powers, the California Assembly refused to stand up to Big Tech); *About Us*, CAL. CONSUMER PRIVACY ACT, *supra* note 19 (creating regulations in an area that legislators refused to regulate).

247. *Compare* Time, Inc. v. Hill, 385 U.S. 374, 415 (1967) (reaffirming that privacy is a right), Griswold v. Conn., 381 U.S. 479, 494 (1965) (citing the Constitution as justification for the right to privacy), *and* Mapp v.

to a person's right to privacy and indicated that the laws should evolve with modern society.[248] While the Internet was developing, between the late 1960s through the early 2000s, the federal government passed legislation protecting individuals' privacy from abuses by essential services such as financial agencies, credit reporting bureaus, and government entities.[249]

The Internet has become essential in today's society, and social media and other services offered by Big Tech are becoming as pervasive as financial institutions.[250] With the frequency and size of data breaches rising, how does the United States justify the continued monetization of Americans?[251] The big question Californians face is how will the government protect its citizens' PII?[252] If laws should evolve to meet the demands of society, then where are the laws that regulate data collection, retention, and use by Big Tech?[253] The answer provided by Mactaggart and Arney is that the Californians must rise up and create the laws themselves when legislatures refuse to legislate.[254]

Ohio, 367 U.S. 643, 643 (1961) (emphasizing the importance of the right to privacy), *with* 15 U.S.C.A. § 6801 (failing to regulate privacy outside of the financial community), *and* 5 U.S.C.A. § 552(a) (imposing restrictions only on information collected by a government agency).

248. Warren & Brandeis, *supra* note 161, at 193.

249. 15 U.S.C.A. § 1681; 15 U.S.C.A. § 6801; 5 U.S.C.A. §§ 551–552(a).

250. *See About Us*, CAL. CONSUMER PRIVACY ACT, *supra* note 19 (discussing how essential mobile phones and computers are in today's society); Ikwap Amos, *Technology's Increasing Pervasiveness Means that the Future is Promising, Albeit a Little Bleak*, IAFRIKAN (Sept. 22, 2016), https://www.iafrikan.com/2016/09/22 /technologys-increasing-pervasiveness-means-that-the-future-is-promising-albeit-a-little-bleak/ (on file with *The University of the Pacific Law Review*).

251. ASSEMBLY COMMITTEE ON PRIVACY & CONSUMER PROTECTION, COMMITTEE ANALYSIS OF AB 2182, at 2 (Apr. 17, 2018); Telephone Interview with Marc Levine, *supra* note 14.

252. *See generally* Telephone Interview with Marc Levine, *supra* note 14 (discussing the lack of privacy regulations and the need for government action).

253. Warren & Brandeis, *supra* note 161, at 193.

254. *See generally* CAL. CIV. CODE § 1798.100 (enacted by Chapter 55) (emanating from the actions of private citizens instead of the legislature); Adler, *supra* note 22.

* * *