Journal of Technology Law & Policy

Volume 23 | Issue 1 Article 2

June 2018

THE CALIFORNIA CONSUMER PRIVACY ACT: TOWARDS A EUROPEAN-STYLE PRIVACY REGIME IN THE UNITED STATES?

Stuart L. Pardau

THE CALIFORNIA CONSUMER PRIVACY ACT: TOWARDS A EUROPEAN-STYLE PRIVACY REGIME IN THE UNITED STATES?

Stuart L. Pardau[*]

* J.D. Stanford Law School and Associate Professor, The David Nazarian College of Business and Economics, California State University, Northridge.

INTRODUCTION

When it comes to technology, over the last two decades the consuming public has rushed forward excitedly in all directions towards new and seemingly revolutionary services, without any deep thought about the business models of well-known tech giants or what important tradeoffs might be contained in the fine print of privacy policies or online terms and conditions.[1] Consumers value Facebook because it offers a way to stay connected with far-away friends, plus a place to raise online storefronts, organize events, and rally people to social or political causes.[2] Google can synchronize your email, contact list, calendar, and other core services, all while offering the most popular Internet search engine and

1. *See, e.g.*, Aaron Smith, *Half of Online Americans Don't Know What a Privacy Policy Is*, PEW RESEARCH: FACT TANK (Dec. 4, 2014), http://www.pewresearch.org/fact-tank/2014/12/04/half-of-americans-dont-know-what-a-privacy-policy-is/; Mark Sableman, *Who Reads Privacy Policies?*, THOMPSON COBURN LLP (May 31, 2017), https://www.thompsoncoburn.com/insights/blogs/internet-law-twists-turns/post/2017-05-31/who-reads-privacy-policies/; David Berreby, *Click to Agree with What? No One Reads Terms of Service, Studies Confirm*, GUARDIAN (Mar. 3, 2017, 8:38 AM), https://www.theguardian.com/technology/2017/mar/03/terms-of-service-online-contracts-fine-print.

2. *See, e.g.*, Kurt Wagner, *8 Ways Facebook Changed the World*, MASHABLE (Feb. 4, 2014), https://mashable.com/2014/02/04/facebook-changed-the-world/#ziCS5YCLTaqV; Jessica Elgot, *From Relationships to Revolutions: Seven Ways Facebook Has Changed the World*, GUARDIAN (Aug. 28, 2015), https://www.theguardian.com/technology/2015/aug/28/from-relationships-to-revolutions-seven-ways-facebook-has-changed-the-world.

what is now also the world's most popular browser.[3] Instagram has perfected what Facebook's feed never quite got right: an elegant, uncluttered space for users to share snapshots of their lives.[4]

Alongside these platform-specific offerings, other new developments in the business of the Internet were also, as measured or gauged by the level of consumer adoption, accepted as obviously good—at least from a utilitarian perspective, the perceived benefit of these new services outweighed the perceived "detriments" associated with the sharing of one's personal information. To name two examples, geolocation services meant consumers could bring into harmony their physical locations with their "place" on the Internet,[5] and the advent of targeted advertising meant more ads you wanted to see and fewer of those you did not.[6]

What could be the problem with any of this?

It has taken some time for consumers to apprehend and process a new reality: to see the Big Data forest for the individual platform trees, so to speak. If Web 1.0 was the Internet of free access to knowledge and a new,

---

3. *Browser & Platform Market Share: July 2018*, W3COUNTER, https://www.w3counter.com/globalstats.php?year=2018&month=7 (last visited Feb. 17, 2019) (showing Chrome at 58% and Safari in a distant second at 14%); *see* Kris Holt, *15 Ways Google Changed the World*, DAILY DOT (Sept. 4, 2013), https://www.dailydot.com/debug/google-15-anniversary-search-maps/.

4. Eric Markowitz, *How Instagram Grew from Foursquare Knock-Off to $1 Billion Photo Empire*, INC. (Apr. 10, 2012), https://www.inc.com/eric-markowitz/life-and-times-of-instagram-the-complete-original-story.html; Kim Mai-Cutler, *From 0 To $1 Billion in Two Years: Instagram's Rose-Tinted Ride to Glory*, TECH CRUNCH (Apr. 9, 2012), https://techcrunch.com/2012/04/09/instagram-story-facebook-acquisition/.

5. *See* Chirag Kukarni, *15 Ways Geolocation Is Totally Changing Marketing*, FORTUNE (Feb. 6, 2017), http://fortune.com/2017/02/06/geolocation-marketing/; Janelle Nanos, *How Companies Use Geolocation Data to Target You*, BOS. GLOBE, http://apps.bostonglobe.com/business/graphics/2018/07/foot-traffic/ (last visited Feb. 17, 2019) ("Geotargeted mobile marketing is one of the fastest growing forms of advertising—and one of the most controversial. . . . In 2017, marketers spent $17.1 billion on geotargeted mobile ads, and the research firm BIA Advisory Services forecasts that number will more than double to $38.7 billion by 2022."). Despite recent widespread adoption of geolocation, there is evidence consumers were slower to adopt this particular technology, especially in the mobile context, than others. *See, e.g.*, JVG, *Adoption of Geolocation Applications Is Still Stagnant*, VENTURE BEAT (Dec. 6, 2011, 11:13 AM), https://venturebeat.com/2011/12/06/geosocial-app-adoption/ ("Thirty percent of online adults in the U.S. are familiar with geolocation applications, but less than six percent of online adults use these apps . . . ").

6. *See* Leslie K. John et al., *Ads That Don't Overstep*, HARV. BUS. REV., Jan.–Feb. 2018, at 62, https://hbr.org/2018/01/ads-that-dont-overstep ("The results [of targeted advertising] have been impressive. Research has shown that digital targeting meaningfully improves the response to advertisements and that ad performance declines when marketers' access to consumer data is reduced.").

exhilarating, and vaguely utopian globalism, then it seems Web 2.0 is the "Internet of Things," consumer profiling, predictive analytics, and targeted advertising.[7] Following the 2018 Cambridge Analytica scandal, Facebook founder Mark Zuckerberg testified for nearly ten hours over the course of two days before both houses of Congress regarding Facebook's privacy practices.[8] These hearings were undoubtedly animated by the perception—real or imagined—that foreign powers had successfully meddled in the U.S. Presidential elections of 2016 through the medium of Facebook. Perhaps for the first time, the U.S. government seemed to be taking a real interest in Facebook's essential business model and its implications for privacy, and even the nature of democracy. During the Senate hearing, Utah Senator Orrin Hatch asked Zuckerberg: "So, how do you sustain a business model in which users don't pay for your service?" Zuckerberg replied, correctly: "Senator, we run ads."[9] So it seems that, even now, it is taking some time for public consciousness—and lawmakers—to catch up.

In contrast with American authorities, European authorities have been asking hard, existential questions about Internet privacy for decades, notably with regard to Facebook and Google: the two giants of Web 2.0.[10] Most importantly, and as a kind of culmination of years of back and forth between the U.S. and Europe on these questions, the General Data Protection Regulation (GDPR) went into effect on May 25, 2018, implementing broad privacy protections for anyone "in the Union," including non-citizens, and instituting remarkably hefty fines for violators.[11]

Now, in the U.S. too, it seems there is budding awareness that Web 2.0 raises more far-reaching and extensive privacy concerns than the average user may have originally considered. It may be that, following this new awareness, and in an effort on the part of tech firms to get ahead of likely legal changes, the appetite for sweeping legislation in the U.S.

---

7. *See* Daniel Nations, *Is Web 3.0 Really a Thing?*, LIFEWIRE (Mar. 24, 2018), https://www.lifewire.com/what-is-web-3-0-3486623 (discussing Web 1.0 and Web 2.0, and the possibility of a "Web 3.0" just around the corner).

8. *See* Cecilia Kang et al., *Mark Zuckerberg Testimony: Day 2 Brings Tougher Questioning*, N.Y. TIMES (Apr. 11, 2018), https://www.nytimes.com/2018/04/11/us/politics/zuckerberg-facebook-cambridge-analytica.html.

9. *See* Sean Burch, *'Senator, We Run Ads': Hatch Mocked for Basic Facebook Question to Zuckerberg*, S.F. CHRON. (Apr. 10, 2018), https://www.sfchronicle.com/entertainment/the-wrap/article/Senator-We-Run-Ads-Hatch-Mocked-for-Basic-12822523.php.

10. *See, e.g.*, Suzanne Daley, *On Its Own, Europe Backs Web Privacy Fights*, N.Y. TIMES (Aug. 9, 2011), https://www.nytimes.com/2011/08/10/world/europe/10spain.html; Hannah Kuchler, *Max Schrems: The Man Who Took on Facebook—and Won*, FIN. TIMES (Apr. 5, 2018), https://www.ft.com/content/86d1ce50-3799-11e8-8eee-e06bde01c544.

11. *See infra* Part III.

is also on the rise.[12] Certainly, there are already a vast array of "privacy" laws on the books at both the state and the federal level. However, these have by and large been aimed at specific, ascertainably urgent and easier-to-understand problems such as data breach notification, protection of sensitive health and financial information, or children's privacy.[13] Following the Cambridge Analytica scandal, Zuckerberg's testimony to Congress and the enactment of GDPR, it seems the Internet and digital privacy are having a moment. Now is a good time to ask whether sweeping legislation in the mold of GDPR might be around the corner in America.[14]

If so, it looks like California is already leading the way towards greater security of the consumer—or to needless overregulation, depending on one's perspective.[15] Governor Jerry Brown signed into law The California Consumer Privacy Act (CCPA or the Act) on June 28, 2018; it goes into effect on January 1, 2020.[16]

Broadly, the CCPA grants consumers four basic rights in connection to their personal data: (1) 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 Act.[17] These rights are largely to be enforced by the California Attorney General, with a narrow private right

---

12. John D. McKinnon & Marc Vartabedian, *Tech Firms, Embattled Over Privacy, Warm to Federal Regulation*, WALL ST. J. (Aug. 6, 2018), https://www.wsj.com/articles/tech-firms-embattled-over-privacy-warm-to-federal-regulation-1533547800 ("U.S. tech companies, battered over their handling of consumers' personal data, are hoping to get ahead of the public and legal fallout by working with policy makers to help shape potential new federal privacy legislation.").

13. *See infra* Part II.

14. *See, e.g.*, Cameron F. Kerry, *Filling the Gaps in U.S. Data Privacy Laws*, BROOKINGS INST.: TECH TANK BLOG (July 12, 2018), https://www.brookings.edu/blog/techtank/2018/07/12/filling-the-gaps-in-u-s-data-privacy-laws/ ("The Cambridge Analytica stories, the Mark Zuckerberg hearings, and the constant reports of major data breaches have increased interest in federal privacy legislation. Various groupings have been convening to develop proposals. The time is ripe for interests to converge on comprehensive federal privacy legislation.").

15. *See* Sarah Jeong, *No One's Ready for GDPR*, VERGE (May 22, 2018, 3:28 PM), https://www.theverge.com/2018/5/22/17378688/gdpr-general-data-protection-regulation-eu (quoting PayPal founder Peter Thiel: "There are no successful tech companies in Europe and they are jealous of the US so they are punishing us.").

16. California Consumer Privacy Act of 2018, CAL. CIV. CODE § 1798.100 (2018) (effective Jan. 1, 2020).

17. Kristen J. Mathews & Courtney M. Bowman, *The California Consumer Privacy Act of 2018*, PROSKAUER ROSE LLP: PRIVACY L. BLOG (July 13, 2018), https://privacylaw.proskauer.com/2018/07/articles/data-privacy-laws/the-california-consumer-privacy-act-of-2018/ [hereinafter *Proskauer Summary*].

of action for data breaches.[18] As discussed in more detail below, the bill was passed in response to—and to keep Californians from voting on—a ballot initiative presenting even more stringent privacy measures than what is contained in the CCPA.[19] Although the bill will likely be amended before it goes into effect in 2020, the final law is almost certain to be a game changer for U.S. privacy.

Because it is the broadest, most overarching privacy law passed in the U.S. to date, the CCPA quickly drew comparisons to GDPR.[20] But is it, in fact, the first step towards a sea change in American privacy law towards a more "European" ethos? As this article explores, the answer to that question is "in some cases, yes, in others, no." Irrespective of this narrow question, the passage of the CCPA presents an opportunity for deep reflection on privacy law in the U.S. and how best to move forward. Specifically, the purpose of this article is three-fold: (1) to briefly survey the privacy law status quo in the U.S. and Europe; (2) to provide an overview the CCPA; and (3) to offer some additional insights and recommendations on how best to further modify and enhance the CCPA to make it more effective in some areas and less sweeping in others. Parts II and III discuss privacy law in the U.S. and in Europe, respectively. Part IV discusses the CCPA, as it was presented in ballot initiative form, and as it was ultimately passed by the California legislature. Part V contemplates the CCPA's potential effect on U.S. privacy law and makes some suggestions for how best to further modify and enhance the law. Part VI contains the conclusion.

I. PRIVACY LAW IN THE U.S.

In the absence of generalized privacy legislation like California's CCPA, privacy law in the wider U.S. remains a complex patchwork of narrowly tailored federal and state laws. Aside from data breach notification laws,[21] these privacy laws can generally be divided into three

---

18. *See infra* Section IV.B.

19. *See infra* Part IV.

20. *See, e.g.*, Mike Khoury, *California's Mini-GDPR? The Newly-Enacted California Consumer Privacy Act of 2018*, LEXOLOGY (July 10, 2018), https://www.lexology.com/library/detail.aspx?g=60487525-76ea-44e3-97a8-3b9b02987c2e/; Allison Grande, *Calif. Privacy Law to Spark GDPR-Like Compliance Efforts*, LAW360 (July 3, 2018, 10:13 PM), https://www.law360.com/articles/1059877/calif-privacy-law-to-spark-gdpr-like-compliance-efforts.

21. Data breach notification laws arguably constitute a fourth major category of privacy laws in the U.S. Although there is no generalized federal law governing security breaches, specific laws like GLBA and HIPAA include breach notification provisions. *See infra* Section II.B. More importantly, all fifty states and the District of Columbia now have their own data breach notification laws. Petrina McDaniel & Keshia Lipscomb, *Data Breach Laws on the Books in Every State: Federal Data Breach Law Hangs in the Balance*, SQUIRE PATTON BOGGS: SEC. & PRIVACY//BYTES (Apr. 30, 2018), https://www.securityprivacybytes.com/2018/04/data-

categories: (1) laws focused on the modality used to collect or transmit personally identifiable information, such as telephone or email communications; (2) laws focused on the type of data collected and transmitted, or on a specific industry, such as health or financial information; and (3) laws aimed at protecting specific groups, such as children.[22]

A. *Modality-Focused Laws*

On both the federal and state levels, a number of laws are aimed at protecting consumer privacy as it relates to a specific modality or method of communication. In every case, the legislation is designed to address what was originally a specific technological development or a set of exigencies which are unique to that particular modality, such as the proliferation of auto-dialers or email SPAM.

1. The TCPA

One of the most prominent among these modality-focused laws is the Telephone Consumer Protection Act (TCPA).[23] Enacted in 1991 in response to massive improvements in telephone dialing technology—and a resultant uptick in telemarketing—the TCPA was an effort by Congress to balance "[i]ndividuals' privacy rights, public safety interests, and commercial freedoms of speech and trade."[24]

Broadly, the TCPA requires prior express consent before making any non-emergency calls using an "automatic telephone dialing system," or "autodialer," to three categories of phone lines: (1) any emergency line, including any "911" line; (2) "any guest room or patient room of a hospital, health care facility, elderly home, or similar establishment"; or (3) "any telephone number assigned to a . . . cellular telephone service."[25] The statute provides that "[t]he term 'automatic telephone dialing system'

---

breach-laws-on-the-books-in-every-state-federal-data-breach-law-hangs-in-the-balance/; *see Comparison of U.S. State and Federal Security Breach Notification Laws*, STEPTOE & JOHNSON (Jan. 21, 2016), https://www.steptoe.com/images/content/6/5/v1/6571/SteptoeDataBreachNotificationChart.pdf

22. *See* Luis Alberto Montezuma, *The Case for a Hybrid Model on Data Protection/Privacy*, IAPP (Feb. 27, 2018), https://iapp.org/news/a/the-case-for-a-hybrid-model-on-data-protectionprivacy/ (describing the U.S. privacy regime as a "sectoral model" and the European approach as a "comprehensive model").

23. 47 U.S.C. § 227 (2018). In addition to the statute itself, the broader universe of TCPA law also includes attendant regulations implemented by the Federal Communications Commission (FCC) and a number of rulings issued by the FCC which offer guidance on the law. *E.g.*, 47 C.F.R. § 64.1200 (2018).

24. Rules & Regulations Implementing the Telephone Consumer Protection Act of 1991, 30 FCC Rcd. 7961, 7964, ¶ 2 (2015) [hereinafter FCC 2015 Order].

25. 47 U.S.C. § 227(b)(1)(A) (2018); 47 C.F.R. § 64.1200(a)(1) (2018).

means equipment which has the capacity[26]—(A) to store or produce telephone numbers to be called, using a random or sequential number generator; and (B) to dial such numbers."[27]

In addition to authorizing state attorneys general and the FCC to enforce its rules,[28] the TCPA also has a private right of action provision, which mandates $500 in statutory damages for each violation and up to $1,500 for each willful violation with no cap on total damages;[29] the statute imposes a "strict liability" standard.[30] All of these factors together have made the TCPA an especially lucrative statute for the plaintiffs' bar—and an especially enduring headache for businesses who regularly engage in telephone communications.[31]

2. CAN-SPAM

Just as the TCPA zeroed in on telephones, the Controlling the Assault of Non-Solicited Pornography And Marketing Act of 2003 (CAN-SPAM) was the first law to set national standards for commercial email communications.[32] CAN-SPAM covers all commercial messages, which are defined in the act as "any electronic mail message the primary purpose of which is the commercial advertisement or promotion of a commercial product or service," and makes no exception for business-to-business communications.[33]

---

26. The autodialer definition, and specifically the FCC's interpretation of the term "capacity," has long been a source of controversy since a number of TCPA cases turn on whether the equipment used by a defendant was, in fact, an autodialer. In a 2015 ruling, the FCC concluded that the term "capacity" includes equipment's "potential functionalities" or "future possibilit[ies]," not just its "present ability." FCC 2015 Order at 7974 ¶ 16, 7975 ¶ 20. But on March 16, 2018, in a long-awaited opinion, the D.C. Circuit concluded that the Commission's autodialer definition was arbitrary and capricious. ACA Int'l v. FCC, 885 F.3d 687, 699 (D.C. Cir. 2018) ("[T]he Commission's interpretation of the term "capacity" in the statutory definition of an ATDS is 'utterly unreasonable in the breadth of its regulatory [in]clusion.'").

27. 47 U.S.C. § 227(a)(1)(A)–(B). In addition to regulating telephone calls and text messages, the TCPA, as amended by the Junk Fax Protection Act (JFPA), also regulates telephone facsimile communications.

28. Richard P. Eckman, *The Telephone Consumer Protection Act Overview (Client Alert)*, PEPPER HAMILTON LLP (Nov. 23, 2015), http://www.pepperlaw.com/publications/the-telephone-consumer-protection-act-overview-2015-11-23/.

29. 47 U.S.C. § 227(b)(3).

30. *See, e.g.*, Alea London Ltd. v. Am. Home Servs., Inc., 638 F.3d 768, 776 (11th Cir. 2011) ("The TCPA is essentially a strict liability statute . . . ").

31. *Analysis: TCPA Litigation Skyrockets Since 2007; Almost Doubles Since 2013*, U.S. CHAMBER INST. FOR LEGAL REFORM (Feb. 5, 2016), http://www.instituteforlegalreform.com/resource/analysis-tcpa-litigation-skyrockets-since-2007-almost-doubles-since-2013.

32. 15 U.S.C. § 7701 (2018).

33. 15 U.S.C. § 7702(2)(A).

Generally, and as described by the Federal Trade Commission (FTC), CAN-SPAM has seven main requirements: (1) "[d]on't use false or misleading header information;" (2) "[d]on't use deceptive subject lines;" (3) "[i]dentify the message as an ad;" (4) "[t]ell recipients where you're located;" (5) "[t]ell recipients how to opt out of receiving future emails from you;" (6) "[h]onor opt-out requests promptly;" and (7) "[m]onitor what others are doing on your behalf."[34]

Because it does not include a private right of action—only allowing the federal government, the attorney general of a state, and Internet service providers to bring actions—CAN-SPAM has not been the same kind of vehicle for litigation as the TCPA. But that does not mean that CAN-SPAM violations cannot be costly: the Act provides for civil and criminal penalties for noncompliance, including statutory damages up to $6 million for willful violations, and even prison terms of up to five years.[35]

3. The CFAA

Like the TCPA and CAN-SPAM, the Computer Fraud and Abuse Act (CFAA) was passed in 1984 to protect a specific type of equipment or "modality"—the computer systems of financial institutions and the federal government.[36] In 1994, the law was amended to include a private right of action; in 1996, the law was amended again to expand the definition of protected computers to encompass all computers used in foreign or interstate commerce.[37]

The central prohibition of the CFAA applies to individuals who access protected computers "without authorization" or in a way that "exceeds authorized access."[38] Under subsection (g) of the CFAA, "[a]ny person who suffers damage or loss by reason of a violation . . . may maintain a

---

34. *CAN-SPAM Act: A Compliance Guide for Business*, FED. TRADE COMM'N (Sept. 2009), https://www.ftc.gov/tips-advice/business-center/guidance/can-spam-act-compliance-guide-business.

35. 15 U.S.C. § 7706(3)(C)(i)–(f)(1); *see also Technology Commentaries: The Federal CAN-SPAM Act—New Requirements for Commercial E-Mail*, JONES DAY (Feb. 2004), http://www.jonesday.com/files/Publication/0ea34eeb-8735-41f6-ad24-5bdedf7a3433/Presentation/PublicationAttachment/26f5b006-e312-4e0e-8aa7-cab46b2126c3/Federal%20CAN-SPAM.pdf.

36. 18 U.S.C. § 1030 (2018).

37. Lee Goldman, *Interpreting the Computer Fraud and Abuse Act*, 13 PITT. J. TECH. L. & POL'Y 1, 2 (2012) ("Whereas the Act originally applied to misuse of computers used by financial institutions or the United States government, the current version covers all computers used in or affecting commerce, including computers located outside the United States that affect commerce or communication in the United States. Given access to the Internet, this covers virtually all business, home and laptop computers.").

38. 18 U.S.C. § 1030(a)(1).

civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief."[39] But private plaintiffs are limited to economic damages and must be able to show losses of at least $5,000.[40]

4. Modality-Focused Laws in California

Like a number of other states, California has its own laws aimed at protecting consumers' privacy against invasive telemarketing practices. Most notably, Business and Professions Code Sections 17590–17594 enshrine a state "do not call" list based on the national "do not call" list;[41] Public Utilities Code Sections 2871–2876 requires robocalls to be introduced by a live person;[42] and the Business and Professions Code Section 17538.41 prohibits unsolicited text advertisements to cell phones or pagers.[43]

Aside from telephone communications, Business and Professions Code Sections 17529 and 17538.45, like CAN-SPAM, also regulate unsolicited commercial email.[44] Mirroring the CFAA, Penal Code Section 502 likewise imposes criminal sanctions for accessing, and without permission, using, abusing, damaging, contaminating, disrupting, or destroying a computer system or network.[45] And perhaps more so than any other state, California also has a host of privacy laws registering more specific modalities, which range from automated license

---

39. 18 U.S.C. § 1030(g).

40. Goldman, *supra* note 37, at 3.

41. CAL. BUS. & PROF. CODE §§ 17590–17594 (West 2018) ("Thus, it is the intent of the Legislature to adopt the California telephone numbers on the national 'do not call' registry as the California 'do not call' registry.").

42. CAL. PUB. UTIL. CODE §§ 2871–2876 (West 2018) ("Whenever telephone calls are placed through the use of an automatic dialing-announcing device, the device may be operated only after an unrecorded, natural voice announcement has been made to the person called by the person calling.").

43. CAL. BUS. & PROF. CODE § 17538.41(a)(1) ("[N]o person, entity conducting business, candidate, or political committee in this state shall transmit, or cause to be transmitted, a text message advertisement to a mobile telephony services handset, pager, or two-way messaging device that is equipped with short message capability or any similar capability allowing the transmission of text messages.").

44. *Id.* § 17529.5(a) (regulating unsolicited commercial e-mails with misleading or falsified headers or information); CAL. BUS. & PROF. CODE § 17538.45(f)(1) (West 2018) (giving e-mail service provider the right to sue those who send spam from its network or to its subscribers).

45. CAL. PEN. CODE § 502 (West 2018) ("It is the intent of the Legislature in enacting this section to expand the degree of protection afforded to individuals, businesses, and governmental agencies from tampering, interference, damage, and unauthorized access to lawfully created computer data and computer systems.").

plate recognition systems to smart TVs, from RFID tags to e-readers, and from automobile "black boxes" to surveillance systems in rental cars.[46]

5. Other Modality-Focused Laws

Aside from the TCPA, CAN-SPAM, and the CFAA, a number of other federal laws have focused either on specific modes of communication or on narrow types of privacy problems. For example, the Identity Theft and Assumption Deterrence Act of 1998 made identity theft a federal crime punishable by up to 15 years in prison and fines up to $250,000;[47] the Electronic Communications Privacy Act of 1986,[48] which updated the Federal Wiretap Act of 1968, encompassed interception of computer and other digital and electronic communications; and the Telemarketing Sales Rule established the National "Do Not Call" Registry.[49]

Also, in addition to the California laws discussed above, there are a host of state laws which govern specific modalities or narrow privacy issues. For example, there are at least forty-five different state laws that govern some aspect of telephone solicitation, including a number of so-called "mini-TCPA" laws, which mirror federal legislation in their breadth.[50] There are also laws in all fifty states governing consent for recording calls, with twelve states requiring the consent of everyone involved in a phone conversation.[51] In addition, there are state laws

---

46. *See Privacy Laws*, STATE OF CAL. DEP'T OF JUST. OFFICE OF THE ATT'Y GEN., https://oag.ca.gov/privacy/privacy-laws (last visited Oct. 28, 2018) [hereinafter *California AG Privacy Summary*].

47. Identity Theft and Assumption Deterrence Act of 1998, Pub. L. No. 105-318, 112 Stat. 3007 (1998) (codified as amended at 18 U.S.C. § 1028 (2006) and 28 U.S.C. § 994 (2006)); *see* United States v. Karro, 257 F.3d 112, 117 (2d Cir. 2001).

48. Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (1986).

49. 16 C.F.R. §§ 310.1–310.9 (2018); *see also The Telemarketing Sales Rule*, FED. TRADE COMM'N CONSUMER INFO., https://www.consumer.ftc.gov/articles/0198-telemarketing-sales-rule (last visited Feb. 17, 2019) ("The Federal Trade Commission's Telemarketing Sales Rule (TSR) puts you in charge of the number of telemarketing calls you get at home. The TSR established the National Do Not Call Registry, which makes it easier and more efficient for you to reduce the number of unwanted telemarketing sales calls you get.").

50. *See* Patricia Pattison & Anthony F. McGann, *State Telemarketing Legislation: A Whole Lotta Law Goin' On*, 3 WYO. L. REV. 167, Appendix A (State Telemarketing Statutes) (2017); Dominique R. Shelton & David Carpenter, *Is Your Organization in Compliance with State Mini-TCPA Laws?*, ALSTON & BIRD (Oct. 7, 2014), https://www.alston.com/-/media/files/insights/publications/2014/10/iprivacy--security-advisoryi-is-your-organization/files/view-advisory-as-pdf/fileattachment/14803-minitcpaadvisory.pdf.

51. *See, e.g.*, KRISTEN RASMUSSEN ET AL., REPORTERS COMMITTEE FOR FREEDOM PRESS, REPORTER'S RECORDING GUIDE (2012), https://www.rcfp.org/wp-content/uploads/imported/RECORDING.pdf.

governing connected televisions, employee email communications, information held by Internet service providers, and e-readers.[52]

B. *Content-Focused Laws*

Aside from laws focused on a mode of communication or kind of document, other federal and state laws seek to regulate privacy in the context of specific types of data or industries. Just as the aforementioned laws seek to address a unique exigency related to a specific form of communication, these laws are intended to protect especially sensitive information.

1. The FCRA

Enacted in 1970, the Fair Credit Reporting Act (FCRA) has been amended a number of times, most notably in the Consumer Credit Reporting Reform Act of 1996 (the 1996 Amendments) and the Fair and Accurate Credit Transactions Act of 2003 (FACT Act).[53] As amended, the statute is designed broadly, to protect "information collected by consumer reporting agencies such as credit bureaus, medical information companies, and tenant screening services."[54] Among other things, the FCRA provides consumers with a bundle of core rights: (1) to know what is in a credit file, (2) to ask for a credit score, (3) to dispute incomplete or inaccurate information, (4) to give consent before reports are provided to employers, and (5) to seek redress in the event of identity theft.[55]

The FCRA may be enforced by states and the FTC.[56] In addition, the FCRA provides individuals with a private right of action, and the ability to recover actual or statutory damages ranging between $100 and $1,000, attorney's fees, costs, and punitive damages if the violation was willful.[57]

---

52. *See California AG Privacy Summary*, *supra* note 46; *State Laws Related to Privacy*, NAT'L CONF. OF STATE LEGISLATURES (Feb. 8, 2019), http://www.ncsl.org/research/telecommunications-and-information-technology/state-laws-related-to-Internet-privacy.aspx [hereinafter *NCSL Privacy Summary*].

53. 15 U.S.C. § 1681 (2018); *see also* FED. TRADE COMM'N, 40 YEARS OF EXPERIENCE WITH THE FAIR CREDIT REPORTING ACT: AN FTC STAFF REPORT WITH SUMMARY OF INTERPRETATIONS (2011), https://www.ftc.gov/sites/default/files/documents/reports/40-years-experience-fair-credit-reporting-act-ftc-staff-report-summary-interpretations/110720fcrareport.pdf.

54. *Fair Credit Reporting Act*, FED. TRADE COMM'N https://www.ftc.gov/enforcement/statutes/fair-credit-reporting-act (last visited Feb. 17, 2019).

55. *A Summary of Your Rights Under the Fair Credit Reporting Act*, FED. TRADE COMM'N, https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf (last visited Feb. 17, 2019).

56. *Id.*

57. Meir Feder & Rajeev Muttreja, *Understanding the Fair Credit Reporting Act*, PRACTICAL LAW, Apr.–May 2016, at 48, 52, http://www.jonesday.com/files/Publication/

2. IPAA

Like the FCRA, the Health Insurance Portability and Accountability Act of 1996 (HIPAA), together with the Standards for Privacy of Individually Identifiable Health Information (the Privacy Rule), is intended to protect an especially sensitive category of data: the health information of patients.[58] Passed in 1996, HIPAA was the first federal statute to regulate private healthcare.[59]

Generally, HIPAA applies to all so-called "covered entities," which include health plans, healthcare clearinghouses, and any healthcare provider that transmits health information in electronic form in connection with certain transactions affected by HIPAA,[60] as well as "business associates," or entities that act on behalf of, or provide certain services to, a covered entity, where those acts or services involve "individually identifiable health information."[61] "Individually identifiable health information" is defined as information including demographic data that relates to an individual's physical or mental health condition, provision of healthcare to the individual, or payment for the provision of health care to the individual.[62]

HIPAA limits permitted uses and disclosures to the following: (1) disclosures to the individual, unless required for access or accounting of disclosures; (2) as required for treatment, payment, and care operations; (3) where individuals agree to disclosure; (4) where disclosure is "incidental" to an otherwise lawful disclosure; (5) for public interest purposes; and (6) where information is disclosed as part of a "limited data set."[63]

---

e42f45d6-a8c6-43fc-a3d7-3fd302b447c6/Presentation/PublicationAttachment/1d5beeac-8049-48ec-9832-a45699daedeb/Understanding%20the%20FCRA.pdf.

58. 42 U.S.C. § 1320d (2018); *see also General Overview of Standards for Privacy of Individually Identifiable Health Information*, U.S. DEP'T OF HEALTH & HUMAN SERVS. (Apr. 3, 2003), https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/general-overview/index.html.

59. *It's Hip to Be Fair, HIPAA: What It Says, What It Means, What We Do, Presented to American Bar Association ERR and EEO Committees*, JONES DAY (Mar. 2004), http://www.jonesday.com/Its-Hip-to-Be-Fair-HIPAA-What-It-Says-What-It-Means-What-We-Do-Presented-to-American-Bar-Association-ERR-and-EEO-Committees-03-01-2004/.

60. *See General Overview of Standards for Privacy of Individually Identifiable Health Information*, *supra* note 58.

61. *Id.*

62. *What Is Individually Identifiable Health Information?*, HIPAA JOURNAL (Jan. 11, 2018), https://www.hipaajournal.com/individually-identifiable-health-information/.

63. *See* JONES DAY, *supra* note 59.

3. The GLBA

Aside from the FCRA and HIPAA, another prominent piece of federal privacy legislation which is aimed at a specific industry or type of information is the Gramm-Leach-Bliley Act (GLBA).[64] Broadly speaking and in the words of the FTC, the GLBA "requires financial institutions—companies that offer consumers financial products or services like loans, financial or investment advice, or insurance—to explain their information-sharing practices to their customers and to safeguard sensitive data."[65]

GLBA violators may be liable for civil and criminal penalties, including fines of $100,000 for each violation and imprisonment for up to five years.[66]

4. Content-Focused Laws in California

As on the federal level, California also has a number of privacy laws aimed at protecting particularly sensitive information. For a few examples, the Consumer Credit Reporting Agencies Act, like the FCRA, places restrictions on credit reporting agencies;[67] the Financial Information Privacy Act, like GLBA—though in more stringent fashion—prohibits financial institutions from sharing or selling personally identifiable nonpublic information;[68] the Confidentiality of Medical Information Act, like HIPAA, restricts the use and disclosure of patients' medical information;[69] and the Credit Card Full Disclosure Act

---

64. 15 U.S.C. § 6802 (2018).

65. *Gramm-Leach-Bliley Act*, FED. TRADE COMM'N, https://www.ftc.gov/tips-advice/business-center/privacy-and-security/gramm-leach-bliley-act (last visited Feb. 17, 2019).

66. 18 U.S.C. §§ 2721–2725 (West 1994 & Supp. 1994) (regulates the disclosure of personal information contained in the records of state motor vehicle departments); Reno v. Condon, 528 U.S. 141, 143 (2000); 18 U.S.C. § 2710(b) (2018) (limiting the conditions under which video rental or sales stores can disclose personally identifiable information, including viewing history).

67. *See* CAL. CIV. CODE § 1785.1(c) (West 2018) ("The Legislature finds and declares as follows: . . . (c) There is a need to ensure that consumer credit reporting agencies exercise their grave responsibilities with fairness, impartiality, and a respect for the consumer's right to privacy.").

68. *See* CAL. FIN. CODE § 4051 (West 2004) ("(a) The Legislature intends for financial institutions to provide their consumers notice and meaningful choice about how consumers' nonpublic personal information is shared or sold by their financial institutions. (b) It is the intent of the Legislature in enacting the California Financial Information Privacy Act to afford persons greater privacy protections than those provided in Public Law 106-102, the federal Gramm-Leach-Bliley Act, and that this division be interpreted to be consistent with that purpose.").

69. *See* CAL. CIV. CODE § 56.07 (West 2001).

allows credit card holders to opt out of the sharing of information by credit card companies.[70]

C. *Laws Protecting Children*

1. COPPA

Aside from privacy laws aimed at specific modalities or types of information, the third main category of privacy laws in the U.S. include laws protecting particularly vulnerable data subjects—children.[71] On the federal level, the Children's Online Privacy Protection Act (COPPA),[72] including the COPPA Rule,[73] is the primary law protecting children's privacy online. Passed in 1998, COPPA makes it unlawful for website operators to collect, use, or disclose children's information without verifiable parental consent.[74]

COPPA gives states and federal agencies, including most notably the FTC, authority to enforce compliance.[75] In addition, civil penalties for violation of the COPPA Rule can be as high as $41,484 per violation.[76]

2. California Laws Protecting Children

Finally, California has what is probably the nation's most robust regime aimed at protecting children's online privacy. The Privacy Rights for California Minors in the Digital World Act restricts certain types of marketing to minors.[77] It also allows minors who are registered users of an operator's site or service to request removal of personal content.[78] California Education Code Sections 49073.1 and 49073.6 and the Student Online Personal Information Protection Act are designed to protect student privacy.[79]

---

70. *See id.* § 1748.12 (West 2002).

71. *See, e.g.*, CAL. PEN. CODE § 964 (West 2003) (protecting personal information of witnesses and victims). Although this section focuses on children, the group most often given special privacy law protection, there are other laws aimed at protecting other sensitive data subjects.

72. *See* 15 U.S.C. §§ 6501–6506 (2018).

73. *See* 16 C.F.R. § 312 (2019).

74. 15 U.S.C. § 6502(b)(1)(A)(ii).

75. *Complying with COPPA: Frequently Asked Questions*, FED. TRADE COMM'N (Mar. 20, 2015), https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions.

76. *Id.*

77. CAL. BUS. & PROF. CODE §§ 22580–22582 (West 2015).

78. *See id.*

79. CAL. EDUC. CODE §§ 49073.1, 49073.6 (West 2016); *see* CAL. BUS. & PROF. CODE § 22584 (West 2016).

3. Other Laws Protecting Children

In addition to COPPA, the Family Educational Rights and Privacy Act of 1964 protects the privacy of student education records,[80] and provisions of HIPAA prohibit third parties from sharing a minor's personal information without the consent of the parent.[81] Likewise, the Children's Internet Protection Act, enacted in 2000, regulates children's access to obscene or harmful content over the Internet.[82] Aside from the California laws discussed below, the Delaware Online Privacy and Protection Act (DOPPA), which strictly regulates advertisements on websites directed at children, represents another state law effort to protect children online.[83]

II. PRIVACY LAW IN EUROPE

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.[84] 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."[85]

---

80. 20 U.S.C. § 1232g (2018). For an article arguing that privacy laws aimed at protecting children simply confer rights on children's parents and are thus insufficient, especially in the age of social media, see Stacey B. Steinberg, *Sharenting: Children's Privacy in the Age of Social Media*, 66 EMORY L.J. 839 (2017).

81. *Can a Minor Child's Doctor Talk to the Child's Parent About the Patient's Mental Health Status and Needs?*, U.S. DEP'T. OF HEALTH & HUMAN SERVS. (Sept. 12, 2017), https://www.hhs.gov/hipaa/for-professionals/faq/2092/can-minor-childs-doctor-talk-childs-parent-about-patients-mental-health-status-and-needs.html.

82. Consolidated Appropriations Act of 2001, Pub. L. No. 106-554, 114 Stat. 2763A-335 (2001).

83. DEL. CODE ANN. tit. 6, §§ 1201C–1206C (2015).

84. Paul M. Schwartz, *The EU-U.S. Privacy Collision: A Turn to Institutions and Procedures*, 126 HARV. L. REV. 1966, 1989 (2013) ("U.S. information privacy regulation was based on liberal norms and market forces, while the EU's information privacy regulations were based on 'social-protection norms' according to which 'data privacy is a political imperative anchored in fundamental human rights protection.'") (quoting Joel R. Reidenberg, *Resolving Conflicting International Data Privacy Rules in Cyberspace*, 52 STAN. L. REV. 1315, 1347 (2000)).

85. P. Amy Monahan, *Deconstructing Information Walls: The Impact of the European Data Directive on U.S. Businesses*, 29 L. & POL'Y INT'L BUS. 275, 277 (1998) ("Consistent with its free market emphasis, the United States takes a very sectoral approach to data protection. Most U.S. legislation focuses on the public sector, leaving the private sector to rely on voluntary compliance. In contrast, Europe has developed more omnibus standards to be applied to both government and private actors."); *see also infra* note 89.

A. *The EU Data Protection Directive*

Privacy laws in Europe stretch back a number of years,[86] but the first really significant and truly continental step towards comprehensive data protection and privacy legislation, passed on October 24, 1995, was Directive 95/46 of the European Parliament and the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, also known as "the Data Protection Directive" or simply, "the Directive."[87] Despite the long-running European emphasis on privacy, discussed above, the Directive was enacted with two competing goals in mind: (1) instituting a streamlined framework to help secure the free movement of data across internal EU borders; and (2) enshrining basic personal privacy and data security guarantees.[88]

Most notably, the Directive provided EU member states and private companies with a harmonized set of best practices as well as privacy and data protection principles. The Directive, in other words, was the first major piece of legislation to articulate broad, overarching terms regarding internet privacy. Expressly citing Article 8 of the European Convention for the Protection of Human Rights (ECPHR), drafted in 1950 and in force since 1953,[89] the Directive declared that "the object of the national laws on the processing of personal data is to protect fundamental rights and freedoms, notably the right to privacy."[90]

---

86. Neil Robinson et al., RAND CORP., REVIEW OF THE EUROPEAN DATA PROTECTION DIRECTIVE 6 (2009), https://www.rand.org/pubs/technical_reports/TR710.html [hereinafter RAND REPORT] ("At the European level, the protection of privacy as an essential human right has been encased in a number of regulatory texts, most of which came into being after the Second World War."); Monahan, *supra* note 85, at 283 ("Fueled by memories of the Third Reich's use of personal data to track targeted populations, European nations have long treated privacy as a fundamental human right.").

87. *See* Directive 95/46/EC, of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L 281) 31, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31995L0046&from=EN [hereinafter Directive].

88. *EU Data Protection Directive*, ELEC. PRIVACY INFO. CTR., https://www.epic.org/privacy/intl/eu_data_protection_directive.html (last visited Feb. 15, 2019).

89. Article 8 provides that "[e]veryone has the right to respect for his private and family life, his home and his correspondence." Convention for the Protection of Human Rights and Fundamental Freedoms, Apr. 11, 1950, E.T.S. No. 005, https://www.echr.coe.int/Documents/Convention_ENG.pdf [hereinafter ECPHR]. *See* Aisha Gani, *What Is the European Convention on Human Rights?*, GUARDIAN (Oct. 3, 2014), https://www.theguardian.com/law/2014/oct/03/what-is-european-convention-on-human-rights-echr.

90. *See* Directive, *supra* note 87, at 32.

Although the Directive was a massive step forward for privacy in the EU,[91] it was ultimately proven to be inadequate to the challenges posed by the Internet's rapid evolutions.[92] Among other weaknesses, the Directive ultimately left it to member states to implement and enforce their own national privacy legislation under the Directive's overarching standards.[93] But the Directive's narrower territorial scope hampered enforcement efforts against entities located outside the EU, most notably large U.S. companies like Google and Facebook—companies often seen by European privacy advocates as the chief violators of European privacy norms.[94]

B. *GDPR*

Following years of drafting and debate, the EU published GDPR in May 2016; the legislation went into effect in all EU Member states as of May 25, 2018.[95] While a number of provisions and principles stayed the same as the Directive, GDPR sweeps in a number of new data collectors and processors, as well as data subjects, and has vastly stronger enforcement mechanisms. In a lecture in January 2017, UK Information Commissioner Elizabeth Denham summed up the transition this way:

---

91. RAND REPORT, *supra* note 86, at 8 ("While the Directive was not conceptually innovative, it has had a very powerful impact in the EU and can be credited with creating a binding and harmonised framework for data protection principles in all Member States.").

92. B.J. Koops, *The Trouble with European Data Protection Law*, 4 INT'L DATA PRIVACY L. 250, 250 (2014) ("The trouble with the [European data protection] law, as with Hitchcock's Harry, is that it's dead. What the statutes describe and how the courts interpret this has usually only a marginal effect on data-processing practices.").

93. Monahan, *supra* note 85, at 286.

94. Despite the Directive's limitations, the European Court of Justice had already begun developing rules that extended European privacy laws abroad. *EU General Data Protection Regulation—Key Changes*, DLA PIPER, https://www.dlapiper.com/en/us/focus/eu-data-protection-regulation/key-changes/ (last visited Feb. 15, 2019) ("Europe's highest court, the Court of Justice of the European Union (the CJEU) has been developing jurisprudence on this concept, recently finding (*Google Spain SL, Google Inc. v. AEPD, Mario Costeja Gonzalez* (C-131/12)) that Google Inc. with EU based sales and advertising operations (in that particular case, a Spanish subsidiary) was established within the EU. More recently, the same court concluded (*Weltimmo v NAIH* (C-230/14)) that a Slovakian property website was also established in Hungary and therefore subject to Hungarian data protection laws.").

95. Commission 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, 2016 O.J. (L 119) 1, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679 [hereinafter GDPR]; JONES DAY, GENERAL DATA PROTECTION REGULATION GUIDE (2004), http://www.jonesday.com/files/upload/GDPR%20Pocket%20Guide%20A5%2004_17_18%20ENGLISH.pdf [hereinafter JONES DAY GDPR GUIDE].

"There's a lot in the GDPR you'll recognise from the current law, but make no mistake, this one's a game changer for everyone."[96]

Perhaps most importantly, GDPR's wide territorial scope has companies all over the world—and in the U.S. in particular—scrambling to adapt themselves to European privacy norms.[97] GDPR applies not only to businesses "established" in the EU, but also to any controller or processor conducting activities related to the offering of goods and services to data subjects "in the Union."[98] The GDPR also applies to the monitoring of such data subjects' behavior.[99] In other words, GDPR has nothing to do with citizenship or protecting the rights of Europeans, per se. Proceeding from a right to privacy that is discussed in Article 1 in universal terms, the law aims to protect anyone in Europe, even tourists.[100]

---

96. Elizabeth Denam, UK Info. Comm'r, Address at the Meeting of the Institute of Chartered Accountants in England and Wales (Jan. 17, 2017) (transcript available at https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2017/01/gdpr-and-accountability/).

97. Jeong, *supra* note 15.

98. Specifically, GDPR Art. 3 provides as follows:

> (1) This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.
>
> (2) This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:
>
> (a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or
>
> (b) the monitoring of their behaviour as far as their behaviour takes place within the Union.
>
> (3) This Regulation applies to the processing of personal data by a controller not established in the Union, but in a place where Member State law applies by virtue of public international law.

GDPR, *supra* note 95, at 32.

99. *Id.*

100. *The GDPR's Reach: Material and Territorial Scope Under Articles 2 and 3*, WILEY REIN LLP (May 2017), https://www.wileyrein.com/newsroom-newsletters-item-May_2017_PIF-The_GDPRs_Reach-Material_and_Territorial_Scope_Under_Articles_2_and_3.html ("Notably, Article 3(2) applies to the processing of personal data of any individual 'in the EU.' The individual's nationality or residence is irrelevant. The GDPR protects the personal data of citizens, residents, tourists, and other persons visiting the EU. So long as an individual is in the EU, any personal information of that person collected by any controller or processor who meets the requirements of Article 3(2) is subject to the GDPR. Where Article 3(2) applies, controllers or processors must appoint an EU-based representative."); *see also* Tess Blair et al., *Whose Data Is*

Additionally, GDPR expands the definition of "personal data," directly regulates processors for the first time, adds a new data protection principle ("accountability"), introduces new data breach notification requirements, and requires Data Protection Officers to be appointed under certain circumstances.[101] GDPR also contains a number of required disclosures for privacy policies including, among others, the identity and contact details of data "controllers";[102] the purposes of the data "processing" and the legal bases for doing so;[103] categories of personal data being processed;[104] categories of recipients receiving personal data;[105] the amount of time personal data is retained, or the factors in making that determination;[106] and the existence of specific consumer rights, such as the right to access, correct, and request deletion of data, as well as the right to lodge a complaint with a supervisory authority.[107]

GDPR introduces new and remarkably tough enforcement mechanisms. Most notably, GDPR introduces revenue-based fines of up to 4% of a company's global revenue.[108] Although it is still unclear, this calculation may include revenues of group companies, which have nothing to do with the collection or processing of the data in question.[109] In addition to revenue-based fines, Article 58 gives broad "investigative" and "corrective" powers to EU supervisory authorities and makes it much easier for data subjects to bring their own claims against controllers and processors.[110]

Finally, as with the "Safe Harbor" regime that was in place under the Directive, U.S. companies may certify GDPR compliance by registering with the U.S. Department of Commerce under the EU-U.S. and

---

Protected Under the GDPR?, LEXOLOGY (June 20, 2018), https://www.lexology.com/library/detail.aspx?g=0dc9663d-ac3b-438e-adcd-1415a45f99ca.

101. *See* GDPR, *supra* note 95, at 33–35; JONES DAY GDPR GUIDE, *supra* note 95, at 1.

102. GDPR, *supra* note 95, at 40. GDPR defines a data "controller" as "the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law." *Id.* at 33.

103. *Id.* at 40. GDPR defines data "processing" as "any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction." *Id.* at 33.

104. *Id.* at 41.

105. *Id.*

106. *Id.*

107. *Id.*

108. *See id.* at 82–83.

109. *See* JONES DAY GDPR GUIDE, *supra* note 95.

110. GDPR, *supra* note 95, at 69–70.

Swiss-U.S. Privacy Shield Frameworks.[111] In order to qualify, U.S. companies must develop a conforming privacy policy, identify an independent recourse mechanism, and self-certify through the Department of Commerce website.[112] As a result, participating organizations are deemed to have "adequate" privacy protection under GDPR.[113]

As of the time of this writing, it still remains to be seen what effect GDPR will have on European and American companies. Although privacy campaigner Max Screms has already initiated at least one high profile lawsuit against Facebook and Google, EU officials have yet to levy any fines.[114]

III. THE CALIFORNIA CONSUMER PRIVACY ACT

Just as the starting point for discussion of European privacy law is the ECPHR and the individual right to privacy, the starting point for discussion of California privacy law is Article I, Section 1 of the California Constitution, which provides that "[a]ll people 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*."[115] California is one of only ten states to enshrine privacy as an enumerated right in its constitution.[116] Perhaps in part because of this explicit constitutional right, California privacy law, even prior to the CCPA, has traditionally been far more elaborate—and strict—than that of any other state. In fact, the California Attorney General website lists 118 different "privacy" laws.[117] Nevertheless, in spite of this broad constitutional protection, and in spite of the California legislature's evident willingness to enact privacy

111. *See Privacy Shield Framework*, INT'L TRADE ADMIN., https://www.privacyshield.gov/welcome (last visited Feb. 24, 2019).

112. *U.S. Businesses*, INT'L TRADE ADMIN., https://www.privacyshield.gov/US-Businesses (last visited Feb. 24, 2019).

113. *Benefits of Participation*, INT'L TRADE ADMIN., https://www.privacyshield.gov/article?id=Benefits-of-Participation (last visited Feb. 24, 2019).

114. Derek Scally, *Max Schrems Files First Cases Under GDPR Against Facebook and Google*, IRISH TIMES (May 25, 2018), https://www.irishtimes.com/business/technology/max-schrems-files-first-cases-under-gdpr-against-facebook-and-google-1.3508177; Michele Gorman, *3 Things That Have (or Haven't) Happened Since the GDPR*, LAW360 (July 18, 2018), https://www.law360.com/articles/1061080/3-things-that-have-or-haven-t-happened-since-the-gdpr.

115. CAL. CONST. art. I, § 1 (emphasis added). *See also* J. Clark Kelso, *California's Constitutional Right to Privacy*, 19 PEPP. L. REV. 327 (1992), https://www.law.berkeley.edu/wp-content/uploads/2016/12/Kelso-Californias-Constitutional-Right-to-Privacy.pdf.

116. *Privacy Protections in State Constitutions*, NAT'L CONFERENCE OF STATE LEGISLATURES (Nov. 7, 2018), http://www.ncsl.org/research/telecommunications-and-information-technology/privacy-protections-in-state-constitutions.aspx.

117. *California AG Privacy Summary*, *supra* note 46.

legislation, the extant privacy laws in California are still narrowly tailored and can fit into the three categories discussed above: laws that are modality-focused, content-focused, or aimed at protecting children or other vulnerable groups.

Prior to the CCPA, the lone exception to this framework in California was the California Online Privacy Protection Act (CalOPPA), effective in 2004, which was already the broadest internet privacy law in the United States.[118] Among other things, CalOPPA—the first law in the nation to do so—requires commercial websites and online services to post a privacy policy.[119] The privacy policy must be posted "conspicuously," must state clearly what information is collected, and who that information is shared with.[120] In 2013, the law was amended to require website privacy policies to disclose whether operators respond to "Do Not Track" signals.[121] However, CalOPPA is focused more on transparency than on empowering consumers to take back control of their data. By contrast, the CCPA is more focused on the issue of consumer control.

A. *The Ballot Initiative*

Notwithstanding any other comparisons to European privacy law, the CCPA's origins, at least, are uniquely Californian. According to a number of interviews he has given, Alastair Mactaggart, the 51-year-old Bay Area real estate mogul behind the ballot initiative, first became "concerned about data privacy" while talking to a Google engineer at a cocktail party.[122] Reportedly, Mactaggart asked the engineer whether he should be "worried" about the information companies like Google were collecting about users.[123] According to Mactaggart, the engineer replied,

---

118. CAL. BUS. & PROF. CODE §§ 22575–22579 (West 2014).

119. *California Online Privacy Protection Act*, CONSUMER FED'N OF CAL. EDUC. FOUND. (July 29, 2015), https://consumercal.org/about-cfc/cfc-education-foundation/california-online-privacy-protection-act-caloppa-3/.

120. *Id.*

121. *California Amends Online Privacy Policy Law to Require Tracking Disclosures*, HUNTON ANDREWS KURTH PRIVACY & INFO. SECURITY LAW BLOG (Sept. 30, 2017), https://www.huntonprivacyblog.com/2013/09/30/california-amends-online-privacy-policy-law-to-require-tracking-disclosures/.

122. Daisuke Wakabayashi, *Silicon Valley Faces Regulatory Fight on Its Home Turf*, N.Y. TIMES (May 13, 2018), https://www.nytimes.com/2018/05/13/business/california-data-privacy-ballot-measure.html.

123. Nicholas Confessore, *The Unlikely Activists Who Took on Silicon Valley—and Won*, N.Y. TIMES MAG. (Aug. 14, 2018), https://www.nytimes.com/2018/08/14/magazine/facebook-google-privacy-data.html.

"If people just understood how much we knew about them, they'd be really worried."[124]

Mactaggart then convinced Rick Arney, a finance executive who had worked as a legislative analyst in the California State Senate, to help him with a ballot initiative.[125] Neither of the pair were especially savvy in privacy: they added Mary Stone Ross, who previously worked at the Central Intelligence Agency and had been legal counsel for the House of Representatives Intelligence Committee.[126]

As any California resident knows, the ballot measure process can play a high-profile and often contentious place in California politics.[127] Generally, there are two ways to put a ballot measure up for a popular vote: (1) the legislature may place constitutional amendments, bond measures, and proposed changes in existing law on the ballot; and (2) any California voter can put on the ballot a referendum—which submits to voters a statute already passed by the legislature—or an initiative that proposes, or "initiates," a statute or constitutional amendment.[128] To qualify an initiative, organizers must secure 365,880 votes.[129] According to reports, Mactaggart, Arney, and Ross submitted more than 600,000.[130] Not surprisingly, a number of major tech companies, including Google and Facebook, publicly opposed the initiative and even created an organization to that end: "The Committee to Protect California Jobs."[131]

---

124. *About Us*, CALIFORNIANS FOR CONSUMER PRIVACY, https://www.caprivacy.org/about-us (last visited Feb. 24, 2019).

125. Daisuke Wakabayashi, *California Passes Sweeping Law to Protect Online Privacy*, N.Y. TIMES (June 28, 2018), https://www.nytimes.com/2018/06/28/technology/california-online-privacy-law.html.

126. *Id.*

127. *See* Hillel Aron, *How California's Ballot Measure Process Got So Kooky*, L.A. WEEKLY (Oct. 22, 2016), http://www.laweekly.com/news/how-californias-ballot-measure-process-got-so-kooky-7526677 (discussing, *inter alia*, Proposition 13, passed in 1978, which drastically reduced property taxes and required two-thirds voter support for future tax increases; Proposition 64, defeated in 1986, which would have added AIDS to the state's list of communicable diseases; Proposition 161, defeated in 1992, which would have legalized assisted suicide; and Proposition 8, passed in 2008, which banned same-sex marriage).

128. *See Ballot Measures*, CAL. SEC'Y OF STATE, http://www.sos.ca.gov/elections/ballot-measures/ (last visited Feb. 15, 2019).

129. *See How to Qualify an Initiative: Statewide Ballot Initiative Guide*, CAL. SEC'Y OF STATE, http://www.sos.ca.gov/elections/ballot-measures/how-qualify-initiative/ (last visited Feb. 15, 2019).

130. Issie Lapowsky, *California Unanimously Passes Historic Privacy Bill*, WIRED (June 28, 2018, 5:57 PM), https://www.wired.com/story/california-unanimously-passes-historic-privacy-bill/.

131. *See* Julia B. Jacobson et al., *Frequently Asked Questions About the California Consumer Privacy Act of 2018*, K&L GATES: "STAY INFORMED" BLOG (July 31, 2018), http://www.klgates.com/frequently-asked-questions-about-the-california-consumer-privacy-act-of-2018-ccpa-07-31-2018/.

As originally drafted, the initiative granted consumers three core 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 consumers under 16 years 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.[132] Summing up these rights, the website launched for the initiative declared the following mission: "Your life is not their business."[133]

In response to a request from concerned legislators that the initiative be withdrawn, the initiative's drafters set a deadline of June 28, 2018 for the legislature to pass comparable privacy legislation—or else face the initiative appearing on the November ballot with risk of passage by the voters in November.[134] Critically, the initiative would have provided lawmakers with little wiggle room to make changes to the law: unlike regular legislation, ballot initiatives cannot be amended by the legislature.[135] Faced with this reality, the legislature hastily introduced A.B. 375, a bill substantially similar to the initiative, which passed on the same day as the deadline.[136] The bill was passed under the same name as the ballot initiative: The California Consumer Privacy Act.

B. *The California Consumer Privacy Act*

Except for a much more limited private right of action and a key whistleblower provision included in the original initiative, A.B. 375 preserves the core rights enshrined by the initiative's drafters and adds a fourth key right: the right to have a business delete a consumer's personal

---

132. Mary Ross & Alastair Mactaggart, *The Consumer Right to Privacy Act of 2018—Version 2*, CAL. OFFICE OF THE ATT'Y GEN. (Nov. 17, 2017), https://oag.ca.gov/system/files/initiatives/pdfs/17-0039%20%28Consumer%20Privacy%20V2%29.pdf [hereinafter *Ballot Initiative*]. *See also About the California Consumer Privacy Act*, CALIFORNIANS FOR CONSUMER PRIVACY, https://www.caprivacy.org/about (last visited Feb. 15, 2019).

133. CALIFORNIANS FOR CONSUMER PRIVACY, *supra* note 124.

134. *See id.* ("In mid-May 2018, we were contacted by Senator Robert Hertzberg and Assemblyman Ed Chau, of the California Legislature, to see if I would withdraw the initiative from the ballot, if the California Legislature passed a law addressing our privacy concerns. We replied that we would withdraw the initiative, *if* the Legislature passed a law replicating all its critical components, prior to our statutory deadline to withdraw, which was 5PM on Thursday June 28th, 2018.").

135. Kristen J. Matthews & Courtney M. Bowman, *The California Consumer Privacy Act of 2018*, PROSKAUER ROSE LLP: PRIVACY LAW BLOG (July 13, 2018), https://privacylaw.proskauer.com/2018/07/articles/data-privacy-laws/the-california-consumer-privacy-act-of-2018/.

136. *See* Heather Kelly, *California Passes Strictest Online Privacy Law in the Country*, CNN BUS. (June 29, 2018, 12:03 PM), https://money.cnn.com/2018/06/28/technology/california-consumer-privacy-act/index.html.

information, with some exceptions.[137] Below is a brief overview of the law's key components.

1. Who (and What) is Covered by the CCPA?

Generally, the CCPA applies to a "business," defined as any 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, and that satisfies one or more of the following thresholds": brings in annual gross revenue "in excess of $25,000,000"; buys, sells, receives, or shares, for commercial purposes, the personal information of 50,000 or more "consumers, households, or devices"; or derives 50% or more of its annual revenues from selling consumers' personal information.[138] The definition also includes "[a]ny entity that controls or is controlled by a business, as defined in [the main "business" definition], and that shares common branding with the business."[139]

The CCPA defines a "consumer" as "a natural person who is a California resident,"[140] and "personal information" as "information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household."[141] The CCPA also lists a number of "personal information" examples, including without limitation: names, aliases, postal addresses, IP addresses, social security numbers, and "other similar identifiers," together with biometric information, geolocation data, "professional or employment-related information," and "education information." This definition, and the Act as a whole, "apply to the collection and sale of all personal information collected by a business from consumers," whether in electronic, paper, or other form.[142]

---

137. CAL. CIV. CODE § 1798.105 (West 2018).

138. *Id.* § 1798.140(c)(1). This definition is broader than the initiative, which set the revenue floor at $50,000,000 and the floor for "consumers or devices" at $100,000. *Ballot Initiative*, *supra* note 132, at 8.

139. *Id.* § 1798.140(c)(2). According to the International Association of Privacy Professionals (IAPP), the law will likely affect more than half a million U.S. companies, "the vast majority of which are small- to medium-sized enterprises." Rita Heimes, *New California Privacy Law to Affect More Than Half a Million U.S. Companies*, IAPP (July 2, 2018), https://iapp.org/news/a/new-california-privacy-law-to-affect-more-than-half-a-million-us-companies/.

140. "Resident" is defined according to state tax regulations. CAL. CIV. CODE § 1798.140(g).

141. *Id.* § 1798.140(o)(1). The Act also expressly excludes certain information covered by other statutes, including HIPAA, the FCRA, the GLBA, and the DPPA. *Id.* § 1798.145.

142. This title is intended to *further the constitutional right of privacy* and to supplement existing laws relating to consumers' personal information, including, but not limited to, Chapter 22 (commencing with Section 22575) of

Critically, the Act also excludes certain personal information covered by federal privacy laws, namely HIPAA, the FCRA, the GLBA, and the DPPA. In cases of overlap with HIPAA, the Act "shall not apply to protected or health information that is collected by a covered entity," as "protected health information" and "covered entity" are defined in the HIPAA Privacy Rule.[143] And in the cases of overlap with the FCRA, the Act "shall not apply to the sale of personal information to or from a consumer reporting agency if that information is to be reported in, or used to generate, a consumer report," and "use of that information is limited by the [FCRA]."[144] If there is overlap with the GLBA and DPPA, the CCPA continues to apply unless it is "in conflict" with the federal statute.[145] The Act also excludes "publicly available information" from the "personal information" definition, though, as discussed below, what is "publicly available" is still vague.[146]

> Division 8 of the Business and Professions Code and Title 1.81 (commencing with Section 1798.80). The provisions of this title are *not limited to information collected electronically or over the Internet*, but apply to the collection and sale of all personal information collected by a business from consumers. Wherever possible, law relating to consumers' personal information should be construed to harmonize with the provisions of this title, but *in the event of a conflict between other laws and the provisions of this title, the provisions of the law that afford the greatest protection for the right of privacy for consumers shall control.*

Id. § 1798.175 (emphasis added).

143. *Id.* § 1798.145(c).

144. *Id.* § 1798.145(d).

145. *Id.* § 1798.145(e)–(f).

146. The Act defines "publicly available" as "information that is lawfully made available from federal, state, or local government records, if any conditions associated with such information," and excludes information that is used for a purpose that is not compatible with the purpose for which the data is maintained and made available in the government records or for which it is publicly maintained"; information that is "deidentified or aggregate consumer information" is also excluded. *Id.* § 1798.140(o)(2). "Aggregate consumer information" means "information that relates to a group or category of consumers, from which individual consumer identities have been removed, that is not linked or reasonably linkable to any consumer or household, including via a device." It "does not mean one or more individual consumer records that have been deidentified." *Id.* § 1798.140(a). "Deidentified" means "information that cannot reasonably identify, relate to, describe, be capable of being associated with, or be linked, directly or indirectly, to a particular consumer, provided that a business that uses deidentified information: (1) Has implemented technical safeguards that prohibit reidentification of the consumer to whom the information may pertain. (2) Has implemented business processes that specifically prohibit reidentification of the information. (3) Has implemented business processes to prevent inadvertent release of deidentified information. (4) Makes no attempt to reidentify the information." *Id.* § 1798.140(h).

2. What Specific Rights Are Conferred on Consumers?

Sections 1798.100–1798.125 convey a number of specific rights on consumers. Under 1798.100, consumers have "the right to request that a business that collects a consumer's personal information disclose to that consumer the categories and specific pieces of personal information the business has collected."[147] In response to these "verifiable consumer requests," the business must provide this information free of charge.[148]

Under Section 1798.105, "[a] consumer shall have the right to request that a business delete any personal information about the consumer which the business has collected from the consumer."[149] Following such request, the business must delete the information from its own records, as well as the records of its "service providers."[150] However, the Act lists some exceptions to this requirement: where retention of personal information is necessary to detect security incidents or protect against fraud, where necessary to comply with a legal obligation, or where such retention enables "solely internal uses that are reasonably aligned with the expectations of the consumer based on the consumer's relationship with the business."[151]

The Act also exempts from the deletion requirement businesses 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 . . . ."[152] Elsewhere in the Act, "research" is defined as "scientific, systematic study and observation, including basic research or applied research that is in the public interest and that adheres to all other applicable ethics and privacy laws or studies conducted in the public

147. *Id.* § 1798.100.

148. *Id.* § 1798.100(d) ("A business that receives a verifiable consumer request from a consumer to access personal information shall promptly take steps to disclose and deliver, free of charge to the consumer, the personal information required by this section.").

149. *Id.* § 1798.105.

150. *Id.* § 1798.105(c).

151. *Id.* § 1798.105(d). Although California had already enshrined a "right to be forgotten" or a "right to erasure" in the "Online Eraser" law, which took effect on January 1, 2015, this right only applied to minors under the age of 18. CAL. BUS. & PROF. CODE § 22580 *et seq. See also* Rahul Kapoor & W. Reece Hirsch, *Get to Know California's 'Online Eraser' Law*, MORGAN LEWIS: TECH & SOURCING (July 12, 2016), https://www.morganlewis.com/blogs/sourcingatmorganlewis/2016/07/get-to-know-californias-online-eraser-law. Nevertheless, despite no U.S. legal requirement to do so, it is not unusual for American businesses to allow users to request deletion. *See, e.g.*, Chris Smith, *How to Delete Your Facebook Account and Reclaim Your Data*, N.Y. POST (Mar. 20, 2018), https://nypost.com/2018/03/20/how-to-delete-your-facebook-account-and-reclaim-your-data/. *But see Privacy Policy*, APPLE INC. (May 22, 2018), https://www.apple.com/legal/privacy/en-ww/ (limiting users' deletion rights where Apple is required to retain it for legitimate business purposes).

152. CAL. CIV. CODE § 1798.105(d)(6).

interest in the area of public health."[153] The Act also requires that:

> Research with personal information that may have been collected from a consumer in the course of the consumer's interactions with a business' service or device for other purposes shall be: (1) Compatible with the business purpose for which it was collected. (2) Subsequently pseudonymized and deidentified, or deidentified and in the aggregate . . . (3) Made subject to technical safeguards that prohibit reidentification . . . (4) Subject to business processes that specifically prohibit reidentification . . . (5) Made subject to business processes to prevent inadvertent release of deidentified information. (6) Protected from any reidentification attempts. (7) Used solely for research purposes that are compatible with the context in which the personal information was collected. (8) Not be used for any commercial purpose.[154]

With respect to Section 1798.110, consumers have the right to request the following from businesses that *collect* their information: (1) categories of personal information collected; "(2) The categories of sources from which the personal information is collected. (3) The business or commercial purpose[155] for collecting or selling personal

---

153. *Id.* § 1798.140(s).

154. The Act defines "pseudonymize" or "pseudonymization" as "the processing of personal information in a manner that renders the personal information no longer attributable to a specific consumer without the use of additional information, provided that the additional information is kept separately and is subject to technical and organizational measures to ensure that the personal information is not attributed to an identified or identifiable consumer." *Id.* § 1798.140(r).

155. "Business purpose" means "the use of personal information for the business's or a service provider's operational purposes, or other notified purposes." That use must be "reasonably necessary and proportionate to achieve the operational purpose for which the personal information was collected or processed or for another operational purpose that is compatible with the context in which the personal information was collected." Business purposes are: (1) "Auditing related to a current interaction with the consumer and concurrent transactions, including, but not limited to, counting ad impressions to unique visitors, verifying positioning and quality of ad impressions, and auditing compliance with this specification and other standards." (2) The detection, prevention and prosecution of security incidents and "deceptive, fraudulent, or illegal activity. (3) Debugging to identify and repair errors that impair existing intended functionality. (4) Short-term, transient use, provided the personal information that is not disclosed to another third party and is not used to build a profile about a consumer or otherwise alter an individual consumer's experience outside the current interaction, including, but not limited to, the contextual customization of ads shown as part of the same interaction. (5) Performing services on behalf of the business or service provider, including maintaining or servicing accounts, providing customer service, processing or fulfilling orders and transactions, verifying customer information, processing payments, providing financing, providing advertising or marketing services, providing analytic services, or providing similar services on behalf of the business or service provider. (6) Undertaking internal research for technological development and demonstration. (7) Undertaking

information. (4) The categories of third parties with whom the business shares personal information. (5) The specific pieces of personal information it has collected about that consumer." "Collect" is defined as "buying, renting, gathering, obtaining, receiving, or accessing any personal information pertaining to a consumer by any means. This includes receiving information from the consumer, either actively or passively, or by observing the consumer's behavior."[156]

Similarly, under Section 1798.115, consumers have the right to request the following from businesses that *sell* the consumer's information: "(1) The categories of personal information 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."[157] "Sell" is defined broadly as "selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's personal information by the business to another business or a third party for monetary or other valuable consideration."[158]

Section 1798.120 provides that a "consumer shall have the right, at any time, to direct a business that sells personal information about the consumer to third parties not to sell the consumer's personal

---

activities to verify or maintain the quality or safety of a service or device that is owned, manufactured, manufactured for, or controlled by the business, and to improve, upgrade, or enhance the service or device that is owned, manufactured, manufactured for, or controlled by the business." *Id.* § 1798.140(d).

Likewise, "commercial purposes" is defined as "to advance a person's commercial or economic interests, such as by inducing another person to buy, rent, lease, join, subscribe to, provide, or exchange products, goods, property, information, or services, or enabling or effecting, directly or indirectly, a commercial transaction." It does not include "engaging in speech that state or federal courts have recognized as noncommercial speech, including political speech and journalism." *Id.* § 1798.140(f).

156. *Id.* § 1798.140(e).

157. *Id.* § 1798.115.

158. *Id.* § 1798.140(t)(1). *But see id.* § 1798.140(t)(2) (excluding from the "sale" definition a number of scenarios, including where "(A) A consumer uses or directs the business to intentionally disclose personal information or uses the business to intentionally interact with a third party; (B) The business uses or shares an identifier . . . for the purposes of alerting third parties that the consumer has opted out of the sale of . . . personal information; (C) The business uses or shares with a service provider," for business purposes, provided "(i) the business has provided notice that information [is] being used or shared" and "(ii) the service provider does not further collect, sell, or use the personal information"; and "(D) The business transfers to a third party the personal information as . . . part of a merger, acquisition, bankruptcy, or other transaction.").

information.[159] This right may be referred to as the right to opt-out."[160] This section also requires an affirmative "opt-in" for consumers under 16 years of age.[161] The Act also requires that businesses "[m]ake available to consumers two or more designated methods for submitting requests for information required to be disclosed . . . including, at a minimum, a toll-free telephone number, and if the business maintains an Internet Web site, a Web site address."[162] The Act also provides that a business receiving a "verifiable consumer request"[163] for information or deletion, for example, must "[d]isclose and deliver the required information to a consumer free of charge within 45 days of receiving" the request.[164]

Finally, Section 1798.125 provides that businesses "shall not discriminate against a consumer because the consumer exercised any of the consumer's rights."[165] Example discrimination includes, but is not limited to: "(A) Denying goods or services to the consumer. (B) Charging different prices or rates for goods or services . . . (C) Providing a different level or quality of goods or services to the consumer. (D) Suggesting the

---

159. *Id.* § 1798.120

160. *Id.* § 1798.120(a).

161. For consumers between 13 and 16, the consumer must opt in; for consumers under 13, the consumer's parent or guardian must opt in. *Id.* § 1798.120(d)

162. *Id.* § 1798.130(a)(1).

163. *Id.* § 1798.130(a)(2). *See also id.* § 1798.140(y) ("[V]erifiable consumer request" means "a request that is made by a consumer, by a consumer on behalf of the consumer's minor child, or by a natural person or a person registered with the Secretary of State, authorized by the consumer to act on the consumer's behalf, and that the business can reasonably verify, pursuant to regulations adopted by the Attorney General pursuant to [Section 1798.185 of the Act] to be the consumer about whom the business has collected personal information.").

164. *Id.* § 1798.130(a)(2). The Act provides further as follows:

> The business shall promptly take steps to determine whether the request is a verifiable consumer request, but this shall not extend the business's duty to disclose and deliver the information within 45 days of receipt of the consumer's request. The time period to provide the required information may be extended once by an additional 45 days when reasonably necessary, provided the consumer is provided notice of the extension within the first 45-day period. The disclosure shall cover the 12-month period preceding the business's receipt of the verifiable consumer request and shall be made in writing and delivered through the consumer's account with the business, if the consumer maintains an account with the business, or by mail or electronically at the consumer's option if the consumer does not maintain an account with the business, in a readily useable format that allows the consumer to transmit this information from one entity to another entity without hindrance. The business shall not require the consumer to create an account with the business in order to make a verifiable consumer request.

Id.

165. *Id.* § 1798.125(a)(1).

consumer will receive a different price."[166] The Act also provides, however, that nothing prohibits a business from charging different prices, or delivering different quality, if the prices or quality are "reasonably related to the value provided to the consumer by the consumer's data."[167] The Act also expressly permits businesses to "offer financial incentives, including payments to consumers as compensation," for the collection, sale, or deletion of personal information.[168]

3. What Must Businesses Disclose in Their Privacy Policies?

Under the Act, a business must "[d]isclose the following information in its online privacy policy or policies . . . and in any California-specific description of consumers' privacy rights"[169]: "A description of a consumer's rights pursuant to Sections 1798.110, 1798.115, and 1798.125[170] and one or more designated methods for submitting requests" for information; "categories of personal information it has collected about consumers in the preceding 12 months;" categories of sources from which personal information has been collected in the preceding 12 months; the business or commercial purpose for collection or sale; categories of personal information it has sold or disclosed for a business purpose in the preceding 12 months; the consumer's right to opt out of the sale of personal information; and the consumer's right to request deletion of personal information.[171] Additionally, "at or before the point of collection," businesses must "inform consumers as to the categories of personal information to be collected and the purposes for which the categories of personal information shall be used."[172]

4. What Additional Notifications Are Required?

Aside from required privacy policy disclosures, the CCPA introduces two more notice requirements with the potential to have a tremendous impact. First, any business required to grant a consumer the right to opt-out of the sale of personal information must also "[p]rovide a clear and

166. *Id.*

167. *Id.* § 1798.125(a)(2).

168. *Id.* § 1798.125(b)(1).

169. "[I]f the business does not maintain those policies," the disclosures may be posted on its Internet Web site. In any case, the information must be updated at least once every 12 months. *Id.* § 1798.130(a)(5).

170. The rights provided in Sections 1798.110, 1798.115, and 1798.125 are discussed above. *See supra* Section III.B.2.

171. CAL. CIV. CODE § 1798.130(a)(5).

172. *Id.* § 1798.100(b).

conspicuous link on the business's Internet homepage,[173] titled 'Do Not Sell My Personal Information,' to an Internet Web page that enables a consumer, or a person authorized by the consumer, to opt-out of the sale of the consumer's personal information."[174]

Second, the business must also include a description of consumers' opt-out rights, along with a separate link to the "Do Not Sell My Personal Information" webpage in its online privacy policy and in any California-specific description of consumers' privacy rights.[175]

5. What Remedies Do Consumers Have?

As passed by the legislature, the broad private right of action included in the ballot initiative was removed. However, under Section 1798.150, "[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 for": (1) statutory damages from $100 to $750 per consumer per incident, or actual damages, whichever is greater; (2) injunctive or declaratory relief; or (3) "[a]ny other relief the court deems proper."[176]

However, the consumer's right to bring an action as described above is subject to the following requirements: (1) before initiating any action on an individual or class-wide basis, the consumer must provide the business with 30 days' written notice of the specific provisions of the CCPA the consumer alleges have been violated, which the business has a 30-day opportunity to cure; (2) the consumer must "notify the Attorney General within 30 days that the action has been filed;" and (3) "[t]he Attorney General, upon receiving such notice, within 30 days, shall do one of the following:" (A) "[n]otify the consumer of the Attorney General's intent to prosecute an action against the violation;" "[i]f the Attorney General does not prosecute within six months, the consumer may proceed with the action;" (B) "[r]efrain from acting within the 30 days, allowing the consumer to bring the action to proceed;" or (C)

---

173. *Id.* § 1798.140(l) ("'Homepage' means the introductory page of an Internet Web site and any Internet Web page where personal information is collected. In the case of an online service, such as a mobile application, homepage means the application's platform page or download page, a link within the application, such as from the application configuration, 'About,' 'Information,' or settings page, and any other location that allows consumers to review [required notices] before downloading the application.").

174. *Id.* § 1798.135(a)(1).

175. *Id.* § 1798.135(a)(2).

176. *Id.* § 1798.150(a)(1).

"[n]otify the consumer that the consumer shall not be permitted to proceed with the action."[177]

6. What Powers Does the Attorney General Have?

In addition to the above right of action, the California Attorney General can also enforce the Act, with civil penalties for violations as high as $7,500 per violation.[178] Of the proceeds of any such lawsuits, 20% goes to a new "Consumer Privacy Fund," which would fund further lawsuits against violators.[179] The remaining 80% goes to "the jurisdiction on whose behalf the action leading to the civil penalty was brought."[180]

The Act also provides that the Attorney General "shall solicit broad public participation" in writing regulations for the Act, including: (1) updating the personal information definition; (2) updating the definition of unique identifiers; (3) "[e]stablishing any exceptions necessary to comply with state or federal law"; (4) establishing additional rules governing consumer requests and opt-outs; (5) adjusting monetary thresholds for company revenue that subject a company to the Act; (6) establishing additional rules to ensure information and notices provided to consumers are easily understood by all consumers, including disabled consumers or foreign language speakers; and (7) establishing additional rules to further consumers' privacy rights, with the goal of minimizing the administrative burden on consumers.[181] The Attorney General may also pursue any other regulations "as necessary to further the purposes" of the Act.[182]

IV. TOWARDS A EUROPEAN-STYLE PRIVACY REGIME?

A. *The CCPA, GDPR, and the Future of American Privacy Law*

Because of its sweeping nature, the CCPA is an unprecedented piece of legislation. By enshrining basic internet privacy rights, transferring essential control over consumer data back to consumers—rather than simply requiring transparency, as with CalOPPA—and placing the onus to enforce the law on state regulators rather than private citizens, California's new law, broadly speaking, has much more in common with

177. *Id.* § 1798.150(b), *amended by* 2018 Cal. Legis. Serv. 735 (West).
178. *Id.* § 1798.155(b).
179. *Id.* § 1798.155(c)(1).
180. *Id.* § 1798.155(c)(2), *amended by* 2018 Cal. Legis. Serv. 735 (West).
181. *Id.* § 1798.185(a).
182. *Id.* § 1798.185(b).

GDPR than with other American privacy laws.[183] But does it also suggest a more "European" future for privacy law in the United States?

As discussed in Section I of this article, the answer is "in some cases, yes, in others, no." While the CCPA may likely be a model—or at least a reference point—for future federal privacy legislation or similar copy-cat laws in other states,[184] underlying norms and values are not as easy to change. And regardless of whether the legislation will be a model for future statutes, it will likely emerge as the de facto national standard given the size and reach of California's economy.[185] Europe has

183. *See* Sarah Meyer, *Tech Companies Ready to Battle New California Data Privacy Law*, CPO MAG. (July 13, 2018), https://www.cpomagazine.com/2018/07/13/tech-companies-ready-to-battle-new-california-data-privacy-law/ ("The legislation bears a striking resemblance to the European Union General Data Protection Regulation (GDPR) and places responsibility for data use squarely in the hands of the consumer."); *Proskauer Summary*, *supra* note 17 ("[I]t's likely that many companies will find the compliance process as much of a struggle as their GDPR compliance efforts."); Lydia de la Torre, *GDPR Matchup: The California Consumer Privacy Act 2018*, IAPP (July 31, 2018), https://iapp.org/news/a/gdpr-matchup-california-consumer-privacy-act/ ("As the first U.S. attempt at a comprehensive data protection law, the CCPA has the potential to become as consequential as the GDPR. After all, California is the fifth largest economy in the world, the home of many technology titans, and traditionally a trend-setting state for data protection and privacy in the U.S."); *California Moves Towards GDPR-Like Privacy Protections in the California Consumer Privacy Act of 2018*, FOLEY & LARDNER LLP (July 2, 2018), https://www.foley.com/california-moves-towards-gdpr-like-privacy-protections-in-the-california-consumer-privacy-act-of-2018-07-02-2018/ ("The new law gives consumers broad rights to access and control of their personal information and imposes technical, notice, and financial obligations on affected businesses. CCPA was enacted to protect the privacy of California consumers and has some similar characteristics to the EU's General Data Protection Regulation (GDPR), including a new and very broad definition of what is included in protected personal information."). *But see* Tim Peterson, *Why California's New Consumer Privacy Law Won't Be GDPR 2.0*, DIGIDAY (July 9, 2018), https://digiday.com/marketing/californias-consumer-privacy-law-has-digital-ad-industry-searching-for-answers/ ("The law does not prevent companies from collecting people's information or give people an option to ask a company to stop collecting their information, differentiating it from GDPR.").

184. Malcolm Chisholm, *California Consumer Privacy Act of 2018 v. GDPR*, FIRST S.F. PARTNERS (June 29, 2018), https://www.firstsanfranciscopartners.com/blog/california-consumer-privacy-act-of-2018-vs-gdpr/ ("California often leads in innovations, and we can expect other states, and possibly the Federal government, to follow this initiative.").

185. *See* Alex Gray, *Which American State Has a Bigger Economy Than India?*, WORLD ECON. FORUM (July 8, 2016), https://www.weforum.org/agenda/2016/07/american-state-bigger-economy-than-india/ ("[I]f California were inserted into the world ranking by GDP according to country, it would come sixth—ahead of France, India, Italy and Brazil."). *See also* Reece Hirsch and Kristin Hadgis, *INSIGHT: California's New, GDPR-Like Privacy Law Is a Game-Changer*, BLOOMBERG BNA (July 11, 2018), https://www.bna.com/insight-californias-new-n73014477375/ ("Whatever the CCPA's national influence on lawmakers, for many companies it will be adopted as a *de facto* national standard."); *California's GDPR? Sweeping California Privacy Ballot Initiative Could Bring Sea Change to U.S. Privacy Regulation and Enforcement*, SIDLEY AUSTIN: PRIVACY AND CYBERSECURITY UPDATE (June 25, 2018), https://www.sidley.com/en/insights/newsupdates/2018/06/sweeping-california-privacy-ballot-initiative-could-bring-sea-change

historically considered the individual right to privacy as a value in and of itself, and has enshrined it explicitly in the ECPHR.[186] On the other hand, the free flow of information and its benefit to free enterprise has historically been much more significant in the U.S.[187] Also critical to the future of privacy legislation in the U.S., and perhaps as a result of these differences in values, the biggest tech companies tend to be American.[188] Despite nascent scrutiny of its practices in recent months, the tech community is likely—as it has in the past—to have considerable influence over future legal developments in the U.S., including amendments to the CCPA between now and 2020.[189]

Assuming that U.S. tech companies will have tremendous influence over the drafting of future privacy legislation—whether at the state or federal level—arguably suggests that any future privacy regime on this side of the Atlantic will be much more favorable to those tech companies than the European regime. It will, in other words, continue to perpetuate the underlying, un-European values that helped Silicon Valley to flourish in the first place. However, there are also good reasons for tech companies, and other companies that traffic in personal information, to favor overarching federal internet privacy legislation. For example, there is always the incentive—once consumers' and their legislators' appetite for legislation has reached a tipping point—for business interests to get out in front of a movement and make concessions.[190] More importantly,

---

("This initiative would likely create a de facto national standard on transparency around third-party sharing as well as consumer rights to restrict data sharing and could affect many business models that depend on data monetization to offer a free good or service.").

186. *See* ECPHR, *supra* note 89.

187. *See* Monahan, *supra* note 85.

188. Kristin Stoller, *The World's Largest Tech Companies 2018: Apple, Samsung Take Top Spots Again*, FORBES (June 6, 2018), https://www.forbes.com/sites/kristinstoller/2018/06/06/worlds-largest-tech-companies-2018-global-2000/#41c38c244de6 ("Though the U.S. remains on top, Asian companies are slowly inching their way onto our list of the top technology companies in the world.").

189. *See* David Meyer, *'We Look Forward to Improvements.' Big Tech Plans to Fight Back Against California's Sweeping New Data Privacy Law*, FORTUNE (July 2, 2018), http://fortune.com/2018/07/02/california-data-privacy-ab-375-big-tech-fightback/ (quoting Google spokeswoman Katherine Williams: "We appreciate that California legislators recognize these issues and we look forward to improvements to address the many unintended consequences of the law."); McKinnon & Vartabedian, *supra* note 12 ("The effort by tech coalitions . . . comes after the industry has fended off many types of federal action on privacy for years."); Meyer, *supra* note 183 ("The battle lines have been drawn in the war for privacy protection. The ballot initiative seems to be off the table for now and tech companies are lobbying strongly to protect their right to use and sell data to thirds parties.").

190. Indeed, according to a recent report in The New York Times, tech companies are already lobbying federal legislators for a more favorable law which would "overrule" the CCPA. Cecilia Kang, *Tech Industry Pursues a Federal Privacy Law, on Its Own Terms*, N.Y. TIMES (Aug. 26, 2018), https://www.nytimes.com/2018/08/26/technology/tech-industry-federal-privacy-law.html

any federal legislation preempting state law, and potentially even supplanting portions of other federal laws such as HIPAA or GLBA, could greatly simplify the complex privacy regime discussed in this Article and thus reduce compliance costs for companies.[191]

It is also worth noting that, in addition to their lobbying advantage, big tech companies are best able—as incumbents, and given their massive financial resources—to comply with privacy legislation and regulations.[192] In other words, sweeping privacy legislation and attendant regulations are likely, as any new legal regime, to hit medium- and small-sized companies hardest.[193]

For now, at least, all U.S. companies will have to continue to navigate a complex and duplicative privacy regime, with overlap of laws governing different, narrower aspects of privacy as well as laws at the federal and state levels. Following enactment of the CCPA, the American regime may become an even more complex hybrid system: at once a uniquely American legal "Wild West," where private citizens and the plaintiff's bar enforce and sometimes abuse a number of key privacy laws, but also a European-style state regulatory Leviathan, with the Federal Trade Commission as the de facto privacy regulator and the California state attorney general moving into a similar role once the CCPA takes effect.[194]

B. *Suggestions for Moving Forward*

Because the text of the CCPA does *not* place any restrictions on how it may be amended, there are, as a number of observers have pointed out, likely to be a number of changes to the law between now and when it goes into effect in 2020.[195] Below are some suggestions that would make

---

("In recent months, Facebook, Google, IBM, Microsoft and others have aggressively lobbied officials in the Trump administration and elsewhere to start outlining a federal privacy law, according to administration officials and the companies. The law would have a dual purpose, they said: It would overrule the California law and instead put into place a kinder set of rules that would give the companies wide leeway over how personal digital information was handled.").

191. *Id.* ("Top lobbyists for other tech companies agreed that [the CCPA] could be more problematic than the new European law, and that it would unleash a patchwork of state laws that would not only strap their businesses but become a regulatory headache, the people briefed on the meeting said.").

192. Chris Wilson, *The GOP Needs a Free Facebook*, WALL ST. J. (Apr. 9, 2018), https://www.wsj.com/articles/the-gop-needs-a-free-facebook-1523315383.

193. Michael Hendrix, *Regulations Impact Small Business and the Heart of America's Economy*, U.S. CHAMBER OF COMMERCE FOUND. (Mar. 14, 2017), https://www.uschamberfoundation.org/blog/post/regulations-impact-small-business-and-heart-americas-economy.

194. *See* Montezuma, *supra* note 22.

195. *See, e.g.*, *Proskauer Summary*, *supra* note 17; Adam Schwartz et al., *How to Improve the California Consumer Privacy Act of 2018*, ELEC. FRONTIER FOUND. (Aug. 8, 2018), https://www.eff.org/deeplinks/2018/08/how-improve-california-consumer-privacy-act-2018;

the CCPA—and U.S. internet privacy law in general—clearer, fairer, and more effective.[196]

1. Make the Private Right of Action More Meaningful

As the law is currently drafted, the California attorney general is in the driver's seat in terms of how the law is enforced. For that reason, much remains to be seen in terms of the impact the law will have on businesses. That said, because the law as it was passed removes the whistleblower provision[197] and the broad private right of action contained in the original ballot initiative, the attorney general is likely left with an impossible task: policing as many as a half million American businesses.[198]

Sue Poremba, *Tech Companies Cool Toward California Consumer Privacy Act*, SECURITY BOULEVARD (July 24, 2018), https://securityboulevard.com/2018/07/tech-companies-cool-toward-california-consumer-privacy-act/ ("Tech companies are expected to fight for changes before the law goes into effect. The bill was pushed through too quickly, they say, and it is too vague.").

196. At least one bill, S.B. 1121, has already been introduced to amend the CCPA. The bill is relatively limited, and only purports to (1) except health care providers and covered entities from the law's purview; (2) "delete the requirement that a consumer bringing a private right of action notify the Attorney General"; and (3) limit civil penalties to be assessed by the Attorney General to not more than $2,500 per violation or $7,500 for intentional violations, rather than a $7,500 limit for all violations. *See* S.B. 1121, 2017–18 Leg. Sess. (Cal. 2018), https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB1121.

197. *See* discussion *infra* Section IV.B.2.

198. *See* Heimes, *supra* note 139. In addition to specific adjustments to the CCPA text, the California legislature should take the opportunity to introduce meaningful cy pres reform. This practice has been particularly critical (and especially controversial) in the privacy context, with a number of high-profile privacy advocacy groups receiving large amounts of funding from privacy litigation. *See* Sara Randazzo, *Google Privacy Case Risks Disrupting a Key Source of Nonprofit Funding*, WALL ST. J. (Mar. 23, 2018), https://www.wsj.com/articles/google-privacy-case-risks-disrupting-a-key-source-of-nonprofit-funding-1521797400. In particular, the legislature should craft a regime in which awards from privacy litigation go only to (1) plaintiffs, (2) whistleblowers, and (3) the Consumer Privacy Fund already created by the CCPA. *See* Ted Frank, *Cy Pres Settlements*, ABA, https://www.americanbar.org/content/dam/aba/administrative/litigation/materials/2016_sac/written_materials/6_cy-pres_settlement.authcheckdam.pdf (summarizing the cy pres doctrine).

Authors have also discussed the constitutionality of the cy pres doctrine. *See* Jonah M. Knobler & Sam A. Yospe, *Frank v. Gaos: Cy Pres Gets Its Day at the Supreme Court*, 19 BLOOMBERG L. CLASS ACTION LITIG. REP. 587, 587–88 (2018), https://www.pbwt.com/content/uploads/2018/06/KnoblerYospePublisCLASS1.pdf. ("Increasingly, courts presiding over class actions employ a controversial practice called cy pres . . . that diverts damages owed to injured class members to non-party charitable institutions. The theory behind cy pres is that, when getting damage awards to class members is difficult, giving that money to a relevant charity is the next-best result. . . . Rule 23, which governs class actions in federal court, says nothing about cy pres. No statute affirmatively authorizes it. The Supreme Court has never said a word about it. . . . Some argue that cy pres is affirmatively prohibited by the Rules Enabling Act, the statute under which

In order for the CCPA to have its intended effect, it may be advisable to make the private right of action more meaningful by allowing citizens to sue in response to violations other than data breaches. The ballot initiative included a private right of action for injured consumers, including statutory damages of $1,000 per violation and up to $3,000 per violation for willful violations.[199] Although legislators should be careful about creating a "cash cow" situation for the plaintiff's bar, a private right of action—perhaps with reduced statutory damages figures—would deputize a host of "private attorneys general," allowing the private sector to better police itself. Provided the amount of litigation and dollar amounts are reasonable, allowing private lawsuits—and thus allowing courts to interpret and flesh out the CCPA's various ambiguities—could also help provide clarity for the business community.[200]

2. Include a Whistleblower Provision

The ballot initiative originally included a whistleblower provision which would have helped deputize watchdogs to ensure compliance. Specifically, the ballot initiative provided that:

> Any person who becomes aware, based on non-public information, that a person or business has violated this Act may file a civil action for civil penalties pursuant to [the Attorney General enforcement section], if prior to filing such action, the person files with the Attorney General a

---

the Federal Rules of Civil Procedure were promulgated. The Act states that those Rules—including Rule 23—'shall not abridge, enlarge or modify any substantive right.' 28 U.S.C. § 2072(b). . . . Indeed, some go even further and argue that class-action cy pres is unconstitutional. . . . For example, Article III's 'case or controversy' requirement may prohibit federal courts from ordering monetary awards to non-parties that are strangers to an adversarial proceeding and lack an injury-in-fact traceable to the defendant.") (citation omitted).

199. *Ballot Initiative*, *supra* note 132, at 13.

200. Unfortunately, the amendment process is not headed that direction. *See* Paul Karlsgodt, *California Consumer Privacy Act: Navigating Consumer Lawsuits & Limiting Remedies*, BAKER HOSTETLER: DATA PRIVACY MONITOR (Aug. 29, 2018), https://www.dataprivacymonitor.com/state-legislation/california-consumer-privacy-act-navigating-consumer-lawsuits-limiting-remedies/ ("The CCPA was amended on June 25 to add subsection (c) of Section 1798.150 to clarify 'Nothing in this act [proposed to be amended from "act" to "title"] shall be interpreted to serve as the basis for a private right of action under any other law.' Based on this amendment, it appears that the California Legislature intends to preclude having a business's violation of the CCPA serve as a basis for a claim under California's Unfair Competition Law (UCL), California Business and Professions Code (BPC) §§ 17200 et seq., which permits a private right of action for claims based on unlawful, unfair, or fraudulent business acts or practices—or under 'any other law.'").

> written request for the Attorney General to commence the action.[201]

Any whistleblower whose civil suit resulted in penalties would have been entitled to "an amount the court determines is reasonable," but "not less than 25 percent and not more than 50 percent of the proceeds of the action."[202]

A similar provision in the CCPA may help the law achieve its stated ends. In reality, the attorney general simply does not have the capacity to police a half million U.S. businesses. Putting the same or a substantially similar whistleblower provision—such as those in Sarbanes-Oxley and Dodd-Frank, for example—back into the legislation would likely result in more effective and more efficient enforcement; requiring whistleblowers to filter their claims through the attorney general could do so without unleashing a tidal wave of frivolous lawsuits.

3. Implement a More Effective Cure Period

The CCPA's thirty-day cure period is also problematic, but from two opposite perspectives. For relatively small or simple violations, a cure period arguably renders the enforcement provisions toothless—businesses will simply fix these types of problems as they surface rather than being proactive and compliant on the front-end. But a thirty-day cure period may be far too short for larger, more complex violations, as company-wide corrections would typically take much longer than this.

If the final version of the CCPA includes a cure period, it may make sense for it to be extended. This would not affect simple violations, which could likely be cured in thirty days, but would allow for systemic problems to be properly addressed and rectified, thus giving the provision meaning. Alternatively, the legislature could institute separate cure periods based on the nature of the violation.

4. Clarify the Definition of "Publicly Available" Information

As discussed above, the CCPA excludes "publicly available information" from the definition of personal information.[203] Publicly available information is defined as "information that is lawfully made available from federal, state, or local government records, if any conditions associated with such information."[204] The law also provides that:

---

201. *Ballot Initiative*, *supra* note 132, at 15.
202. *Id.* at 16.
203. CAL. CIV. CODE § 1798.140(o)(2) (West 2018).
204. *Id.*

> "Publicly available" does not mean biometric information collected by a business about a consumer without the consumer's knowledge. Information is not "publicly available" if that data is used for a purpose that is not compatible with the purpose for which the data is maintained and made available in the government records or for which it is publicly maintained. "Publicly available" does not include consumer information that is deidentified or aggregate consumer information.[205]

Despite these additional clarifications, the statute's definition remains vague. Most importantly, the inquiry into whether the purposes of the information's use and the original purposes for which it is maintained are "compatible" may raise a host of arguable questions about how personal information is being used. In the absence of further guidance in the statute, courts and regulators will likely have to drill down and ask questions about the original intent and purpose of statutes governing publicly available information in government records in order to determine whether subsequent uses are "compatible with the purpose for which the data is maintained." Likewise, there may be arguments around what constitutes "aggregate" consumer information.

5. Clarify the Deletion Requirement

As discussed above, Section 1798.105 allows a consumer to "request that a business delete any personal information about the consumer which the business has collected from the consumer."[206] But this deletion requirement potentially raises as many questions as it answers. Does the information have to be deleted forever? What if the information is later reobtained in some other, lawful way? The Act also requires businesses that receive a deletion request to also "direct any service providers to delete the consumer's personal information."[207] But what if the service provider refuses or is unable to comply? And how, in any case, would the covered business verify the service provider's compliance? Will the covered business be directly liable for any acts or omissions of the service provider? The structure contemplated here may result in a contractual flow similar to the GDPR data protection agreements and standard contractual clauses arising out of the data processor–data controller relationships.[208]

---

205. *Id.*

206. *Id.* § 1798.105(a).

207. *Id.* § 1798.105(c).

208. For an overview of data protection agreements between controllers and processors and standard contractual clauses, see *New Standard Contractual Clauses for Data Transfers Out of*

Additionally, the deletion requirement contains a number of exceptions, which are open to interpretation. For example, the business is not required to comply with the request if it is necessary to maintain the personal information in order to "provide a good or service requested by the consumer."[209] Does this inherently require businesses to respond to a deletion request by informing consumers how deletion of their data might affect services they are receiving, or are businesses allowed to simply ignore the request unless the consumer expressly requests deletion *even if it means canceling his or her services*? This section also allows business to maintain personal information in order to "[e]xercise free speech, ensure the right of another consumer to exercise his or her right of free speech, or exercise *another right provided for by law*."[210] What rights are included in this last, catch-all language? The right to perform contract obligations to a third party?

This section also allows businesses to maintain personal information "[t]o enable solely internal uses that are reasonably aligned with the expectations of the consumer based on the consumer's relationship with the business"[211] or to "use the consumer's personal information, internally, in a lawful manner that is compatible with the context in which the consumer provided the information."[212] As with the "publicly available information" definition, the CCPA's reference to "the expectations of the consumer," not defined, introduces needless ambiguity into the statute and should be cleaned from the law. Although businesses of course have an idea of consumer expectations in certain kinds of simple cases—a consumer who gives her phone number to a delivery company would expect her number be given to the delivery man in case the delivery man cannot find her house, for example—but there are likely to be a number of situations where "consumer expectations" will be complex and impossible for businesses to divine. Likewise, the allowance for internal uses that are "compatible with the context in which the consumer provided the information" raises similar questions about the meaning of "compatibility" discussed above.

6. Clarify the Interplay with Federal Statutes

As discussed above, the CCPA exempts certain personal information that is also covered by HIPAA, the GLBA, the FCRA, and the DPPA.[213]

---

the European Union Raise Concerns, JONES DAY (July 2010), https://www.jonesday.com/new_standard_contractual_clauses/.

209. CAL. CIV. CODE § 1798.105(d)(1).

210. *Id.* § 1798.105(d)(4) (emphasis added).

211. *Id.* § 1798.105(d)(7).

212. *Id.* § 1798.105(d)(9).

213. *Id.* § 1798.145(c)–(f).

But these exemptions are, as with other key terms in the Act, plagued by ambiguities. For example, in the case of HIPAA, the statute says that it "shall not apply to . . . protected health information that is collected by a covered entity."[214] But what about information collected *on behalf* of a covered entity? Does the exclusion apply to business associates, as a general matter?[215]

In the cases of overlaps with the GLBA and DPPA, what constitutes a conflict between these two laws and the CCPA that would trigger an exclusion? Must the conflict be direct? What about additional terms present in one statute but not another? Does the fact that the CCPA includes statutory damages but the GLBA does not constitute a conflict? And how do the provisions excluding GLBA- and DPPA-covered information in the case of a conflict interplay with Section 1798.175 of the CCPA, which states that "in the event of a conflict between other laws and the provisions of this title, the provisions of the law that afford the greatest protection for the right of privacy for consumers shall control."[216] Does this mean that in cases where there *is* a conflict between the Act and the relevant federal statute, the CCPA may nevertheless apply if it is deemed to afford greater privacy protections?

There are even more fundamental questions about interplay with federal statutes. Why have a full exemption for personal information covered by HIPAA and the FCRA, but only this qualified exemption for the GLBA and DPPA? And why choose these four laws over other privacy laws in the first place?

---

214. *Id.* § 1798.145(c)(1)(A). Under HIPAA, a "covered entity" is defined as (1) health plans, (2) health care clearinghouses, and (3) health care providers who electronically transmit any health information in connection with transactions for which HHS has adopted standards, and may include a business associate of another covered entity. 45 C.F.R. § 160.103 (2019); *see Who Must Comply with HIPAA Privacy Standards?*, U.S. DEP'T. OF HEALTH & HUMAN SERVS., https://www.hhs.gov/hipaa/for-professionals/faq/190/who-must-comply-with-hipaa-privacy-standards/index.html (last updated July 26, 2013).

215. A "business associate" is "a person or entity that performs certain functions or activities that involve the use or disclosure of protected health information on behalf of, or provides services to, a covered entity." *Business Associates*, U.S. DEPT. OF HEALTH & HUMAN SERVS., https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/business-associates/index.html (last updated July 26, 2013); *see* Adam H. Greene, *How a Rushed California Law Will Change the Privacy and Security Landscape for Mobile Health Apps*, LEXOLOGY (July 27, 2018), https://www.lexology.com/library/detail.aspx?g=06756c7a-61a5-4230-8505-7e2f26baa169 ("It is unclear whether the law will apply to protected health information of mobile health app developers who are business associates under HIPAA.").

216. CAL. CIV. CODE § 1798.175.

7. Clarify the 12-Month Requirement

The legislature should also amend the CCPA to clarify that requirements to disclose what personal information has been collected, sold, or disclosed for a business purpose in the "preceding 12 months" is not a running requirement, but rather a requirement to update such information once each calendar year.[217] As currently crafted, it is not at all clear whether this is an annual requirement, or a requirement that businesses constantly update this 12-month "lookback" so that it is always accurate. The latter would be unreasonable. Consider, for example, a situation where a market research firm enters into an agreement with a panel company, pursuant to which the panel company provides the market research firm with access to panels for survey research purposes. Does the CCPA require the market research firm to check in with the panel company (and any other panel companies it has engaged) every day to make sure the panel company is not collecting new categories of personal information from panel members? Is the panel company required to keep a running tab of what information its myriad clients are collecting from its panel members?

The reality is that many businesses, even small- and medium-sized businesses, have relationships and data sets that are often highly dynamic. They may have several agreements, pursuant to which they may share large quantities of personal information. Additionally, they may collect personal information from other businesses that are not parties to the agreements. These factors require businesses to offer individuals an accurate 12-month snapshot of what it is doing with personal information. Accordingly, the legislature should clarify that the 12-month requirement is an *annual* requirement to update its disclosures.

8. Expand the Carve-Out for "Research"

As discussed above, the Act exempts from the deletion requirement businesses 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 . . . "[218] Elsewhere in the Act, "research" is defined as "scientific, systematic study and observation, including basic research or applied

---

217. The phrase "preceding 12 months" appears a number of places in Section 1798.130, which among other things requires businesses to: "Identify by category or categories the personal information collected about the consumer in the preceding 12 months"; "[i]dentify by category or categories the personal information of the consumer that the business sold in the preceding 12 months"; and "[i]dentify by category or categories the personal information of the consumer that the business disclosed for a business purpose in the preceding 12 months." *Id.* § 1798.130(a)(3)(B), (a)(4)(B)–(C).

218. *Id.* § 1798.105(d)(6).

research that is in the public interest and that adheres to all other applicable ethics and privacy laws or studies conducted in the public interest in the area of public health."[219]

As currently drafted, this exception appears to be very narrow, applying only to non-profit or academic research. The research definition should be expanded to include for-profit research. It is not only academic researchers who deal in personal information without the end goal of direct marketing and sales to consumers.[220] For-profit market research firms also play a critical role in helping ensure healthy relationships between businesses and consumers, doctors and patients, and politicians and constituents by helping for-profit and non-profit businesses, as well as governmental entities, better understand the public.[221] This distinction between direct sales and marketing on one hand, and research—including for-profit research—on the other, is well established in the privacy context. The FTC's Telemarketing Sales Rule, for example, forbids "sales under the guise of research," or "sugging," a ban for which the market research industry actively lobbied.[222] Likewise, the FCC has for decades drawn this distinction in its TCPA rules.[223]

Furthermore, because the research carve-out only applies to the deletion requirement, it fails to adequately protect research from the burdens of the CCPA. Because the CCPA—as are a number of other internet privacy laws—is focused on more directly commercial uses of personal information, a broader exemption for research, like that in place

---

219. *Id.* § 1798.140(s).

220. The Insights Association, the largest trade association for the market research industry, binds its members to an ethics code which forbids members from advertising and direct marketing based on a respondent's participation in research. *See Insights Association Code of Standards and Ethics for Marketing Research and Data Analytics*, INSIGHTS ASS'N (May 10, 2018), https://www.insightsassociation.org/issues-policies/insights-association-code-standards-and-ethics-market-research-and-data-analytics-0 ("When engaging in non-research activities (for example, promotional or commercial activities directed at data subjects, including but not limited to advertising and direct marketing), do not permit any direct action to be taken against an individual based on his or her participation in research.").

221. *See id.*

222. Telemarketing Sales Rule, 16 C.F.R. § 310 *et seq.* *See* Diane K. Bowers, *Sugging Banned at Last*, MKTG. RESEARCH, Fall 1995, at 40 ("With support from the Direct Marketing Association and the National Association of Attorneys General, the Council for Marketing and Opinion Research (CMOR) succeeded in having an amendment approved to prevent 'sugging' (selling under the guise of research).").

223. *See, e.g.*, Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991, 7 FCC Rcd. 8752 ¶ 41 (1992) ("[T]he exemption for non-commercial calls from the prohibition on prerecorded messages to residences includes calls conducting research, [or] market surveys . . . "); Rules & Regulations Implementing the Telephone Consumer Protection Act of 1991, Report and Order, 27 FCC Rcd. 1830 ¶ 28 (2012) (explaining that "research or survey calls" made with an autodialer to residential wireline consumers do not require consent if they do not contain telemarketing messages).

in the TCPA context, would better protect the valuable role researchers play in the marketplace without hampering the law's broader objectives.

9. Streamline the Disclosure Requirements

Finally, the legislature should streamline the requirements around what must be disclosed to consumers regarding the collection, sale, and use of their personal information. As discussed above, Section 1798.130 requires businesses to disclose a host of information in its online privacy policies, including: a description of a consumer's rights; categories of personal information collected; categories of sources from which personal information has been collected; business or commercial purposes for collection or sale; categories of personal information sold or disclosed for a business purpose; the right to opt out of the sale of personal information; and the consumer's right to request deletion of personal information.[224] In addition, under Section 1798.110, businesses that collect the personal information must also disclose the specific pieces of personal information collected.[225]

There are a handful of problems with these disclosure requirements as presently drafted. First, the statute offers very limited guidance on what might constitute "categories" of personal information or sources of personal information collected[226]: information and sources of information could theoretically be grouped in any number of ways. Because the costs to businesses of comprehensive audits of their data practices for the purpose of defining these categories are likely to outweigh the benefits, the Act should instead impose a more comprehensive, general requirement that a business disclose the nature of its business as it relates to the collection of personal information.

Second, requiring businesses to disclose with any specificity the business or commercial purposes of their data collection and use practices may cross a line by requiring businesses to disclose closely held strategic information or even trade secrets. Here, too, substituting a broader requirement that businesses explain the nature of their business models in more general terms would serve the Act's purposes.

Third, instead of including an open-ended requirement that businesses disclose all the "specific pieces" of personal information collected if

---

224. CAL. CIV. CODE § 1798.130(a)(5).

225. *Id.* § 1798.110(a)(5), (c)(5).

226. The only guidance offered is found in the Act's introductory section: "Many businesses collect personal information from California consumers. They may know where a consumer lives and how many children a consumer has, how fast a consumer drives, a consumer's personality, sleep habits, biometric and health information, financial information, precise geolocation information, and social networks, to name a few categories." *Id.* § 1798.100(e), *amended by* 2018 Cal. Legis. Serv. 735 (West).

requested by an individual, the Act should set a list of pieces of information which must be disclosed. This could be accomplished efficiently by using the personal information examples included in Section 1798.140(o)(1) as a checklist. Further, the list of examples in this section could be an exclusive list, which would remove ambiguity around what specific pieces of information should be disclosed to the individual, as well as clarify the personal information definition.[227]

Finally, legislators should delete the requirement that privacy policies include a "description of a consumer's rights pursuant to Sections 1798.110, 1798.115, and 1798.125."[228] Statistics show that consumers already actually bother to read privacy policies at a dismally low rate.[229] Requiring companies to explain to consumers multiple provisions of a complex statute, in addition to disclosures that are already specific to other laws like GDPR, will only undermine the purpose of privacy policies in the first place: that users read and understand how a business is collecting, using, and sharing or selling their information.

CONCLUSION

While it has taken some time for consumers to apprehend the full scope and nature of Web 2.0, there seems to be a new appetite among consumers and legislators alike for broad, sweeping privacy legislation. Certainly, there are already a large number of privacy laws on the books, but these have largely been aimed at specific, ascertainably urgent and easier-to-understand problems such as data breach notification, protection of sensitive health and financial information, or children's privacy.[230]

In contrast with America, Europe has relied less on plaintiffs' lawyers and private attorneys general, and more on centralized regulators—most notably through GDPR, passed earlier this year.[231] Is sweeping legislation in the mold of GDPR around the corner in America?[232] Maybe, maybe

---

227. *See id.* § 1798.140(o)(1) ("Personal information includes, but is not limited to, the following . . . "). A reasonable amendment might be to delete the phrase "but is not limited to" from this section.

228. *Id.* § 1798.130(a)(5)(A).

229. *See* sources cited *supra* note 1; Florian Schaub, *Nobody Reads Privacy Policies—Here's How to Fix That*, SALON (Oct. 14, 2017), https://www.salon.com/2017/10/14/nobody-reads-privacy-policies-heres-how-to-fix-that_partner/ ("In 2008 a study estimated that it would take 244 hours a year for the typical American internet user to read the privacy policies of all websites he or she visits . . . ").

230. *See supra* Part II.

231. *See supra* Part III.

232. *See, e.g.*, Cameron F. Kerry, *Filling the Gaps in U.S. Data Privacy Laws*, BROOKINGS INST. (July 12, 2018), https://www.brookings.edu/blog/techtank/2018/07/12/filling-the-gaps-in-u-s-data-privacy-laws/ ("The Cambridge Analytica stories, the Mark Zuckerberg hearings, and

not. But if so, the CCPA will likely be at the center of this development, both as a potential model for federal legislation or copy-cat laws in other states, and even as a de facto national privacy law when it goes into effect in 2020. Broadly, the CCPA grants consumers four basic rights in connection to their personal data: (1) the right to know what personal information is collected; (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 Act.[233] These rights are largely to be enforced by the California Attorney General, with a narrow private right of action for data breaches.[234]

Although the bill will likely be amended before it goes into effect in 2020, the final law is almost certain, in light of the size and reach of the California economy, to be a game changer for U.S. privacy law. A number of amendments would make the law clearer and fairer, both to businesses and individual data subjects, including: making the private right of action more meaningful; a whistleblower provision to make take some of the enforcement burden off the attorney general; implementing a more effective cure period; clarifying the definition of "publicly available" information, the deletion requirement, the statute's interplay with federal statutes, and the 12-month notification requirement; expanding the carve-out for research; and streamlining the disclosure requirements.

---

the constant reports of major data breaches have increased interest in federal privacy legislation. Various groupings have been convening to develop proposals. The time is ripe for interests to converge on comprehensive federal privacy legislation.").

233. *Proskauer Summary*, *supra* note 17.

234. *See supra* Section IV.B.5.