

# Privacy and Data Security Litigation: 2020 Update



Copyright 2020, The Sedona Conference.  
All rights reserved.



## Working Group 11 2020 Midyear Meeting

September 30, 2020

### Privacy and Data Security Litigation: 2020 Update

Kenneth J. Withers, ed.<sup>1</sup>

While schools, businesses, courts, and government agencies operated at dramatically reduced levels or closed entirely through much of 2020, litigation and regulatory activity in world of privacy and data security did not grind entirely to a halt. There were several important developments in the United States and internationally. This memo briefly summaries some of the most important developments of the past year, some predating the pandemic, and attaches some useful client alerts or blog postings contributed by our panelists.

#### I. FTC: EQUITABLE MONETARY RELIEF

The Federal Trade Commission's jurisdiction in the data privacy and security arena is derived from Section 5 of the FTC Act,<sup>2</sup> on the theory that the failure to implement reasonable security measures to protect consumer data may constitute an unfair trade practice, if consumers were induced to do business based on false or misleading representations about privacy and security. The FTC is empowered to investigate violations of Section 5 and issue "cease and desist" orders pursuant to administrative procedure. Section 19 of the Act authorizes the FTC to seek judicial enforcement of those administrative orders, subject to a three-year statute of limitations and conduct that the FTC can demonstrate was "dishonest or fraudulent."<sup>3</sup> Section 13(b) of the Act, on the other hand, allows the FTC to go directly

---

<sup>1</sup> The Editor thanks David Cohen of Orrick Herrington & Sutcliffe, LLP; Elysia Solomon of Humana, Inc.; and Lesley Weaver of Bleichmar Fonti & Auld LLP for their contributions to this memorandum, but the opinions expressed herein are entirely those of the editor, as are any errors or omissions.

<sup>2</sup> 15 U.S.C §45.

<sup>3</sup> 15 U.S.C §57b(a)(2)

to federal court, which opens the door to the full range of judicial remedies.<sup>4</sup> One question currently before the Supreme Court is whether Section 13(b) be extended to authorize the FTC to go beyond the scope of administrative-style remedies and sue for monetary equitable relief, such as restitution or disgorgement. Two cases currently before the Supreme Court may decide that question.

The stage for this was set by a Third Circuit decision in 2019 that questioned the FTC's standing to bring an action in federal court in the absence of specific allegations that a part is "violating, or about to violate" a law within the FTC's jurisdiction. *FTC v. Shire ViroPharma, Inc.*<sup>5</sup> was an antitrust suit in which the FTC alleged that the defendant had engaged in a scheme to frustrate a rival pharmaceutical company's efforts to bring a generic version of one of its products to market. However, by the time the FTC was in federal court, the defendant had not only discontinued the specific actions that the FTC found unlawful, it had spun off the division of the company involved in that product. The Third Circuit held that the FTC had no actionable claim for either an injunction or disgorgement of alleged oil-gotten gains, as alleged misconduct had ceased and the FTC's allegations to support a claim regarding future conduct were "woefully inadequate."<sup>6</sup>

In consolidated actions, the Supreme Court will take up the question left unanswered in *Shire* of whether the FTC can seek monetary equitable relief under Section 13(b) in the first place. In *AMG Capital Management, LLC v. FTC*,<sup>7</sup> the FTC sued a payday lender for allegedly failing to provide consumers with adequate disclosures. The FTC won in district court and was awarded \$1.27 billion in equitable relief. On appeal, the Ninth Circuit upheld the award, holding that Section 13(b) carries with it the right to grant "ancillary" relief, including restitution and disgorgement.<sup>8</sup> In *FTC v. Credit Bureau Center, LLC*,<sup>9</sup> The defendant allegedly advertised "free" credit reports, without disclosing to consumers that by accepting the offer, they would be enrolled in an expensive ongoing credit monitoring service. The district court ordered the defendant to pay more than \$5 million in restitution. On appeal, the Seventh Circuit overruled its own precedent and held that Section 13(b)'s

---

<sup>4</sup> 15 U.S.C. §53.

<sup>5</sup> 917 F. 3d. 147 (3d Cir. 2019).

<sup>6</sup> *Id.* at 160.

<sup>7</sup> 910 F. 3d 417 (9<sup>th</sup> Cir. 2018); *cert granted*, \_\_\_ S. Ct. \_\_\_, 2020 WL 3856250 (U.S. July 9, 2020).

<sup>8</sup> *Id.* at 426.

<sup>9</sup> 937 F. 3d 764 (7<sup>th</sup> Cir. 2019); *cert. granted*, \_\_\_ S. Ct. \_\_\_, 2020 WL 3865251 (U.S. July 9, 2020).

“grant of authority to order injunctive relief does not implicitly authorize an award of restitution.”<sup>10</sup>

## II. FTC CONSENT DECREES

In 2018, the FTC was handed a defeat by the Eleventh Circuit when it ruled that a consent decree it obtained in a high-profile data privacy and security case was void for vagueness. *LabMD Inc. v. FTC*<sup>11</sup> was particularly significant, as it was the first time an FTC data security order had been litigated. The case originated when the FTC brought an enforcement action against a medical testing lab, alleging that the lab engaged in unfair trade practices by failing to implement measures necessary to establish “reasonable security” over patient data. An FTC administrative law judge dismissed the action on the grounds that the FTC failed to establish that LabMD’s conduct caused or was likely to cause substantial harm. The full commission reversed and issued an order requiring that LabMD implement “reasonable security.” On appeal, the Eleventh Circuit vacated the FTC’s order that it failed to provide LabMD with fair notice of what conduct was prohibited or required, and that enforcement of the order would place the court in the impermissible role of managing the business in behalf of the FTC.<sup>12</sup>

In the wake of LabMD, the FTC has revised the language in standard consent decrees. The current language no longer refers to a “reasonable security program,” but instead lists a panoply of specific data privacy and security measures, including yearly employee training, access controls, monitoring systems, patch management systems, encryption, a documented assessment program, periodic reports to the company’s board, and an annual certification of compliance to the FTC. However, commentators have noted that these measures, which vary from decree to decree, are themselves vague, and more importantly, do not represent an “safe harbor” for compliance. They are considered “necessary but not necessarily sufficient.”<sup>13</sup>

As counter intuitive as it may seem, it appears that companies that actually litigate FTC enforcement actions in court fare better in this regard than those who accept the standard consent orders. In two actions, one recent and one pre-dating *LabMD*, litigants were able to get more specific and narrowly drafted orders. In particular, these stipulated orders provide that if the company obtains an assessment

---

<sup>10</sup> *Id.* at 767.

<sup>11</sup> 894 F.3d 1221 (11<sup>th</sup> Cir. 2018).

<sup>12</sup> *Id.* at 1235-37.

<sup>13</sup> *See generally*, Douglas Meal, et al., “FTC Data Security Consent Orders Are New But Not Improved,” attached as Appendix D.

certifying its compliance with a specified security standard, it will be deemed compliant with the order's requirements.<sup>14</sup>

### III. CALIFORNIA CONSUMER PROTECTION ACT

Enforcement of California's sprawling Consumer Protection Act<sup>15</sup> commenced on July 1 of this year, although the Attorney General's Office didn't finalize the CCPA regulations until August 14.<sup>16</sup> Under the CCPA, the Attorney General has the power to fine violators \$2,500 per violation not cured within 30 days of notice, to fine violators \$7,500 per violation if the acts are found to be "intentional," and to obtain injunctive relief. As of the writing of this memorandum, the Attorney General has filed no actions under CCPA, but was reported to have sent approximately 30 initial compliance demand letters on or about July 1. These have focused on businesses that were found to have inadequate privacy disclosures of "Do Not Sell" links on their web sites—violations which may be easily cured, thus avoiding litigation.

However, California has a private right of action under Cal. Civ. Code §1798.81.5, predating the CCPA, for failure to maintain "reasonable security" resulting in actual damages. And effective as of January 1 of this year, the CCPA created a new private right of action, Cal. Civ. Code §1798.150, with statutory damages for consumers whose nonencrypted or nonredacted personal information is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of a business's violation of the duty to implement and maintain reasonable security practices and procedures. It is important to note that the definition of "personal information" in this provision was taken from California's existing data security law, not the broader definition found in the CCPA. "Personal information" is defined as an individual's name in combination with one or more of the following, in nonencrypted or nonredacted form:

- Social Security number
- Driver's license or California identification card number
- Financial account number in combination with access code or password
- Medical information
- Health insurance information

---

<sup>14</sup> Proposed Stipulated Order, Fed. Trade Comm'n v. D-Link Sys., Inc., No. 3:17-CV-00039-JD, ECF No. 272-1, at 9-10 (N.D. Cal. Jul. 2, 2019); Stipulated Order, Fed. Trade Comm'n v. Wyndham Worldwide Corp. *et al.*, No. 2:13-cv-01887, ECF No. 283, at 8-9 (D. N.J. Dec. 11, 2015).

<sup>15</sup> Title 1.81.5. California Consumer Privacy Act of 2018 [1798.100 - 1798.199]. Full text provided as Appendix E.

<sup>16</sup> Full text provided as Appendix F.

As of the writing of this memorandum, over 60 actions have been filed related to CCPA. Most of these have been filed in federal court, and not all expressly invoke CCPA. None have progressed to judgment, although there have been some early settlements, as in *Barnes v. Hanna Andersson & Salesforce*,<sup>17</sup>

Many of these actions challenging data collection practices are based on California's Unfair Competition Law (UCL), Bus. & Profs. Code §17200, which provides for a broader private right of action. Examples include *Cullen v. Zoom Video Commc'ns Inc.*<sup>18</sup> and the high-profile *In re Plaid Inc. Privacy Litigation*.<sup>19</sup> These have been characterized by some commentators as attempts to “bootstrap” CCPA into the UCL.<sup>20</sup> Actions that expressly invoke CCPA raise a number of questions that have yet to be resolved, including

- Does the private right of action apply to non-California residents?
- Does it apply retroactively, to incidents before January 1, 2020?
- Is the information in question “personal information” for purposes of the private right of action?<sup>21</sup>

One significant question, raised by *Anurag Gupta, et al., v. Aeries Software, Inc.*,<sup>22</sup> and *Karter v. Epiq Systems*,<sup>23</sup> is whether the defendant is a “business,” subject to the private right of action, or a “service provider,” which would not be.

Another significant question is the efficacy of mandatory arbitration clauses or class action waivers in consumer contracts. CCPA expressly prohibits invocation of these as defenses. Cal. Civ. Code §1798.192 states, “Any provision of a contract or agreement ... that purports to waive or limit in any way a consumer’s ... right to a remedy or means of enforcement, shall be contrary to public policy ... and unenforceable.” This has not stopped litigants from arguing that Federal Arbitration Act<sup>24</sup> preempts any such provision in state law.<sup>25</sup>

---

<sup>17</sup> No. 3:20-cv-00812-EMC (N.D. Cal.).

<sup>18</sup> No. 5:20-cv-02155-SVK (N.D. Cal.).

<sup>19</sup> No. 4:20-cv-03056-DMR (N.D. Cal.).

<sup>20</sup> Ropes & Gray, “California Privacy Update: Litigation Under the CCPA,” Webinar, Sept. 22, 2020. The editor acknowledges the producers of this webinar for providing considerable useful intelligence which he has shamelessly plagiarized to populate this section, but any errors or omissions are solely the responsibility of the editor.

<sup>21</sup> *See, e.g.*, *Rahman v. Marriott Int’l, Inc.*, No. 8:20-cv-00654 (C.D. Cal.).

<sup>22</sup> No. 8:20-cv-00995-FMO-ADS (C.D. Cal.).

<sup>23</sup> No. 8:20-cv-1385 (C.D. Cal.).

<sup>24</sup> 9 U.S.C. §2

<sup>25</sup> *See, e.g.*, *Fuentes v. Sunshine Behavioral Health Group, LLC*, No. 8:20-cv-00487 (C.D. Cal.); *Atkinson v. Minted, Inc.*, No. 3:20-cv-03869 (N.D. Cal.).

#### IV. CALIFORNIA PRIVACY RIGHTS ACT

Before the ink was dry on the on the regulations to enforce the CCPA, privacy advocates had already collected the necessary number of signatures to place an even more expansive data privacy and security law on the ballot for the November 3, 2020 election. California Proposition 24,<sup>26</sup> the proposed California Privacy Rights Act (CPRA), would augment the CCPA in several ways. First, it would expand the private right of action to be available for breaches involving email addresses and passwords and eliminate the 30-day period to “cure” a data breach. It would add additional protections for “sensitive data” and require deletion of data that is no longer necessary for the purpose for which it was collected. Data collection and processing would need to be justified in terms of necessity and proportionality, much like the requirements of the GDPR, and would provide consumers the right to opt out of “sharing” of personal information, not just “sale.” And perhaps most significantly, the CPRA would to establish a California Privacy Protection Agency (CPPA), which would be the first dedicated privacy agency in the U.S.

Californians for Consumer Privacy, which is backing Proposition 24, claims that polling shows the CPRA enjoying 81% of voter approval in polls.<sup>27</sup> However, the CPRA has received its share of criticism from consumer advocates, who point to the “opt out” provisions as placing the burden on consumer to protect their own privacy, and for allowing business to offer financial incentives to consumers who waive the data sale or sharing restrictions.<sup>28</sup>

#### V. PRIVILEGE PROTECTION FOR EXPERT REPORTS AND FINDINGS

In November of 2019, Working Group 11 published its *Commentary on Application of Attorney-Client Privilege and Work-Product Protection to Documents*

---

<sup>26</sup> Full text provided as Appendix G.

<sup>27</sup> Californians for Consumer Privacy, “New Poll From Goodwin/Simon Research Shows Prop 24, The California Privacy Rights Act, Receives 81% Support From Voters,” Aug. 3, 2020, <https://www.caprivacy.org/new-poll-from-goodwin-simon-research-shows-prop-24-the-california-privacy-rights-act-receives-81-support-from-voters/>.

<sup>28</sup> Angelica Cabral, “Prop 24 seemingly seeks to expand internet privacy, critics say it won’t,” The Californian, September 8, 2020, <https://www.thecalifornian.com/story/news/2020/09/08/proposition-24-centers-internet-privacy/5739293002/>.

*and Communications Generated in the Cybersecurity Context*,<sup>29</sup> in which it advocated for a qualified privilege, protecting from disclosure the reports of forensic investigators, called in by companies and their law firms to investigate, evaluate, and make response recommendations in the wake of data privacy and security incidents. However, this is not a settled area of the law. Three recent cases illustrate the issues and come to different conclusions. Coincidentally, in all three cases, the companies involved engaged the Mandiant Services division of security technology company Firefly, Inc. to provide forensic assistance to prepare for and respond to litigation as a result of a significant breach.

In the *Dominion Dental Services* case<sup>30</sup>, arising out of the discovery of a nearly decade-long pattern of unauthorized access to patient financial and medical information, the court concluded that Mandiant was retained before the breach was discovered and well before litigation stemming from that breach could have been anticipated, and that the report was used for non-litigation purposes. The fact that a separate retention agreement was executed once litigation was reasonably anticipated that expressly incorporated counsel in the direction of the work was not controlling, and the subsequent agreement was identical in nearly every other respect with the prior agreement.

Similarly, in *Capital One*,<sup>31</sup> a case in which a putative class of consumers allege various claims against Capital One arising out of the data security incident Capital One suffered in 2019, the magistrate judge ordered Capital One to produce to plaintiffs a report of the incident that Mandiant prepared. The magistrate judge found that Capital One had retained Mandiant well in advance of the data incident in question, had been paid out of the business operations budget (and not “legal”), and that Mandiant’s report had been provided to third parties for purposes unrelated to the litigation. However, in later proceedings, the same magistrate judge denied a motion to compel production of a report generated by PricewaterhouseCoopers.<sup>32</sup> The judge’s order provides no details or analysis, but a transcript of the hearing, which may provide greater insight, is available.<sup>33</sup>

---

<sup>29</sup> 21 SEDONA CONF. J. 1 (2020), available for free download at <https://thesedonaconference.org/download-publication?fid=5375>.

<sup>30</sup> In Re: Dominion Dental Servs. USA, Inc. Data Breach Litig., 2019 WL 7592343 (E.D. Va. Dec. 19, 2019)

<sup>31</sup> In Re: Capital One Consumer Data Security Breach Litig., No. 1:19-md-02915, 2020 WL 2731238 (E.D. Va. May 26, 2020); *aff’d*, 2020 WL 3470261 (E.D. Va. June 25, 2020)

<sup>32</sup> In Re: Capital One Consumer Data Security Breach Litig., No. 1:19-md-02915, 2020 WL 5016930 (E.D. Va. Aug. 21, 2020)

<sup>33</sup> <https://www.johnreedstark.com/wp-content/uploads/sites/180/2020/09/TranscriptCapOne-82120-Anderson.pdf>.

These holding run counter to the holding in *Experian*,<sup>34</sup> in which the forensic report and findings were protected from disclosure as work product. But as noted by the court in *Dominion Dental Services*, the *Experian* court found that while the defendant had worked with Mandiant in the past, there was no continuous business relationship, distribution of the report was tightly limited to the litigation team, and no effort was made to use the report to assure regulators, customers, and the general public that the defendant had the incident under control.

Based on these cases, some recommended best practices emerge for establishing and maintaining work product protection and attorney-client communication privilege when directing forensic experts to investigate data incidents in preparation for, or in response to, anticipated or pending litigation:

- (1) Keep terms and deliverables in the Statement of Work (“SOW”) for a privileged engagement distinct from prior generic SOWs for general business and non-litigation purposes.
- (2) Consider who signs the SOW and how invoices are paid. SOWs signed for by legal counsel for the company (either outside or in-house) and invoices paid through the company’s legal department (directly or indirectly through outside counsel bills) could have stronger claims to privilege.
- (3) Spell out in the SOW that support for litigation defense is the primary purpose of the engagement.
- (4) Ensure that counsel for the company are the sole directors of the terms and deliverables of the forensic team’s work under the privileged engagement.
- (5) Carefully consider and direct who outside of the legal team the third-party forensic team briefs and who receives the reports and findings.
- (6) Limit the use of the findings and reports to litigation defense support and not for other purposes, e.g., regulatory reporting and accounting.

## VI. THE SCHREMS LITIGATION

Austrian privacy campaigner Max Schrems has been engaged in protracted litigation against Facebook for several years, resulting in an array of European court

---

<sup>34</sup> In re *Experian Data Breach Litig.*, SACV 15-01592 AG, 2017 WL 4325583 (C.D. Cal. May 18, 2017).

and regulatory decisions that have had significant impact on the cross-border transfer of personal data, particularly between EU members countries and the United States. And every decision rendered in the ongoing litigation seems to raise more questions than it answers. The landmark *Schrems II* decision<sup>35</sup> rendered by the Court of Justice of the European Union (CJEU) in July is no exception.

Max Schrems was a law student attending the University of Santa Clara on an exchange program when he was apparently taken aback by a presentation by a Facebook data privacy lawyer. Upon his return to Austria, he began compiling a long list of data privacy grievances against Facebook and launched a website, <http://europe-v-facebook.org>. He launched a class action challenging Facebook's invocation of the "Safe Harbor" framework to justify the routine transfer of data from Facebook's European customers to its servers in the United States, as the United States was not then – nor is it now – recognized by the European Union as having "adequate" privacy laws and regulations to guarantee European citizens relatively equivalent rights regarding the collection and processing of their personal data as they have in the EU. Facebook's European operations are based in Ireland, so the Irish data protection authority and Irish courts have been enmeshed in this complex set of actions, as well as European agencies and courts.

In 2015, Schrems won a landmark ruling in the CJEU (*Schrems I*) which invalidated Safe Harbor on the basis that U.S.-based business entities importing personal data from the EU could not guarantee that the data, once in the U.S., would not be subject to surveillance and collection by U.S. law enforcement and national security agencies, and European citizens had no avenues for legal redress of privacy grievances in U.S. courts.<sup>36</sup> This resulted in the scrapping of Safe Harbor and its replace by a supposedly more stringent framework, Privacy Shield. However, the underlying objections to cross-border data transfers to the U.S. (and presumably other countries that fail to obtain "adequacy" determinations by the EU) noted by the court in *Schrems I* remained, and soon the Irish authorities were facing another round of complaints against Facebook. The Irish court applied to the CJEU for a determination of its powers to review (and possibly invalidate) transfers under Privacy Shield and another transfer mechanism, Standard Contractual Clauses. In *Schrems II*, the court held despite the fact that Privacy Shield and Standard Contractual Clauses had been negotiated by the European Commission and were

---

<sup>35</sup> Data Protection Comm'r v. Facebook Ireland, Ltd. and Schrems, No. C-311/18 (CJEU July 16, 2020).

<sup>36</sup> Schrems v. Data Protection Comm'r, No. C-362/14 (CJEU Oct. 6, 2015).

enforceable EU-wide, members-state data protection authorities and courts were still empowered to investigate and determine whether business entities were abiding by the terms of these arrangements, or could effectively guarantee the data protections promised. Privacy Shield was declared to be invalid, and transfers under Standard Contractual Clauses were now open to case-by-case examination by the appropriate national data protection authorities, making them significantly less certain.

While the CJEU remanded the case back to the Irish courts for further proceedings in light of its determination that the national courts had jurisdiction, the Irish Data Protection Commissioner has opened a new independent investigation of Facebook, as the General Data Protection Regulation (GDPR) now governs. This opens Facebook up to the full panoply of potential remedies under GDPR, while the Irish courts are procedurally limited in the remedies they can order.

There has been some argument about the impact and scope of *Schrems II*. On the one hand, it leaves businesses scrambling to find an alternative to Privacy Shield, although the U.S. Department of Commerce continues to administer the program, including accepting applications for self-certification and re-certification. Standard Contractual Clauses remain on the books and have been incorporated into countless contracts that are supposedly still enforceable. The European Commission was already looking into updating the approved clause language but is several years away from approving new clauses. And there is a view that the practical impact of *Schrems II* is limited to the sort of ongoing bulk transfers of data that would get the attention of U.S. law enforcement and national security agencies, not ordinary business-related data traffic. On the other hand, *Schrems* and other European privacy advocates have formed a new organization, “noyb,” which stands for None of Your Business. On the heels of the *Schrems II* decision, noyb has filed complaints in all 30 EU and EEA member states against more than 100 businesses whose web sites routinely share visitor data with Google or Facebook.<sup>37</sup>

## VII. TIKTOK, WECHAT, AND THE GLOBAL MOVEMENT TOWARDS DATA LOCALIZATION

TikTok is a social media platform currently downloaded more often than Facebook. ByteDance, its Chinese-based parent company, is the world’s most

---

<sup>37</sup> See generally, Electronic Privacy Information Center, “Max Schrems v. Data Protection Commissioner (CJEU - Safe Harbor)”, <https://epic.org/privacy/intl/schrems/>.

valuable unlisted technology startup, at between approximately \$100 billion. It has become wildly popular with teenagers, especially during the pandemic, when young people are hungry for social interaction. TikTok users are presented with an endless stream of one-minute videos uploaded by other users. They can indicate their interest or with a swipe skip videos they are not interested in watching. Each time they do so, the app's algorithm adapts what is served up next. Reactions, challenges, and contests generate collaboration and almost addictive engagement. In the process, TikTok collects data and builds a highly detailed and nuanced profile of each user.

WeChat is another wildly popular app, especially in China and other Asia Pacific markets. WeChat is more than an app. It is an entire online environment, supplanting email, text messaging, business applications, banking and retail digital payment systems, ride-hailing services, food delivery services, travel agencies – all within the WeChat “universe.” Chinese businesspeople and students overseas, and extended Chinese families across the globe, rely on WeChat to stay connected to home. WeChat has an estimated 700 million users and is owned by TenCent, the Chinese gaming and social media giant. It is estimated that WeChat, as a division of TenCent, has a market worth of over \$80 billion.

While the activities of TikTok and WeChat might legitimately raise concerns about data privacy under any circumstances, the fact that these two mega-apps are owned by Chinese companies and hosted on Chinese servers has grabbed the attention of U.S. national security agencies, Congress, and the White House. The concerns are less about consumer data privacy – there are no reports of significant data breaches involving either TikTok or WeChat – than about national security. China has data protection laws that are similar to those in other industrialized countries<sup>38</sup> and in August of this year introduced more comprehensive draft legislation, which is expected to be finalized and go into effect next year. But the Peoples Republic of China is increasingly considered a “surveillance state,” as state agencies have virtual carte blanche to monitor digital traffic, and Chinese authorities routinely censor offending content, flood the app with pro-government content, and

---

<sup>38</sup> Article 111 of General Provisions of the Civil Law of the People's Republic of China sets out the basic principle that natural persons' personal data shall be protected by law; any organization or individual must collect personal data after obtaining the data subject's consent and conduct the collection according to the law and they shall ensure the security of the personal data collected. Illegal collection, use, processing, or transmission of others' personal data, illegal sale or purchase of personal data, or illegal disclosure of personal data are all prohibited. The Cybersecurity Law sets out the legal principles and high-level requirements on protection of personal data collected or processed via networks. Certain provisions are similar to GDPR.

monitor the activities of dissidents. WeChat users are sensitive to this and modify their online behavior accordingly.<sup>39</sup>

This summer, U.S. officials took the extraordinary step, citing national security concerns, or attempting to shut down TikTok and WeChat in the United States, or force sales of the apps to U.S.-based buyers. Effective September 20, the Department of Commerce prohibited a broad range of “transactions” involving the two apps. In a statement issued on September 18, the Department announced:

As of September 20, 2020, the following transactions are prohibited:

1. Any provision of service to distribute or maintain the **WeChat** or **TikTok** mobile applications, constituent code, or application updates through an online mobile application store in the U.S.;
2. Any provision of services through the **WeChat** mobile application for the purpose of transferring funds or processing payments within the U.S.

As of September 20, 2020, for WeChat and as of November 12, 2020, for TikTok, the following transactions are prohibited:

1. Any provision of internet hosting services enabling the functioning or optimization of the mobile application in the U.S.;
2. Any provision of content delivery network services enabling the functioning or optimization of the mobile application in the U.S.;
3. Any provision directly contracted or arranged internet transit or peering services enabling the function or optimization of the mobile application within the U.S.;
4. Any utilization of the mobile application’s constituent code, functions, or services in the functioning of software or services developed and/or accessible within the U.S.

Any other prohibitive transaction relating to WeChat or TikTok may be identified at a future date. Should the U.S. Government determine that WeChat’s or TikTok’s illicit behavior is being replicated by another app

---

<sup>39</sup> The Economist, “Donald Trump has caused panic among millions of WeChat users,” August 13, 2020, <https://www.economist.com/china/2020/08/13/donald-trump-has-caused-panic-among-millions-of-wechat-users>.

somehow outside the scope of these executive orders, the President has the authority to consider whether additional orders may be appropriate to address such activities.

The announcement goes on to state that “the President has provided until November 12 for the national security concerns posed by TikTok to be resolved. If they are, the prohibitions in this order may be lifted.” Note that WeChat has not been given such consideration.

This announcement resulted in the immediate deletion of TikTok and WeChat from Apple and Google application catalogues, although it did not disrupt operations for those who already had the app on their devices. U.S.-based companies that do extensive online marketing through WeChat were left scrambling to understand what was meant by “transactions.”

As a practical matter, the announcement and the negotiations leading up to it are forcing ByteDance and TenCent to divest themselves of their U.S. operations. As of this writing, Microsoft, Oracle, and Walmart have all been mentioned as potential buyers for TikTok. Neither Facebook nor Google have expressed interest in buying WeChat, as it can be viewed as a competitor, and if either U.S. entity made a bid, it would raise serious antitrust concerns.

The forced departure of TikTok and WeChat from the American market is part of a larger global trend of “data localization,” whereby national governments require that citizens’ data be held only on domestic servers and cross-border data transfers are strictly regulated or prohibited outright. While the protection of personal data is used as the justification for data localization, the more significant drivers are national security interests. Ironically, under China’s Cybersecurity law, article 37 requires IT infrastructure operators to store all personal information they collect from users (sales, marketing, accounting, etc.) within mainland.<sup>40</sup> Russia recently introduced administrative fines for violation of its 2015 data localization law, ranging from 2 to 18 million rubles (approximately \$30,000 - \$280,000).<sup>41</sup> But this is a global phenomenon, raising questions about the future of global digital commerce and communication, international comity and cooperation, and whether individual actually “own” their own data.

---

<sup>40</sup> Yuxi Wei, “Chinese Data Localization Law: Comprehensive but Ambiguous,” Univ. of Washington Jackson School of Int. Studies, Feb. 7, 2018, <https://jsis.washington.edu/news/chinese-data-localization-law-comprehensive-ambiguous/>.

<sup>41</sup> Xenia Melkova, Alla Naglis, Data Localization in Russia: Now Backed with Big Fines, JDSupra, June 21, 2019, <https://www.jdsupra.com/legalnews/data-localization-in-russia-now-backed-18981/>.

Appendices

Appendix A

Aravind Swaminathan, et al., “Third Circuit Shire Decision May Spell Trouble for FTC Cybersecurity Enforcement Plans” (Mar. 13, 2019).  
Reprinted with permission of the authors.

Appendix B

Jonathan Drenfeld and David Cohen, “Pending U.S. Supreme Court Cases May Restrict FTC’s Pursuit of Monetary Relief in Privacy and Cybersecurity Matters” (July 24, 2020). Reprinted with permission of the authors.

Appendix C

Jonathan Drenfeld, et al., “Recent FTC Cybersecurity Settlements Highlight Benefits and Risks of Settling vs. Litigating” (Aug. 21, 2019). Reprinted with permission of the authors.

Appendix D

Doug Meal, et al., “FTC Data Security Consent Orders Are New But Not Improved” (Mar. 23, 2020). Reprinted with permission of the authors.

Appendix E

California Civil Code, TITLE 1.81.5. California Consumer Privacy Act of 2018 (current as of Sept. 25, 2020)

Appendix F

California Office of the Attorney General, CHAPTER 20. CALIFORNIA CONSUMER PRIVACY ACT REGULATIONS (Aug. 14, 2020)

Appendix G

Alastair Mactaggart, Submission of Amendments to The California Privacy Rights and Enforcement Act of 2020, Version 3, No. 19-0021, and Request to Prepare Circulating Title and Summary (Amendment) (Docketed Nov. 13, 2019)

Appendix H

Colleen Theresa Brown, et al., The Return of the Mac: “CCPA 2.0 Qualifies for California’s November 2020 Ballot and Could Usher In Sweeping Changes to CCPA” (June 26, 2020). (Reprinted with permission of the publisher)

Appendix I

In Re: Capital One Consumer Data Security Breach Litigation, MDL No. 1:19md2915 (AJT/JFA) (E.D. Va. June 25, 2020) (Memorandum Opinion and Order)

## Appendix A

Aravind Swaminathan, et al.

“Third Circuit Shire Decision May Spell Trouble for FTC Cybersecurity Enforcement Plans” (Mar. 13, 2019).

Reprinted with permission of the authors.



# Trust Anchor

## Third Circuit *Shire* Decision May Spell Trouble for FTC Cybersecurity Enforcement Plans

Aravind Swaminathan (<https://blogs.orrick.com/trustanchor/author/aswaminathan/>), Jonathan Direnfeld (<https://blogs.orrick.com/trustanchor/author/jdirenfeld/>) and David Cohen (<https://blogs.orrick.com/trustanchor/author/davidcohen/>)



In June 2018, medical laboratory LabMD obtained the first-ever court decision overturning a Federal Trade Commission (FTC) cybersecurity enforcement action. (The team directing that effort – led by Doug Meal and Michelle Visser – **joined** (<https://www.orrick.com/News/2019/01/Orrick-Assembles-Premier-Cyber-and-Privacy-Team-and-Launches-Boston-Office>) Orrick in January 2019). There, the Eleventh Circuit **held** (<https://assets.documentcloud.org/documents/4496096/labMD-ca11-20180606.pdf>) that an FTC cease-and-desist order imposing injunctive relief requiring LabMD to implement “reasonable” data security was impermissibly vague. In the wake of *LabMD*, the FTC’s new Chairman,

Joseph Simons, **stated** (<https://www.law.com/nationallawjournal/2018/06/20/ftcs-limited-data-privacy-power-makes-chair-joe-simons-nervous/>) that he was “very nervous” that the agency lacked the remedial authority it needed to deter allegedly insufficient data security practices and that, among other things, the FTC was exploring whether it has additional untapped authority it could use in this space. In this regard, Chairman Simons and Commissioner Rebecca Kelly Slaughter **announced**

([https://www.ftc.gov/system/files/documents/public\\_statements/1407368/182\\_3038\\_nectar\\_sandpiper\\_patriot\\_rks\\_and\\_jjs\\_concurring\\_statement\\_0.pdf](https://www.ftc.gov/system/files/documents/public_statements/1407368/182_3038_nectar_sandpiper_patriot_rks_and_jjs_concurring_statement_0.pdf)) that the FTC is examining whether it can “further maximize its enforcement reach, in all areas, through strategic use of additional remedies” such as “monetary relief.”

But on February 25, 2019, the Third Circuit issued a **decision** (<https://www2.ca3.uscourts.gov/opinarch/181807p.pdf>) in *FTC v. Shire Viropharma, Inc.* that may make it extremely difficult for the FTC to obtain such “monetary relief” in most privacy and cybersecurity actions. In *Shire*, the court held that to pursue relief in federal court under Section 13(b) of the FTC Act, the FTC must allege facts plausibly suggesting that the company “is violating, or is about to violate,” the law – not merely that the company violated the law in the past, and not merely that the company is “likely” to violate the law in the future. Although *Shire* was an antitrust case that proceeded under Section 13(b), that same section of the FTC Act is the principal authority on which the FTC relies to pursue monetary relief in consumer protection actions, including privacy and cybersecurity enforcement actions. The FTC is likely to face hurdles in demonstrating that, in the ordinary privacy and cybersecurity action, a company “is violating, or is about to violate,” laws enforced by the FTC.

### Background on the FTC’s Enforcement Powers

The FTC can initiate an enforcement action if it has “reason to believe” that Section 5 of the FTC Act, which prohibits unfair competition and unfair or deceptive trade practices, is being violated. The FTC takes the position that a failure to implement “reasonable” cybersecurity or privacy practices can constitute an “unfair” practice, and that making false or misleading statements about such practices can be a “deceptive” trade practice under the statute.

Prior to the enactment of Section 13(b) in 1973, the FTC relied on its traditional administrative enforcement authority, which allowed the FTC to initiate an administrative proceeding to issue an order to “cease and desist” violations of Section 5 but did not permit imposition of financial relief. Section 19 of the FTC Act permits the FTC to pursue a federal court action to obtain equitable money relief for violations of these administrative cease-and-desist orders, but only when a “reasonable man would have known under the circumstances” that the conduct was “dishonest or fraudulent,” and these actions are subject to a three-year statute of limitations. Section 19 also permits actions for equitable money relief in federal court when a company has violated a specific FTC rule, again subject to the three-year limitation period. Most privacy and cybersecurity cases, however, do not involve violations of cease-and-desist orders or FTC rules.

With the addition of Section 13(b), the FTC Act gave the FTC the authority to proceed against a company directly to federal court in certain circumstances, even before any administrative adjudication has occurred, and even in the absence of any rule violation. Specifically, under Section 13(b) the FTC gained the authority to (1) seek injunctive relief in federal court pending the completion of the FTC administrative proceeding when the FTC “has reason to believe” that a person or entity “is violating, or is about to violate” any law enforced by the FTC, and (2) seek a permanent injunction “in proper cases.” Subsequently, the FTC adopted an expansive view of its power to bring federal court enforcement actions under Section 13(b), and started bringing cases in federal court seeking monetary relief under equitable doctrines such as restitution, disgorgement and rescission of contracts. The FTC also asserted that its statutory power to seek a “permanent injunction” was a standalone grant of authority that entitled the FTC to bring a federal court action irrespective of whether a defendant “is violating, or is about to violate” the law. By tying its theories to these equitable doctrines, the FTC took much of its enforcement activity outside otherwise severe limitations on its ability to seek money relief. Until recently, courts universally accepted the FTC’s expansive view of its authority under Section 13(b). As a result, it is the FTC’s **policy** (<https://www.ftc.gov/about-ftc/what-we-do/enforcement-authority>) that “[a] suit under Section 13(b) is preferable to the adjudicatory process because, in such a suit, the court may award both prohibitory and monetary equitable relief in one step.”

### ***FTC v. Shire ViroPharma, Inc.***

The Third Circuit’s decision in *Shire ViroPharma*, however, delivers a stinging rebuke to the FTC’s “preferable” approach. The FTC sued the defendant in the U.S. District Court for the District of Delaware, alleging that between 2006 and 2012 Shire had engaged in an anticompetitive campaign of repetitive and meritless filings with the FDA to delay generic competition and therefore maintain its monopoly on its branded drug. Shire moved to dismiss the FTC’s complaint, arguing that the FTC had exceeded its authority under Section 13(b). Specifically, Shire asserted that Section 13(b) does not provide the FTC with independent authority to seek a permanent injunction and money relief under Section 13(b), but rather limits the actions to those cases where the FTC can plead that a defendant “is violating or is about to violate” the law. On March 20, 2018, Judge Richard Andrews granted Shire’s motion to dismiss, and rejected the FTC’s long-held assertion that Section 13(b) provides it with the independent authority to seek permanent injunctive and monetary relief in federal court for past violations of the FTC Act and regulations.

The Third Circuit affirmed last month, **holding** (<https://www2.ca3.uscourts.gov/opinarch/181807p.pdf>) that “Section 13(b) requires that the FTC have reason to believe a wrongdoer ‘is violating’ or ‘is about to violate’ the law.” It found that the plain language of Section 13(b) does not permit the FTC to pursue conduct that merely occurred in the past; rather, it

allows the FTC to pursue only “existing or impending conduct.” The court explained that this reading is bolstered by the history of Section 13(b), which Congress “expected to be used for obtaining injunctions against illegal conduct pending completion of FTC administrative hearings.” And, the court rejected the FTC’s assertion that it can plead a company is “about to violate” the law by demonstrating a mere “reasonable likelihood” that its past violations will recur. Rather, “‘is violating’ or ‘is about to violate’ means what it says – the FTC must make a showing that a defendant is violating or is about to violate the law.” And because “Shire indisputably is not currently violating the law, nor is it alleged to be poised to do so anytime in the foreseeable future,” the FTC’s complaint “fail[ed] to state a claim upon which relief can be granted.” The court thus affirmed the dismissal of the FTC’s claims for both permanent injunctive and monetary relief.

### **What to Do Now – Taking Advantage of *Shire***

Companies can take advantage of the Third Circuit’s decision in *Shire* and potentially cut off the FTC’s ability to obtain monetary relief for privacy and cybersecurity breaches by taking some basic steps. Because *Shire* limits damages to prospective violations, the key is to take immediate steps to identify, remediate and validate any security vulnerabilities to ensure that the company can demonstrate that it is no longer “about to” violate the law. Here is what to consider doing and including in your incident response plan:

- Ensuring that a “root cause analysis” is a key part of incident response and investigation, where focus is placed on the “whats,” “hows” and “whys” that lead to the incident;
- Developing a comprehensive understanding of the remediation measures that are necessary and appropriate to prevent the incident from recurring, which typically means identifying security vulnerabilities, missing patches, changes to data collection, use, sharing practices, etc. For security breaches, the forensics team can play a significant part in helping determine remediation activities.
- Working with senior management to allocate the resources (both people-power and monetary) that will be needed to fully implement remediation measures, and developing a timetable for remediation efforts;
- Implementing all agreed-upon remediation measures, whether policy-based, technical or physical, and validating that they are functioning correctly by conducting post-remediation testing (giving due consideration to testing that is broader than just the root-cause, to manage related risks);
- Conducting regular assessments against affected systems and processes, generally, and remediating accordingly (with accompanied validation); and
- Documenting the above, to maintain an accurate record of investigation, remediation, assessment and validation activities to be used with regulators and/or putative plaintiffs

### **FTC’s Response to *Shire***

While *Shire* may impose significant hurdles to the FTC’s ability to pursue federal court actions, the FTC may have other options. For example, the FTC may take the position that it is nevertheless permitted to utilize Section 19 of the FTC Act to obtain monetary relief in federal court following the issuance of an administrative cease and desist order for a first-time violation of Section 5. But even if that position were correct, any such monetary relief would be subject to a three-year statute of limitations and limited to conduct that was “dishonest or fraudulent.”

The FTC may also consider leveraging its administrative adjudication process, which is notoriously slow and burdensome and over which the FTC Commissioners exercise the final decision-making authority (subject to judicial review), to force companies to agree to unfavorable settlement agreements. In particular, the FTC may seek to have companies enter into 20-year administrative consent orders with broader conduct provisions regulating future

privacy and cybersecurity actions. While FTC administrative consent orders do not usually contain monetary penalties, they carry the potential for fines of \$42,530 per violation (which the FTC may contend applies to each consumer subject to a breach) that occurs at any point over the 20-year term of the order.

No doubt, Chairman Joseph Simons, with his deep background in antitrust regulation, watched these developments closely. It might be why he recently **urged** (<https://www.nytimes.com/2019/03/08/technology/ftc-facebook-joseph-simons.html>) Congress to expand the FTC's privacy-enforcement powers and allow it to impose fines more easily, write new rules and hire more experts. "It's important that we get civil penalty authority," he said. "For companies that have lots of money, the impact would be sufficient to deter them." Championing the role of the FTC as the police for how all companies and nonprofits – not just technology companies – collect and handle people's digital data, Chairman Simons has made clear that this chapter is not yet closed.

◀ 3

## Appendix B

Jonathan Drenfeld and David Cohen

“Pending U.S. Supreme Court Cases May Restrict FTC’s Pursuit of Monetary Relief in Privacy and Cybersecurity Matters” (July 24, 2020)

Reprinted with permission of the authors.



# Trust Anchor

## Pending U.S. Supreme Court Cases May Restrict FTC's Pursuit of Monetary Relief in Privacy and Cybersecurity Matters

Jonathan Direnfeld (<https://blogs.orrick.com/trustanchor/author/jdirenfeld/>) and David Cohen

(<https://blogs.orrick.com/trustanchor/author/davidcohen/>)



Earlier this month, the U.S. Supreme Court agreed to hear a pair of cases that provide it with the opportunity to severely restrict the Federal Trade Commission's ("FTC's") authority to obtain equitable money relief in consumer protection enforcement actions, including privacy and cybersecurity matters. Under Section 13(b) of the FTC Act, in certain circumstances the FTC is empowered to bring actions in federal court to seek temporary restraining orders and injunctions for violations of the Act. In two consolidated cases, *FTC v. Credit Bureau Center, LLC* and *AMG Capital Management, LLC v. FTC*, the Supreme Court will now consider whether, as the FTC claims, this provision also authorizes the agency to

seek equitable money relief for such violations, even though the provision makes no mention of money relief. The decision will have broad implications because the FTC has relied on Section 13(b) to seek monetary relief in consumer protection enforcement actions, including privacy and cybersecurity matters. A ruling against the FTC could substantially alter the FTC's approach to privacy and cybersecurity enforcement.

The FTC's privacy and cybersecurity enforcement actions typically rely on Section 5 of the FTC Act, which prohibits unfair or deceptive trade practices. The FTC takes the position that a failure to implement "reasonable" cybersecurity or privacy practices can constitute an "unfair" practice, and that making false or misleading statements about such practices can be a "deceptive" trade practice under the statute.

The FTC can enforce Section 5 in two ways. First, it can rely on its traditional administrative enforcement authority, which allows the FTC to initiate an administrative proceeding to issue an order to "cease and desist" violations of Section 5, but only provides for monetary relief in limited circumstances. Second, in certain situations the FTC can sue directly in federal court under Section 13(b) of the FTC Act. Although Section 13(b) authorizes only "injunctions," the FTC often brings cases under this section in federal court seeking monetary relief under equitable doctrines such as restitution, disgorgement and rescission of contracts.

Until recently, courts universally accepted the FTC's expansive view that its authority under Section 13(b) to obtain "injunctions" enables it to seek equitable monetary relief. But that has begun to change. In *Credit Bureau*, the Seventh Circuit rejected the FTC's position that Section 13(b) authorizes monetary relief on the ground that an implied equitable monetary remedy would be incompatible with the FTC Act's express remedial scheme. Most notably, the court observed that the FTC Act has two detailed remedial provisions expressly authorizing equitable money relief if the FTC follows certain procedures. The FTC's broad reading of Section 13(b) would allow the agency to circumvent these conditions on obtaining equitable money relief, contrary to the intent of Congress. And in *AMG*

*Capital Management*, although the Ninth Circuit considered itself bound to follow its prior precedent allowing the FTC to obtain money relief under Section 13(b), two of the three panel members joined a special concurrence arguing that this position is “no longer tenable.” And a **decision from the Third Circuit last year**

(<https://blogs.orrick.com/trustanchor/2019/03/13/third-circuit-shire-decision-may-spell-trouble-for-ftc-cybersecurity-enforcement-plans/>), while not addressing whether the FTC is barred from pursuing money relief under Section 13(b), held that to pursue such relief the FTC must, at a minimum, allege facts plausibly suggesting that the company “is violating, or is about to violate,” the law.

If the Supreme Court restricts or eliminates the FTC’s pursuit of equitable money relief under Section 13(b), its decision would represent a significant setback for the FTC’s recent attempts to expand its remedial authority in privacy and cybersecurity cases, among others. In June 2018, medical laboratory LabMD obtained the first-ever court decision overturning an FTC cybersecurity enforcement action, convincing the Eleventh Circuit that an FTC cease-and-desist order imposing injunctive relief requiring LabMD to implement “reasonable” data security was impermissibly vague. (The team directing that effort – led by Doug Meal and Michelle Visser – joined Orrick in January 2019.) In the wake of *LabMD*, the FTC’s new Chairman, Joseph Simons, stated that he was “very nervous” that the agency lacked the remedial authority it needed to deter allegedly insufficient data security practices and that, among other things, the FTC was exploring whether it has additional untapped authority it could use in this space. The FTC has followed through on that promise in the ensuing years, pursuing a wide range of additional remedies, including equitable money relief. An adverse ruling by the Supreme Court could strike a severe blow to the FTC’s efforts on this front.

Such a ruling is entirely possible. Just last month in *SEC v. Liu*, the Supreme Court recognized limits on the disgorgement power of the Securities and Exchange Commission, determining that it is restricted to situations where the remedy does not exceed a wrongdoer’s net profits and is awarded for victims. However, unlike the FTC Act, the SEC Act specifically authorizes the SEC to seek “equitable relief.” Therefore, the consolidated *AMG* and *Credit Bureau* cases afford the Supreme Court an opportunity to recognize even greater restrictions on the FTC’s authority to obtain equitable money relief under Section 13(b) – or, as the Seventh Circuit did in *Credit Bureau*, to reject such authority altogether.

While in the short term such a ruling may reduce the monetary risks of FTC privacy and cybersecurity enforcement for companies collecting personal information, it could serve as a catalyst for a legislative proposal that would provide the FTC significant new authority to police privacy and security violations and assess civil penalties.

To discuss these cases in more detail, or for advice on the FTC’s privacy and cybersecurity enforcement program more generally, please feel free to contact any member of our privacy & cybersecurity team, which has immense experience in this area.

## Appendix C

Jonathan Drenfeld, et al.

“Recent FTC Cybersecurity Settlements Highlight Benefits and Risks of Settling vs. Litigating” (Aug. 21, 2019)

Reprinted with permission of the authors.



# Trust Anchor

## Recent FTC Cybersecurity Settlements Highlight Benefits and Risks of Settling vs. Litigating

Jonathan Direnfeld (<https://blogs.orrick.com/trustanchor/author/jdirenfeld/>), David Cohen (<https://blogs.orrick.com/trustanchor/author/davidcohen/>) and Monica A. Svetoslavov (<https://blogs.orrick.com/trustanchor/author/msvetoslavov/>)



Amidst mounting pressure to pursue cybersecurity more aggressively, the Federal Trade Commission (“FTC”), the federal government’s most active enforcer in the space, has recently imposed increasingly stringent cybersecurity requirements in its consent orders. Given that FTC consent orders typically carry 20-year terms and **a potential fine of \$42,530** (<https://www.ftc.gov/news-events/press-releases/2019/03/ftc-publishes-inflation-adjusted-civil-penalty-amounts>) (which the FTC may contend applies to each consumer subject to a breach), it is vital for companies faced with an FTC cybersecurity investigation to take every possible step to narrow the scope of relief requested by the FTC. Several recent FTC cybersecurity

settlements illustrate an emerging pattern: a company that litigates may secure a better deal than it would have received in an initial settlement, if not defeat the action entirely. But when considering whether to settle or litigate with the FTC, companies must still balance the various legal, business, and reputational risks at stake.

How the decision to settle or litigate can directly affect the relief imposed is evident in the FTC’s 2019 cybersecurity settlements: **Unixiz** ([https://www.ftc.gov/system/files/documents/cases/i-dressup\\_stipulated\\_order\\_ecf\\_4-24-19.pdf](https://www.ftc.gov/system/files/documents/cases/i-dressup_stipulated_order_ecf_4-24-19.pdf)), **ClixSense** ([https://www.ftc.gov/system/files/documents/cases/172\\_3003\\_clixsense\\_decision\\_and\\_order\\_7-2-19.pdf](https://www.ftc.gov/system/files/documents/cases/172_3003_clixsense_decision_and_order_7-2-19.pdf)), **LightYear** ([https://www.ftc.gov/system/files/documents/cases/172\\_3051\\_dealerbuilt\\_decision\\_order.pdf](https://www.ftc.gov/system/files/documents/cases/172_3051_dealerbuilt_decision_order.pdf)), **Equifax** ([https://www.ftc.gov/system/files/documents/cases/172\\_3203\\_equifax\\_order\\_signed\\_7-23-19.pdf](https://www.ftc.gov/system/files/documents/cases/172_3203_equifax_order_signed_7-23-19.pdf)), and **D-Link** ([https://www.ftc.gov/system/files/documents/cases/dlink\\_proposed\\_order\\_and\\_judgment\\_7-2-19.pdf](https://www.ftc.gov/system/files/documents/cases/dlink_proposed_order_and_judgment_7-2-19.pdf)).

### The FTC Has Been More Aggressive in Cybersecurity Enforcement

In April 2019, the FTC announced its first settlements of the year related to cybersecurity. In conjunction with this announcement, the FTC released an **official statement** ([https://www.ftc.gov/system/files/documents/cases/2019-03-19\\_idressupclixsense\\_statement\\_final.pdf](https://www.ftc.gov/system/files/documents/cases/2019-03-19_idressupclixsense_statement_final.pdf)) highlighting the new “strong injunctive provisions” in the settlements that went “beyond the requirements from previous data security orders.” The FTC announcement made clear that these new requirements “reflect[ed] the beginning of [its] thinking” on how to “strengthen[] and improve[]...in the areas of privacy and data security.” True to its word, the FTC’s subsequent settlements have been even more stringent.

Every 2019 cybersecurity settlement contained two key provisions not found in previous orders. First, a senior officer must annually certify compliance with the order. Second, a defendant must cooperate with a third-party assessor under much stricter requirements, including a prohibition against making misrepresentations to the assessor and assessor requirements related to document preservation.

But the FTC did not stop with merely adding some new provisions: it also bolstered old ones. Provisions relating to a company's information security program have been increasingly more stringent. For example, in the **FTC's 2018 settlement with Blu Products**

([https://www.ftc.gov/system/files/documents/cases/172\\_3025\\_c4657\\_blu\\_decision\\_and\\_order\\_9-10-18.pdf](https://www.ftc.gov/system/files/documents/cases/172_3025_c4657_blu_decision_and_order_9-10-18.pdf)), the information security program listed a handful of general requirements, including employing and monitoring safeguards to protect from risks. The LightYear Order in 2019, however, added five specific safeguard requirements (including data access controls and encryption) as well as specific requirements to test the effectiveness of safeguards (including vulnerability and penetration testing). The LightYear Order also included a new requirement that the information security program be presented annually to the board of directors (or similar governing body).

Despite significantly expanded provisions in the Unixiz, ClixSense, and LightYear settlements, these were just a warm-up. For its main act, the FTC presents Equifax. The information security program in the Equifax Order contains *eight* pages of requirements compared to a mere three pages in the Unixiz order. While the Equifax Order contains many of the same security program provisions as other orders, it takes each one giant leap forward. It does not just require that a program be documented in writing; it specifies particular information that must be included in the documentation (e.g., risk assessments). It does not just require safeguards; it specifies particular safeguards that must be included (e.g., patch management policies and information security training programs). It does not just require periodic testing of safeguards; it specifies particular safeguard tests that must be included (e.g., vulnerability and penetration testing). These heightened and painstakingly specific provisions are particularly significant given the requirements will continue for *two decades*.

To be sure, companies welcome guidance from regulators as to what measures they can take to maintain a legally adequate cybersecurity program. Indeed, in *LabMD v. FTC*, one company successfully persuaded the U.S. Court of Appeals for the Eleventh Circuit last year to overturn an FTC cybersecurity order—the first time a court had ever done so—precisely because the order failed to provide any such guidance.<sup>[1]</sup> Critically, however, most of the 2019 FTC orders do not fix the FTC's prior mistake, because their provisions merely state that the steps taken by the company must "include" those that are listed in the order, not that the listed measures comprise the entire universe of what the company must do. In other words, while the 2019 orders list particular measures that are *necessary* for compliance, most of them continue to leave companies guessing as to what would be *sufficient*. This lack of guidance increases the likelihood of further liability down the line.<sup>[2]</sup>

The FTC has also recently taken other steps to ramp up the relief it seeks in its cybersecurity consent orders, including seeking opportunities to impose **monetary relief** (<https://blogs.orrick.com/trustanchor/2019/03/13/third-circuit-shire-decision-may-spell-trouble-for-ftc-cybersecurity-enforcement-plans/>) (which it obtained from Equifax as part of a coordinated settlement of consumer class actions) and **individual officer liability** (<https://blogs.orrick.com/trustanchor/2019/05/29/putting-individuals-in-the-urthbox-ftc-goes-after-individual-executives-for-unfair-and-deceptive-practices/>).

### Companies That Litigate May Get Narrower Relief

One of the 2019 FTC consent orders, however, is significantly better for the defendant than the others. It was obtained by a company that, before settling, litigated with the FTC to the eve of trial. In January 2017, the **FTC brought claims** ([https://www.ftc.gov/system/files/documents/cases/170105\\_d-link\\_complaint\\_and\\_exhibits.pdf](https://www.ftc.gov/system/files/documents/cases/170105_d-link_complaint_and_exhibits.pdf)) of unfair and deceptive practices against D-Link in connection with allegedly insecure Internet routers and cameras. Nine months later, a California judge granted D-Link's motion to dismiss three of the FTC's six counts.<sup>[3]</sup> After extensive pre-trial briefing on the remaining counts in which D-Link highlighted the many weaknesses in the FTC's case, the FTC announced a settlement with D-Link on July 2, 2019.

Notably, the information security program requirement in the D-Link consent order contained a safe harbor provision in D-Link's favor: if D-Link obtains a certification from an assessor that D-Link complies with a particular software security standard and provides notice to consumers when product security updates are discontinued, then D-Link is deemed to have satisfied the requirement to have a comprehensive software security program, no matter what objections the FTC might otherwise have to D-Link's implementation of that program. The order thus gives D-Link a clear, understandable and achievable avenue to maintain compliance. Such a safe harbor provision is not standard in FTC cybersecurity consent orders and is a far cry from the eight pages of specific requirements imposed on Equifax.

In fact, only one other FTC settlement has ever contained a similar safe harbor provision—the **agency's 2015 settlement with Wyndham** (<https://www.ftc.gov/system/files/documents/cases/151211wyndhamstip.pdf>). Just like D-Link, Wyndham litigated against the FTC, which survived an initial motion to dismiss but then faced numerous obstacles to succeeding at trial.<sup>[4]</sup> Wyndham's efforts proved fruitful, as it obtained the first-ever information security program safe harbor provision in a consent order from the FTC. Safe harbors for obtaining certifications are beneficial not only in the clarity they provide, but also because the companies in question may already be obtaining the certifications in the ordinary course of business. In this way the order's substantive requirements may impose no additional burden on the company.

The D-Link consent order also contains other similarities to the Wyndham consent order, including, among other things, a lack of any restrictions on the company's consumer-facing statements about cybersecurity (even though the complaints alleged the companies made deceptive statements about cybersecurity) and the absence of any significant injunctive relief against the company's parent corporations.

And, as noted above, the only other company to litigate significantly against the FTC—LabMD—persuaded a court to overturn the FTC's action altogether.

### **The Decision: Settle or Litigate**

The beneficial outcomes achieved by the three companies who have engaged in significant litigation with the FTC—D-Link, Wyndham, and LabMD—are not flukes. The FTC's authority in the cybersecurity space is subject to important limits. A company that demonstrates a willingness to assert those limits in court puts the FTC on notice that it may well lose at trial, making the agency more willing to settle on better terms. By contrast, the FTC will likely insist on relief more favorable to the agency if it knows that no court will ever test it on the merits.

To be sure, a company must weigh numerous factors when deciding whether to settle or litigate—not just the strength of its legal arguments (including arguments against the relief the FTC is seeking), but also business considerations, litigation costs, and reputational risks. But given the experience of D-Link, Wyndham, and LabMD, the upside in what a consent decree might contain by pressing forward with litigation cannot be ignored. Narrower relief in a consent order (or no relief at all) translates into significantly reduced litigation risk, because violations of such orders are subject to substantial civil penalties—a remedy the FTC typically cannot otherwise impose.

Our Cyber, Privacy & Data Innovation Team has immense experience in this area, including leading the LabMD and Wyndham matters discussed above. Should your company be faced with an inquiry or investigation by the FTC, you may eventually be faced with this decision: settle or litigate. And even from the moment the FTC investigation is opened, there are numerous opportunities to persuade the FTC that the agency should drop its investigation altogether. Our team can arm you with the knowledge and guidance you need to decide the best path forward.

<sup>[1]</sup> LabMD, Inc. v. Fed. Trade Comm'n, 894 F.3d 1221 (11th Cir. 2018).

<sup>[2]</sup> See, e.g., Fed. Trade Comm'n, LifeLock to Pay \$100 Million to Consumers to Settle FTC Charges it Violated 2010 Order (Feb. 17, 2015), <https://www.ftc.gov/news-events/press-releases/2015/12/lifelock-pay-100-million-consumers-settle-ftc-charges-it-violated> (<https://www.ftc.gov/news-events/press-releases/2015/12/lifelock-pay-100-million-consumers-settle-ftc-charges-it-violated>) (LifeLock paid \$100 million to settle claims it violated FTC order requirements to establish and maintain a comprehensive information security program).

<sup>[3]</sup> Fed. Trade Comm'n v. D-Link Sys., Inc., No. 3:17-CV-00039-JD, 2017 WL 4150873, at \*3-5 (N.D. Cal. Sept. 19, 2017) (dismissing two of five deception claims for lack of specificity and sole unfairness claim for failing to allege any consumer injury).

<sup>[4]</sup> Fed. Trade Comm'n v. Wyndham Worldwide Corp., 799 F.3d 236 (3d Cir. 2015) (affirming denial of Wyndham's motion to dismiss).

◀ 1

## Appendix D

Doug Meal, et al.

“FTC Data Security Consent Orders Are New But Not Improved” (Mar. 23, 2020)

Reprinted with permission of the authors.

# FTC Data Security Consent Orders Are New But Not Improved

By **Doug Meal, Michelle Visser, David Cohen and Joseph Santiesteban** (March 23, 2020, 4:01 PM EDT)

The director of the Federal Trade Commission's Bureau of Consumer Protection recently blogged[1] about recent changes to the FTC's data security orders that were designed in part to address the vagueness problem that led the U.S. Court of Appeals for the Eleventh Circuit in *LabMD Inc. v. FTC* to strike down an FTC order.[2]

The changes reflected in the FTC's latest data security orders have, however, in fact done little to address the *LabMD* court's concern or other potential overreaches of the orders traditionally entered by the FTC in data security cases.

While the newer FTC orders no longer refer to a reasonable security program, they retain the requirement that the program be both comprehensive and designed to meet certain objectives.

In addition, the newer orders include a litany of required, albeit vaguely defined, security measures that vary from order to order and that each order states are merely the minimum necessary for the company's program to meet the order's comprehensiveness and design mandates, leaving the FTC room to argue that implementation of these measures does not necessarily constitute compliance with the order.

The result is a new order that is little (if any) more precise than the traditional FTC data security order struck down in *LabMD*. Moreover, the new orders retain other features of the traditional orders that render them vulnerable to being struck down.

Companies facing potential FTC enforcement in the data security context should consider raising these deficiencies with the agency if the matter results in settlement negotiations, and, if the matter proceeds to litigation, they should also consider raising them with the adjudicator.

## LabMD

The bureau director's blog explains that since the early 2000s when the FTC began privacy and cybersecurity enforcement, FTC data security orders were fairly standard.[3] They required a company to implement "a comprehensive information security program reasonably designed to protect the security, confidentiality, and integrity of personal information" and subjected the company to biennial outside assessments, among other things, typically for 20 years.[4]

In 2018, however, in *LabMD*, the first and still only litigated case regarding the enforceability of an FTC data security order, the Eleventh Circuit struck down as impermissibly vague an order containing the FTC's standard language.[5]



Doug Meal



Michelle Visser



David Cohen

There, the FTC brought an enforcement action against a cancer detection laboratory, claiming the company had engaged in an unfair trade practice by failing to employ a variety of controls that the FTC claimed “taken together” were necessary for the company to have reasonable security for certain patient data.[6]



Joseph Santiesteban

At trial before an FTC administrative law judge, the administrative law judge dismissed the case after finding that the FTC had failed to prove that LabMD’s alleged conduct caused or was likely to cause substantial injury to consumers. [7] The full commission, however, reversed the administrative law judge, found that LabMD’s security measures violated Section 5 and instituted an order against LabMD containing the standard features.[8]

The Eleventh Circuit vacated the FTC’s order. The court explained that the concept of specificity is crucial for due process in FTC enforcement because a vague order (1) fails to provide companies with fair notice of what conduct is prohibited and (2) places a court in the impermissible role of “managing [a company’s] business in accordance with the Commission’s wishes.”[9]

The court held that the LabMD order was not sufficiently specific because it commanded LabMD’s information security program “to meet an indeterminable standard of reasonableness.”[10] The court also held that the order “fail[s] to state with specificity the actions LabMD must take to bring its program into compliance with the order.”[11]

### **FTC’s New Data Security Orders**

The bureau director’s blog explains that since LabMD, the FTC has modified its standard data security order language in an attempt to address the vagueness problem. The changes are also purportedly designed to incorporate learnings from recent FTC hearings.[12]

The blog references seven recent FTC data security orders,[13] and it asserts that these newer orders reflect three categories of changes to the traditional FTC data security order. First, the newer orders are supposedly more specific, requiring particular security measures, including, for example, “yearly employee training, access controls, monitoring systems for data security incidents, patch management systems, and encryption.”[14]

Second, the newer orders supposedly increase assessor accountability by requiring assessors to “identify evidence to support their conclusions, including independent sampling, employee interviews, and document review.”[15] Moreover, “assessors must retain documents related to the assessment, and cannot refuse to provide those documents to the FTC on the basis of certain privileges.”[16]

Third, companies must “present their Board or similar governing body with their written information security program,” and a senior official must “provide annual certifications of compliance to the FTC.”[17]

### **Vagueness Remains**

While the new FTC orders each identify a litany of security measures required to satisfy the order’s mandate to implement a comprehensive security program designed to achieve certain objectives, the FTC’s new standard language remains vulnerable to a vagueness challenge because it specifies that such measures are necessary, but not necessarily sufficient, to achieve compliance with the order.

For instance, the Equifax Inc. order requires the company to establish, implement and maintain “a comprehensive information security program (‘Information Security Program’) designed to protect the security, confidentiality, and integrity of Personal Information.”[18] The order then specifies eight pages of requirements that Equifax “must, at a minimum” comply with in order for the program to satisfy the overall comprehensiveness and design requirements.[19]

The FTC’s use of “at a minimum,” however, leaves the FTC room to argue that the order’s eight pages of requirements, while being necessary, are not necessarily by themselves sufficient, to satisfy the general obligation to implement an information security program that is both comprehensive and

“designed to protect the security, confidentiality, and integrity of Personal Information.”[20]

Moreover, many of the individual requirements are themselves vague because, like the overarching comprehensive and design requirements, they don’t specify what a company must do to meet those individual requirements.

For instance, the Equifax order requires the company to “[d]esign, implement, maintain, and document safeguards that control for the material internal and external risks [Equifax] identifies to the security, confidentiality, or integrity of Personal Information.”[21]

The order then states that such safeguards shall also include a host of measures relating to patching, inventorying, access controls, password controls, privilege control, encryption and training.[22]

Thus, these sub-requirements and sub-sub-requirements are defined in a manner that would enable the FTC to argue that they are not in and of themselves sufficient to achieve the individual requirement in question. Many of the subrequirements and sub-subrequirements, moreover, are open to multiple interpretations.

For example, the Equifax order requires Equifax to assess and document material risks, to implement strong password requirements, and ensure the use of secure development practices. Whether risks are material, passwords are strong, or development practices are secure, however, could be fodder for the same sort of “battle of the experts” that the LabMD court found would signify an impermissibly vague order.[23]

At bottom then, the FTC’s new standard language looks to be no more precise than the “reasonable” security standard struck down in LabMD and accordingly could be subject to a vagueness challenge along the lines of the argument successfully made in that case.

The FTC cannot plausibly explain its continuing refusal to enter into orders that provide sufficient guidance on how to achieve compliance by arguing it is somehow impossible for the FTC to do so.

The agency has twice negotiated data security consent orders that provided this exact sort of clarity in the form of safe harbors — that is, provisions stating that if the company obtains an assessment certifying its compliance with a specified security standard, then it will be deemed compliant with the requirement to maintain a security program that meets the order’s comprehensiveness and design requirements.[24]

The FTC only agreed to these two safe harbors, however, after the companies litigated with the agency for years. The FTC’s divergence from its standard order in these two cases underscores the potential value of litigating with the FTC rather than accepting a prelitigation offer of its new — but unimproved — standard data security order.

### **Improper Scope of Relief**

In addition to remaining vulnerable to a vagueness challenge, the FTC’s new data security orders retain the prior orders’ burdensome relief provisions that may well exceed the scope of the FTC’s remedial authority. The new FTC orders, like the prior ones, are subject to challenge for requiring security measures that are not otherwise legally required and for covering practices that are not reasonably related to the practices the FTC originally challenged as unlawful.[25]

They are also vulnerable on the ground that they do not merely prohibit certain conduct, but require affirmative action on the company’s part — a type of relief courts are particularly hesitant to uphold and that go well beyond the mere “cease and desist” order that the FTC is statutorily limited to obtaining via an administrative proceeding.[26]

The affirmative relief embodied in both the prior orders and the new ones is even more inappropriate in circumstances where the company’s existing security practices were not themselves alleged to be unlawful, and instead the company was merely alleged to have misrepresented those practices to consumers.[27] And in both contexts, the prior and new orders are of questionable validity in requiring the company to conduct, and pay for out of its own pocket, a biannual assessment of its compliance with the order.

## Conclusion

The FTC's self-described "new and improved"[28] data security consent orders are certainly new in some respects, but they are not, unfortunately, improved. Companies facing potential FTC enforcement should raise the continuing deficiencies in these orders with the agency if the matter results in settlement negotiations, and, if the matter proceeds to litigation, they should also raise them with the adjudicator.

---

*Doug Meal is a partner and head of the cyber and data privacy litigation and regulatory enforcement practice at Orrick Herrington & Sutcliffe LLP.*

*Michelle Visser is a partner at the firm.*

*David Cohen is of counsel at the firm.*

*Joseph Santiesteban is an associate at the firm.*

*The authors thank Orrick associate James Liu for contributing to this article.*

*The opinions expressed are those of the author(s) and do not necessarily reflect the views of the firm, its clients, or Portfolio Media Inc., or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.*

[1] Federal Trade Comm'n, New and improved FTC data security orders: Better guidance for companies, better protection for consumers, (Jan 6, 2020) <https://www.ftc.gov/news-events/blogs/business-blog/2020/01/new-improved-ftc-data-security-orders-better-guidance>.

[2] *LabMD, Inc. v. Fed. Trade Comm'n* , 894 F.3d 1221, 1237 (11th Cir. 2018).

[3] Federal Trade Comm'n, *supra* note 1.

[4] *Id.*

[5] *LabMD*, 894 F.3d at 1237.

[6] *Id.* at 1225.

[7] *Id.*

[8] *LabMD*, 894 F.3d at 1226-27.

[9] *LabMD*, 894 F.3d at 1235-37; see also, e.g., Fed. Trade Comm'n, LifeLock to Pay \$100 Million to Consumers to Settle FTC Charges it Violated 2010 Order (Feb. 17, 2015), <https://www.ftc.gov/news-events/press-releases/2015/12/lifelock-pay-100-million-consumers-settle-ftc-charges-it-violated> (LifeLock paid \$100 million to settle claims it violated FTC order requirements to establish and maintain a comprehensive information security program).

[10] *LabMD*, 894 F.3d at 1236.

[11] *Id.* at n.42.

[12] See Federal Trade Comm'n, *supra* note 1. (citing Federal Trade Comm'n, FTC Hearing #9: Data Security, Hearings on Competition and Consumer Protection in the 21st Century (Dec. 11-12, 2018), <https://www.ftc.gov/news-events/events-calendar/ftc-hearing-competition-consumer-protection-21st-century-december-2018>).

[13] Stipulated Order, Fed. Trade Comm'n v. Equifax Inc., No. 1:19-cv-03297-TWT, ECF No. 6 (N.D. Ga. Jul. 23, 2019),

[https://www.ftc.gov/system/files/documents/cases/172\\_3203\\_equifax\\_order\\_signed\\_7-23-19.pdf](https://www.ftc.gov/system/files/documents/cases/172_3203_equifax_order_signed_7-23-19.pdf); Proposed Stipulated Order, Fed. Trade Comm’n v. D-Link Sys., Inc., No. 3:17-CV-00039-JD, ECF No. 272-1 (N.D. Cal. Jul. 2, 2019), [https://www.ftc.gov/system/files/documents/cases/dlink\\_proposed\\_order\\_and\\_judgment\\_7-2-19.pdf](https://www.ftc.gov/system/files/documents/cases/dlink_proposed_order_and_judgment_7-2-19.pdf); Proposed Stipulated Order, United States of Am. v. Unixiz, Inc. et al., No. 5:19-cv-2222, ECF No. 3 (N.D. Ca. Apr. 24, 2019), [https://www.ftc.gov/system/files/documents/cases/i-dressup\\_stipulated\\_order\\_ecf\\_4-24-19.pdf](https://www.ftc.gov/system/files/documents/cases/i-dressup_stipulated_order_ecf_4-24-19.pdf); Decision and Order, In the matter of InfoTrax, LLC, et al., No. 162-3130, Dkt. No. C-4696 (F.T.C. Dec. 30, 2019), [https://www.ftc.gov/system/files/documents/cases/c-4696\\_162\\_3130\\_infotrax\\_order\\_clean.pdf](https://www.ftc.gov/system/files/documents/cases/c-4696_162_3130_infotrax_order_clean.pdf); Consent Order, In the matter of Retina-X Studios, LLC, et al., No. 172-3118 (F.T.C. Oct. 22, 2019), [https://www.ftc.gov/system/files/documents/cases/172\\_3118\\_-\\_retina-x\\_studios\\_agreement\\_containing\\_consent\\_order.pdf](https://www.ftc.gov/system/files/documents/cases/172_3118_-_retina-x_studios_agreement_containing_consent_order.pdf); Decision and Order, In the Matter of LightYear Dealer Technologies, LLC, d/b/a DealerBuilt, No. 172-3051, Dkt. No. C-4687 (F.T.C. Sept. 3, 2019), [https://www.ftc.gov/system/files/documents/cases/172\\_3051\\_c-4687\\_dealerbuilt\\_decision\\_order.pdf](https://www.ftc.gov/system/files/documents/cases/172_3051_c-4687_dealerbuilt_decision_order.pdf); Decision and Order, In the Matter of James V. Grago, Jr., individually and d/b/a ClixSense.com, No. 172-3003, Dkt. No. C-4678 (F.T.C. June 19, 2019), [https://www.ftc.gov/system/files/documents/cases/172\\_3003\\_clixsense\\_decision\\_and\\_order\\_7-2-19.pdf](https://www.ftc.gov/system/files/documents/cases/172_3003_clixsense_decision_and_order_7-2-19.pdf).

[14] Federal Trade Comm’n, *supra* note 1.

[15] *Id.*

[16] *Id.*

[17] *Id.*

[18] Equifax, *supra* note 13, at 12.

[19] *Id.* at 12-19.

[20] Moreover, while each of the orders requires a program that is both “comprehensive” and “designed” to meet those objectives, each order arguably defines “comprehensive” and “designed” differently by requiring different security measures, further confusing what is actually required to satisfy the FTC’s expectation of a “comprehensive security program.” Compare, e.g., Equifax, *supra* note 13, at 12-19, with Lightyear Order, *supra* note 13, at 2-4. Unless, of course, the FTC does not actually intend each list of required measures to be an exhaustive list of what is required, which would render each order impermissibly vague under the reasoning set forth in LabMD as discussed herein.

[21] Equifax, *supra* note 13, at 14.

[22] *Id.* at 14-17.

[23] *Id.* at 13, 15-16; see LabMD, 894 F.3d at 1237.

[24] Proposed Stipulated Order, Fed. Trade Comm’n v. D-Link Sys., Inc., No. 3:17-CV-00039-JD, ECF No. 272-1, at 9-10 (N.D. Cal. Jul. 2, 2019), [https://www.ftc.gov/system/files/documents/cases/dlink\\_proposed\\_order\\_and\\_judgment\\_7-2-19.pdf](https://www.ftc.gov/system/files/documents/cases/dlink_proposed_order_and_judgment_7-2-19.pdf); Stipulated Order, Fed. Trade Comm’n v. Wyndham Worldwide Corp. et al., No. 2:13-cv-01887, ECF No. 283, at 8-9 (D. N.J. Dec. 11, 2015), <https://www.ftc.gov/system/files/documents/cases/151211wyndhamstip.pdf>.

[25] See 1 Stephanie W. Kanwit, Fed. Trade Comm’n § 11:2 (2019).

[26] See *id.*; see also 11A Mary Kae Kane, Federal Practice and Procedure (Wright & Miller) § 2942 (3d ed. 2019). While the Eleventh Circuit did not need to reach these issues in LabMD, since the court invalidated the order in that case on vagueness grounds, the Eleventh Circuit did explain that FTC cease and desist orders are intended to contain “prohibitions” and that “the order’s prohibitions must be stated with clarity and precision.” LabMD, 894 F.3d at 1235-36.

[27] See Statement of Comm'r Orson Swindle, In re Int'l Outsourcing, Group, No. 992-3245, n.1 (July 12, 2000), <https://www.ftc.gov/sites/default/files/documents/cases/2000/07/ftc.gov-iogswin.htm> ("Indeed, when a defendant makes the false claim that its product is efficacious, the usual remedy is to prohibit the defendant from making the same or similar false efficacy claims, not to mandate that the defendant make its product "reasonably efficacious."").

[28] Federal Trade Comm'n, *supra* note 1.

## Appendix E

California Civil Code

TITLE 1.81.5. California Consumer Privacy Act of 2018 (current as of Sept. 25, 2020)


[Home](#)
[Bill Information](#)
[California Law](#)
[Publications](#)
[Other Resources](#)
[My Subscriptions](#)
[My Favorites](#)
**Code:** 
**Section:** 


[Up^](#) [Add To My Favorites](#)

### CIVIL CODE - CIV

**DIVISION 3. OBLIGATIONS [1427 - 3273]** (*Heading of Division 3 amended by Stats. 1988, Ch. 160, Sec. 14. )*

**PART 4. OBLIGATIONS ARISING FROM PARTICULAR TRANSACTIONS [1738 - 3273.16]** (*Part 4 enacted 1872. )*

**TITLE 1.81.5. California Consumer Privacy Act of 2018 [1798.100 - 1798.199]** (*Title 1.81.5 added by Stats. 2018, Ch. 55, Sec. 3. )*

**1798.100.** (a) A consumer shall 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.

(b) A business that collects a consumer's personal information shall, at or before the point of collection, 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. A business shall not collect additional categories of personal information or use personal information collected for additional purposes without providing the consumer with notice consistent with this section.

(c) A business shall provide the information specified in subdivision (a) to a consumer only upon receipt of a verifiable consumer request.

(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. The information may be delivered by mail or electronically, and if provided electronically, the information shall be in a portable and, to the extent technically feasible, readily useable format that allows the consumer to transmit this information to another entity without hindrance. A business may provide personal information to a consumer at any time, but shall not be required to provide personal information to a consumer more than twice in a 12-month period.

(e) This section shall not require a business to retain any personal information collected for a single, one-time transaction, if such information is not sold or retained by the business or to reidentify or otherwise link information that is not maintained in a manner that would be considered personal information.

(*Amended by Stats. 2019, Ch. 757, Sec. 1. (AB 1355) Effective January 1, 2020.*)

**1798.105.** (a) 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.

(b) A business that collects personal information about consumers shall disclose, pursuant to Section 1798.130, the consumer's rights to request the deletion of the consumer's personal information.

(c) A business that receives a verifiable consumer request from a consumer to delete the consumer's personal information pursuant to subdivision (a) of this section shall delete the consumer's personal information from its records and direct any service providers to delete the consumer's personal information from their records.

(d) A business or a service provider shall not be required to comply with a consumer's request to delete the consumer's personal information if it is necessary for the business or service provider to maintain the consumer's personal information in order to:

(1) Complete the transaction for which the personal information was collected, fulfill the terms of a written warranty or product recall conducted in accordance with federal law, provide a good or service requested by the consumer, or reasonably anticipated within the context of a business' ongoing business relationship with the consumer, or otherwise perform a contract between the business and the consumer.

- (2) Detect security incidents, protect against malicious, deceptive, fraudulent, or illegal activity; or prosecute those responsible for that activity.
- (3) Debug to identify and repair errors that impair existing intended functionality.
- (4) Exercise free speech, ensure the right of another consumer to exercise that consumer's right of free speech, or exercise another right provided for by law.
- (5) Comply with the California Electronic Communications Privacy Act pursuant to Chapter 3.6 (commencing with Section 1546) of Title 12 of Part 2 of the Penal Code.
- (6) Engage in public or peer-reviewed scientific, historical, or statistical research in the public interest that adheres to all other applicable ethics and privacy laws, when the business' deletion of the information is likely to render impossible or seriously impair the achievement of such research, if the consumer has provided informed consent.
- (7) To enable solely internal uses that are reasonably aligned with the expectations of the consumer based on the consumer's relationship with the business.
- (8) Comply with a legal obligation.
- (9) Otherwise use the consumer's personal information, internally, in a lawful manner that is compatible with the context in which the consumer provided the information.

*(Amended by Stats. 2019, Ch. 751, Sec. 1. (AB 1146) Effective January 1, 2020.)*

**1798.110.** (a) A consumer shall have the right to request that a business that collects personal information about the consumer disclose to the consumer the following:

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

(b) A business that collects personal information about a consumer shall disclose to the consumer, pursuant to paragraph (3) of subdivision (a) of Section 1798.130, the information specified in subdivision (a) upon receipt of a verifiable consumer request from the consumer.

(c) A business that collects personal information about consumers shall disclose, pursuant to subparagraph (B) of paragraph (5) of subdivision (a) of Section 1798.130:

- (1) The categories of personal information it has collected about consumers.
- (2) The categories of sources from which the personal information is collected.
- (3) The business or commercial purpose for collecting or selling personal information.
- (4) The categories of third parties with whom the business shares personal information.
- (5) That a consumer has the right to request the specific pieces of personal information the business has collected about that consumer.

(d) This section does not require a business to do the following:

- (1) Retain any personal information about a consumer collected for a single one-time transaction if, in the ordinary course of business, that information about the consumer is not retained.
- (2) Reidentify or otherwise link any data that, in the ordinary course of business, is not maintained in a manner that would be considered personal information.

*(Amended by Stats. 2019, Ch. 757, Sec. 2. (AB 1355) Effective January 1, 2020.)*

**1798.115.** (a) A consumer shall have the right to request that a business that sells the consumer's personal information, or that discloses it for a business purpose, disclose to that consumer:

- (1) The categories of personal information that the business collected about the consumer.
- (2) The categories of personal information that the business sold about the consumer and the categories of third parties to whom the personal information was sold, by category or categories of personal information for each category 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.

(b) A business that sells personal information about a consumer, or that discloses a consumer's personal information for a business purpose, shall disclose, pursuant to paragraph (4) of subdivision (a) of Section 1798.130, the information specified in subdivision (a) to the consumer upon receipt of a verifiable consumer request from the consumer.

(c) A business that sells consumers' personal information, or that discloses consumers' personal information for a business purpose, shall disclose, pursuant to subparagraph (C) of paragraph (5) of subdivision (a) of Section 1798.130:

(1) The category or categories of consumers' personal information it has sold, or if the business has not sold consumers' personal information, it shall disclose that fact.

(2) The category or categories of consumers' personal information it has disclosed for a business purpose, or if the business has not disclosed the consumers' personal information for a business purpose, it shall disclose that fact.

(d) A third party shall not sell personal information about a consumer that has been sold to the third party by a business unless the consumer has received explicit notice and is provided an opportunity to exercise the right to opt-out pursuant to Section 1798.120.

*(Amended by Stats. 2019, Ch. 757, Sec. 3. (AB 1355) Effective January 1, 2020.)*

**1798.120.** (a) 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 information. This right may be referred to as the right to opt-out.

(b) A business that sells consumers' personal information to third parties shall provide notice to consumers, pursuant to subdivision (a) of Section 1798.135, that this information may be sold and that consumers have the "right to opt-out" of the sale of their personal information.

(c) Notwithstanding subdivision (a), a business shall not sell the personal information of consumers if the business has actual knowledge that the consumer is less than 16 years of age, unless the consumer, in the case of consumers at least 13 years of age and less than 16 years of age, or the consumer's parent or guardian, in the case of consumers who are less than 13 years of age, has affirmatively authorized the sale of the consumer's personal information. A business that willfully disregards the consumer's age shall be deemed to have had actual knowledge of the consumer's age. This right may be referred to as the "right to opt-in."

(d) A business that has received direction from a consumer not to sell the consumer's personal information or, in the case of a minor consumer's personal information has not received consent to sell the minor consumer's personal information shall be prohibited, pursuant to paragraph (4) of subdivision (a) of Section 1798.135, from selling the consumer's personal information after its receipt of the consumer's direction, unless the consumer subsequently provides express authorization for the sale of the consumer's personal information.

*(Amended by Stats. 2019, Ch. 757, Sec. 4. (AB 1355) Effective January 1, 2020.)*

**1798.125.** (a) (1) A business shall not discriminate against a consumer because the consumer exercised any of the consumer's rights under this title, including, but not limited to, by:

(A) Denying goods or services to the consumer.

(B) Charging different prices or rates for goods or services, including through the use of discounts or other benefits or imposing penalties.

(C) Providing a different level or quality of goods or services to the consumer.

(D) Suggesting that the consumer will receive a different price or rate for goods or services or a different level or quality of goods or services.

(2) Nothing in this subdivision prohibits a business from charging a consumer a different price or rate, or from providing a different level or quality of goods or services to the consumer, if that difference is reasonably related to the value provided to the business by the consumer's data.

(b) (1) A business may offer financial incentives, including payments to consumers as compensation, for the collection of personal information, the sale of personal information, or the deletion of personal information. A business may also offer a different price, rate, level, or quality of goods or services to the consumer if that price or difference is directly related to the value provided to the business by the consumer's data.

(2) A business that offers any financial incentives pursuant to this subdivision shall notify consumers of the financial incentives pursuant to Section 1798.130.

(3) A business may enter a consumer into a financial incentive program only if the consumer gives the business prior opt-in consent pursuant to Section 1798.130 that clearly describes the material terms of the financial incentive program, and which may be revoked by the consumer at any time.

(4) A business shall not use financial incentive practices that are unjust, unreasonable, coercive, or usurious in nature.

*(Amended by Stats. 2019, Ch. 757, Sec. 5. (AB 1355) Effective January 1, 2020.)*

**1798.130.** (a) In order to comply with Sections 1798.100, 1798.105, 1798.110, 1798.115, and 1798.125, a business shall, in a form that is reasonably accessible to consumers:

(1) (A) Make available to consumers two or more designated methods for submitting requests for information required to be disclosed pursuant to Sections 1798.110 and 1798.115, including, at a minimum, a toll-free telephone number. A business that operates exclusively online and has a direct relationship with a consumer from whom it collects personal information shall only be required to provide an email address for submitting requests for information required to be disclosed pursuant to Sections 1798.110 and 1798.115.

(B) If the business maintains an internet website, make the internet website available to consumers to submit requests for information required to be disclosed pursuant to Sections 1798.110 and 1798.115.

(2) Disclose and deliver the required information to a consumer free of charge within 45 days of receiving a verifiable consumer request from the consumer. The business shall promptly take steps to determine whether the request is a verifiable consumer request, but this shall not extend the business' 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' 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 may require authentication of the consumer that is reasonable in light of the nature of the personal information requested, but shall not require the consumer to create an account with the business in order to make a verifiable consumer request. If the consumer maintains an account with the business, the business may require the consumer to submit the request through that account.

(3) For purposes of subdivision (b) of Section 1798.110:

(A) To identify the consumer, associate the information provided by the consumer in the verifiable consumer request to any personal information previously collected by the business about the consumer.

(B) Identify by category or categories the personal information collected about the consumer in the preceding 12 months by reference to the enumerated category or categories in subdivision (c) that most closely describes the personal information collected.

(4) For purposes of subdivision (b) of Section 1798.115:

(A) Identify the consumer and associate the information provided by the consumer in the verifiable consumer request to any personal information previously collected by the business about the consumer.

(B) Identify by category or categories the personal information of the consumer that the business sold in the preceding 12 months by reference to the enumerated category in subdivision (c) that most closely describes the personal information, and provide the categories of third parties to whom the consumer's personal information was sold in the preceding 12 months by reference to the enumerated category or categories in subdivision (c) that most closely describes the personal information sold. The business shall disclose the information in a list that is separate from a list generated for the purposes of subparagraph (C).

(C) Identify by category or categories the personal information of the consumer that the business disclosed for a business purpose in the preceding 12 months by reference to the enumerated category or categories in subdivision (c) that most closely describes the personal information, and provide the categories of third parties to whom the consumer's personal information was disclosed for a business purpose in the preceding 12 months by reference to the enumerated category or categories in subdivision (c) that most closely describes the personal information disclosed. The business shall disclose the information in a list that is separate from a list generated for the purposes of subparagraph (B).

(5) Disclose the following information in its online privacy policy or policies if the business has an online privacy policy or policies and in any California-specific description of consumers' privacy rights, or if the business does not maintain those policies, on its internet website and update that information at least once every 12 months:

(A) A description of a consumer's rights pursuant to Sections 1798.100, 1798.105, 1798.110, 1798.115, and 1798.125 and one or more designated methods for submitting requests.

(B) For purposes of subdivision (c) of Section 1798.110, a list of the categories of personal information it has collected about consumers in the preceding 12 months by reference to the enumerated category or categories in subdivision (c) that most closely describe the personal information collected.

(C) For purposes of paragraphs (1) and (2) of subdivision (c) of Section 1798.115, two separate lists:

(i) A list of the categories of personal information it has sold about consumers in the preceding 12 months by reference to the enumerated category or categories in subdivision (c) that most closely describe the personal information sold, or if the business has not sold consumers' personal information in the preceding 12 months, the business shall disclose that fact.

(ii) A list of the categories of personal information it has disclosed about consumers for a business purpose in the preceding 12 months by reference to the enumerated category in subdivision (c) that most closely describe the personal information disclosed, or if the business has not disclosed consumers' personal information for a business purpose in the preceding 12 months, the business shall disclose that fact.

(6) Ensure that all individuals responsible for handling consumer inquiries about the business' privacy practices or the business' compliance with this title are informed of all requirements in Sections 1798.100, 1798.105, 1798.110, 1798.115, and 1798.125, and this section, and how to direct consumers to exercise their rights under those sections.

(7) Use any personal information collected from the consumer in connection with the business' verification of the consumer's request solely for the purposes of verification.

(b) A business is not obligated to provide the information required by Sections 1798.110 and 1798.115 to the same consumer more than twice in a 12-month period.

(c) The categories of personal information required to be disclosed pursuant to Sections 1798.110 and 1798.115 shall follow the definition of personal information in Section 1798.140.

*(Amended by Stats. 2019, Ch. 763, Sec. 1.3. (AB 25) Effective January 1, 2020.)*

**1798.135.** (a) A business that is required to comply with Section 1798.120 shall, in a form that is reasonably accessible to consumers:

(1) Provide a clear and conspicuous link on the business's Internet homepage, 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. A business shall not require a consumer to create an account in order to direct the business not to sell the consumer's personal information.

(2) Include a description of a consumer's rights pursuant to Section 1798.120, along with a separate link to the "Do Not Sell My Personal Information" Internet Web page in:

(A) Its online privacy policy or policies if the business has an online privacy policy or policies.

(B) Any California-specific description of consumers' privacy rights.

(3) Ensure that all individuals responsible for handling consumer inquiries about the business's privacy practices or the business's compliance with this title are informed of all requirements in Section 1798.120 and this section and how to direct consumers to exercise their rights under those sections.

(4) For consumers who exercise their right to opt-out of the sale of their personal information, refrain from selling personal information collected by the business about the consumer.

(5) For a consumer who has opted-out of the sale of the consumer's personal information, respect the consumer's decision to opt-out for at least 12 months before requesting that the consumer authorize the sale of the consumer's personal information.

(6) Use any personal information collected from the consumer in connection with the submission of the consumer's opt-out request solely for the purposes of complying with the opt-out request.

(b) Nothing in this title shall be construed to require a business to comply with the title by including the required links and text on the homepage that the business makes available to the public generally, if the business maintains a separate and additional homepage that is dedicated to California consumers and that includes the required links and text, and the business takes reasonable steps to ensure that California consumers are directed to the homepage for California consumers and not the homepage made available to the public generally.

(c) A consumer may authorize another person solely to opt-out of the sale of the consumer's personal information on the consumer's behalf, and a business shall comply with an opt-out request received from a person authorized

by the consumer to act on the consumer's behalf, pursuant to regulations adopted by the Attorney General.

*(Amended (as added by Stats. 2018, Ch. 55, Sec. 3) by Stats. 2018, Ch. 735, Sec. 8. (SB 1121) Effective September 23, 2018. Section operative January 1, 2020, pursuant to Section 1798.198.)*

**1798.140.** For purposes of this title:

(a) "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. "Aggregate consumer information" does not mean one or more individual consumer records that have been deidentified.

(b) "Biometric information" means an individual's physiological, biological, or behavioral characteristics, including an individual's deoxyribonucleic acid (DNA), that can be used, singly or in combination with each other or with other identifying data, to establish individual identity. Biometric information includes, but is not limited to, imagery of the iris, retina, fingerprint, face, hand, palm, vein patterns, and voice recordings, from which an identifier template, such as a faceprint, a minutiae template, or a voiceprint, can be extracted, and keystroke patterns or rhythms, gait patterns or rhythms, and sleep, health, or exercise data that contain identifying information.

(c) "Business" means:

(1) A sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners that collects consumers' personal information or on the behalf of which that 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:

(A) Has annual gross revenues in excess of twenty-five million dollars (\$25,000,000), as adjusted pursuant to paragraph (5) of subdivision (a) of Section 1798.185.

(B) Alone or in combination, annually buys, receives for the business's commercial purposes, sells, or shares for commercial purposes, alone or in combination, the personal information of 50,000 or more consumers, households, or devices.

(C) Derives 50 percent or more of its annual revenues from selling consumers' personal information.

(2) Any entity that controls or is controlled by a business as defined in paragraph (1) and that shares common branding with the business. "Control" or "controlled" means ownership of, or the power to vote, more than 50 percent of the outstanding shares of any class of voting security of a business; control in any manner over the election of a majority of the directors, or of individuals exercising similar functions; or the power to exercise a controlling influence over the management of a company. "Common branding" means a shared name, servicemark, or trademark.

(d) "Business purpose" means the use of personal information for the business's or a service provider's operational purposes, or other notified purposes, provided that the use of personal information shall 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) Detecting security incidents, protecting against malicious, deceptive, fraudulent, or illegal activity, and prosecuting those responsible for that activity.

(3) Debugging to identify and repair errors that impair existing intended functionality.

(4) Short-term, transient use, provided that the personal information 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 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.

(e) "Collects," "collected," or "collection" means 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.

(f) "Commercial purposes" means 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. "Commercial purposes" do not include for the purpose of engaging in speech that state or federal courts have recognized as noncommercial speech, including political speech and journalism.

(g) "Consumer" means a natural person who is a California resident, as defined in Section 17014 of Title 18 of the California Code of Regulations, as that section read on September 1, 2017, however identified, including by any unique identifier.

(h) "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.

(i) "Designated methods for submitting requests" means a mailing address, email address, internet web page, internet web portal, toll-free telephone number, or other applicable contact information, whereby consumers may submit a request or direction under this title, and any new, consumer-friendly means of contacting a business, as approved by the Attorney General pursuant to Section 1798.185.

(j) "Device" means any physical object that is capable of connecting to the internet, directly or indirectly, or to another device.

(k) "Health insurance information" means a consumer's insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the consumer, or any information in the consumer's application and claims history, including any appeals records, if the information is linked or reasonably linkable to a consumer or household, including via a device, by a business or service provider.

(l) "Homepage" means the introductory page of an internet website 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 the notice required by subdivision (a) of Section 1798.135, including, but not limited to, before downloading the application.

(m) "Infer" or "inference" means the derivation of information, data, assumptions, or conclusions from facts, evidence, or another source of information or data.

(n) "Person" means an individual, proprietorship, firm, partnership, joint venture, syndicate, business trust, company, corporation, limited liability company, association, committee, and any other organization or group of persons acting in concert.

(o) (1) "Personal information" means information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household. Personal information includes, but is not limited to, the following if it identifies, relates to, describes, is reasonably capable of being associated with, or could be reasonably linked, directly or indirectly, with a particular consumer or household:

(A) Identifiers such as a real name, alias, postal address, unique personal identifier, online identifier, internet protocol address, email address, account name, social security number, driver's license number, passport number, or other similar identifiers.

(B) Any categories of personal information described in subdivision (e) of Section 1798.80.

(C) Characteristics of protected classifications under California or federal law.

(D) Commercial information, including records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies.

(E) Biometric information.

(F) Internet or other electronic network activity information, including, but not limited to, browsing history, search history, and information regarding a consumer's interaction with an internet website, application, or advertisement.

(G) Geolocation data.

(H) Audio, electronic, visual, thermal, olfactory, or similar information.

(I) Professional or employment-related information.

(J) Education information, defined as information that is not publicly available personally identifiable information as defined in the Family Educational Rights and Privacy Act (20 U.S.C. Sec. 1232g; 34 C.F.R. Part 99).

(K) Inferences drawn from any of the information identified in this subdivision to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.

(2) "Personal information" does not include publicly available information. For purposes of this paragraph, "publicly available" means information that is lawfully made available from federal, state, or local government records. "Publicly available" does not mean biometric information collected by a business about a consumer without the consumer's knowledge.

(3) "Personal information" does not include consumer information that is deidentified or aggregate consumer information.

(p) "Probabilistic identifier" means the identification of a consumer or a device to a degree of certainty of more probable than not based on any categories of personal information included in, or similar to, the categories enumerated in the definition of personal information.

(q) "Processing" means any operation or set of operations that are performed on personal data or on sets of personal data, whether or not by automated means.

(r) "Pseudonymize" or "Pseudonymization" means 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.

(s) "Research" means 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 interest in the area of public health. Research with personal information that may have been collected from a consumer in the course of the consumer's interactions with a business's service or device for other purposes shall be:

(1) Compatible with the business purpose for which the personal information was collected.

(2) Subsequently pseudonymized and deidentified, or deidentified and in the aggregate, such that the information cannot reasonably identify, relate to, describe, be capable of being associated with, or be linked, directly or indirectly, to a particular consumer.

(3) Made subject to technical safeguards that prohibit reidentification of the consumer to whom the information may pertain.

(4) Subject to business processes that specifically prohibit reidentification of the information.

(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.

(9) Subjected by the business conducting the research to additional security controls that limit access to the research data to only those individuals in a business as are necessary to carry out the research purpose.

(t) (1) "Sell," "selling," "sale," or "sold," means 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.

(2) For purposes of this title, a business does not sell personal information when:

(A) A consumer uses or directs the business to intentionally disclose personal information or uses the business to intentionally interact with a third party, provided the third party does not also sell the personal information, unless that disclosure would be consistent with the provisions of this title. An intentional interaction occurs when the consumer intends to interact with the third party, via one or more deliberate interactions. Hovering over, muting, pausing, or closing a given piece of content does not constitute a consumer's intent to interact with a third party.

(B) The business uses or shares an identifier for a consumer who has opted out of the sale of the consumer's personal information for the purposes of alerting third parties that the consumer has opted out of the sale of the consumer's personal information.

(C) The business uses or shares with a service provider personal information of a consumer that is necessary to perform a business purpose if both of the following conditions are met:

(i) The business has provided notice of that information being used or shared in its terms and conditions consistent with Section 1798.135.

(ii) The service provider does not further collect, sell, or use the personal information of the consumer except as necessary to perform the business purpose.

(D) The business transfers to a third party the personal information of a consumer as an asset that is part of a merger, acquisition, bankruptcy, or other transaction in which the third party assumes control of all or part of the business, provided that information is used or shared consistently with Sections 1798.110 and 1798.115. If a third party materially alters how it uses or shares the personal information of a consumer in a manner that is materially inconsistent with the promises made at the time of collection, it shall provide prior notice of the new or changed practice to the consumer. The notice shall be sufficiently prominent and robust to ensure that existing consumers can easily exercise their choices consistently with Section 1798.120. This subparagraph does not authorize a business to make material, retroactive privacy policy changes or make other changes in their privacy policy in a manner that would violate the Unfair and Deceptive Practices Act (Chapter 5 (commencing with Section 17200) of Part 2 of Division 7 of the Business and Professions Code).

(u) "Service" or "services" means work, labor, and services, including services furnished in connection with the sale or repair of goods.

(v) "Service provider" means a sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners, that processes information on behalf of a business and to which the business discloses a consumer's personal information for a business purpose pursuant to a written contract, provided that the contract prohibits the entity receiving the information from retaining, using, or disclosing the personal information for any purpose other than for the specific purpose of performing the services specified in the contract for the business, or as otherwise permitted by this title, including retaining, using, or disclosing the personal information for a commercial purpose other than providing the services specified in the contract with the business.

(w) "Third party" means a person who is not any of the following:

(1) The business that collects personal information from consumers under this title.

(2) (A) A person to whom the business discloses a consumer's personal information for a business purpose pursuant to a written contract, provided that the contract:

(i) Prohibits the person receiving the personal information from:

(I) Selling the personal information.

(II) Retaining, using, or disclosing the personal information for any purpose other than for the specific purpose of performing the services specified in the contract, including retaining, using, or disclosing the personal information for a commercial purpose other than providing the services specified in the contract.

(III) Retaining, using, or disclosing the information outside of the direct business relationship between the person and the business.

(ii) Includes a certification made by the person receiving the personal information that the person understands the restrictions in subparagraph (A) and will comply with them.

(B) A person covered by this paragraph that violates any of the restrictions set forth in this title shall be liable for the violations. A business that discloses personal information to a person covered by this paragraph in compliance with this paragraph shall not be liable under this title if the person receiving the personal information uses it in violation of the restrictions set forth in this title, provided that, at the time of disclosing the personal information, the business does not have actual knowledge, or reason to believe, that the person intends to commit such a violation.

(x) "Unique identifier" or "Unique personal identifier" means a persistent identifier that can be used to recognize a consumer, a family, or a device that is linked to a consumer or family, over time and across different services, including, but not limited to, a device identifier; an Internet Protocol address; cookies, beacons, pixel tags, mobile ad identifiers, or similar technology; customer number, unique pseudonym, or user alias; telephone numbers, or other forms of persistent or probabilistic identifiers that can be used to identify a particular consumer or device. For purposes of this subdivision, "family" means a custodial parent or guardian and any minor children over which the parent or guardian has custody.

(y) "Verifiable 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 paragraph (7) of subdivision (a) of Section 1798.185 to be the consumer about whom the business has collected personal information. A business is not obligated to provide information to the consumer pursuant to Sections 1798.100, 1798.105, 1798.110, and 1798.115 if the business cannot verify, pursuant to this subdivision and regulations adopted by the Attorney General pursuant to paragraph (7) of subdivision (a) of Section 1798.185, that the consumer making the request is the consumer about whom the business has collected information or is a person authorized by the consumer to act on such consumer's behalf.

*(Amended by Stats. 2019, Ch. 757, Sec. 7.5. (AB 1355) Effective January 1, 2020.)*

**1798.145.** (a) The obligations imposed on businesses by this title shall not restrict a business' ability to:

(1) Comply with federal, state, or local laws.

(2) Comply with a civil, criminal, or regulatory inquiry, investigation, subpoena, or summons by federal, state, or local authorities.

(3) Cooperate with law enforcement agencies concerning conduct or activity that the business, service provider, or third party reasonably and in good faith believes may violate federal, state, or local law.

(4) Exercise or defend legal claims.

(5) Collect, use, retain, sell, or disclose consumer information that is deidentified or in the aggregate consumer information.

(6) Collect or sell a consumer's personal information if every aspect of that commercial conduct takes place wholly outside of California. For purposes of this title, commercial conduct takes place wholly outside of California if the business collected that information while the consumer was outside of California, no part of the sale of the consumer's personal information occurred in California, and no personal information collected while the consumer was in California is sold. This paragraph shall not permit a business from storing, including on a device, personal information about a consumer when the consumer is in California and then collecting that personal information when the consumer and stored personal information is outside of California.

(b) The obligations imposed on businesses by Sections 1798.110 to 1798.135, inclusive, shall not apply where compliance by the business with the title would violate an evidentiary privilege under California law and shall not prevent a business from providing the personal information of a consumer to a person covered by an evidentiary privilege under California law as part of a privileged communication.

(c) (1) This title shall not apply to any of the following:

(A) Medical information governed by the Confidentiality of Medical Information Act (Part 2.6 (commencing with Section 56) of Division 1) or protected health information that is collected by a covered entity or business associate governed by the privacy, security, and breach notification rules issued by the United States Department of Health and Human Services, Parts 160 and 164 of Title 45 of the Code of Federal Regulations, established pursuant to the Health Insurance Portability and Accountability Act of 1996 (Public Law 104-191) and the Health Information Technology for Economic and Clinical Health Act (Public Law 111-5).

(B) A provider of health care governed by the Confidentiality of Medical Information Act (Part 2.6 (commencing with Section 56) of Division 1) or a covered entity governed by the privacy, security, and breach notification rules issued by the United States Department of Health and Human Services, Parts 160 and 164 of Title 45 of the Code of Federal Regulations, established pursuant to the Health Insurance Portability and Accountability Act of 1996 (Public Law 104-191), to the extent the provider or covered entity maintains patient information in the same manner as medical information or protected health information as described in subparagraph (A) of this section.

(C) Information collected as part of a clinical trial subject to the Federal Policy for the Protection of Human Subjects, also known as the Common Rule, pursuant to good clinical practice guidelines issued by the International Council for Harmonisation or pursuant to human subject protection requirements of the United States Food and Drug Administration.

(2) For purposes of this subdivision, the definitions of "medical information" and "provider of health care" in Section 56.05 shall apply and the definitions of "business associate," "covered entity," and "protected health information" in Section 160.103 of Title 45 of the Code of Federal Regulations shall apply.

(d) (1) This title shall not apply to an activity involving the collection, maintenance, disclosure, sale, communication, or use of any personal information bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living by a consumer reporting agency, as defined in subdivision (f) of Section 1681a of Title 15 of the United States Code, by a furnisher of information, as set forth in Section 1681s-2 of Title 15 of the United States Code, who provides information for use in a consumer report, as defined in subdivision (d) of Section 1681a of Title 15 of the United States Code, and by a user of a consumer report as set forth in Section 1681b of Title 15 of the United States Code.

(2) Paragraph (1) shall apply only to the extent that such activity involving the collection, maintenance, disclosure, sale, communication, or use of such information by that agency, furnisher, or user is subject to regulation under the Fair Credit Reporting Act, section 1681 et seq., Title 15 of the United States Code and the information is not used, communicated, disclosed, or sold except as authorized by the Fair Credit Reporting Act.

(3) This subdivision shall not apply to Section 1798.150.

(e) This title shall not apply to personal information collected, processed, sold, or disclosed pursuant to the federal Gramm-Leach-Bliley Act (Public Law 106-102), and implementing regulations, or the California Financial Information Privacy Act (Division 1.4 (commencing with Section 4050) of the Financial Code). This subdivision shall not apply to Section 1798.150.

(f) This title shall not apply to personal information collected, processed, sold, or disclosed pursuant to the Driver's Privacy Protection Act of 1994 (18 U.S.C. Sec. 2721 et seq.). This subdivision shall not apply to Section 1798.150.

(g) (1) Section 1798.120 shall not apply to vehicle information or ownership information retained or shared between a new motor vehicle dealer, as defined in Section 426 of the Vehicle Code, and the vehicle's manufacturer, as defined in Section 672 of the Vehicle Code, if the vehicle or ownership information is shared for the purpose of effectuating, or in anticipation of effectuating, a vehicle repair covered by a vehicle warranty or a recall conducted pursuant to Sections 30118 to 30120, inclusive, of Title 49 of the United States Code, provided that the new motor vehicle dealer or vehicle manufacturer with which that vehicle information or ownership information is shared does not sell, share, or use that information for any other purpose.

(2) For purposes of this subdivision:

(A) "Vehicle information" means the vehicle information number, make, model, year, and odometer reading.

(B) "Ownership information" means the name or names of the registered owner or owners and the contact information for the owner or owners.

(h) (1) This title shall not apply to any of the following:

(A) Personal information that is collected by a business about a natural person in the course of the natural person acting as a job applicant to, an employee of, owner of, director of, officer of, medical staff member of, or contractor of that business to the extent that the natural person's personal information is collected and used by the business solely within the context of the natural person's role or former role as a job applicant to, an employee of, owner of, director of, officer of, medical staff member of, or a contractor of that business.

(B) Personal information that is collected by a business that is emergency contact information of the natural person acting as a job applicant to, an employee of, owner of, director of, officer of, medical staff member of, or contractor of that business to the extent that the personal information is collected and used solely within the context of having an emergency contact on file.

(C) Personal information that is necessary for the business to retain to administer benefits for another natural person relating to the natural person acting as a job applicant to, an employee of, owner of, director of, officer of, medical staff member of, or contractor of that business to the extent that the personal information is collected and used solely within the context of administering those benefits.

(2) For purposes of this subdivision:

(A) "Contractor" means a natural person who provides any service to a business pursuant to a written contract.

(B) "Director" means a natural person designated in the articles of incorporation as such or elected by the incorporators and natural persons designated, elected, or appointed by any other name or title to act as directors, and their successors.

(C) "Medical staff member" means a licensed physician and surgeon, dentist, or podiatrist, licensed pursuant to Division 2 (commencing with Section 500) of the Business and Professions Code and a clinical psychologist as defined in Section 1316.5 of the Health and Safety Code.

(D) "Officer" means a natural person elected or appointed by the board of directors to manage the daily operations of a corporation, such as a chief executive officer, president, secretary, or treasurer.

(E) "Owner" means a natural person who meets one of the following:

(i) Has ownership of, or the power to vote, more than 50 percent of the outstanding shares of any class of voting security of a business.

(ii) Has control in any manner over the election of a majority of the directors or of individuals exercising similar functions.

(iii) Has the power to exercise a controlling influence over the management of a company.

(3) This subdivision shall not apply to subdivision (b) of Section 1798.100 or Section 1798.150.

(4) This subdivision shall become inoperative on January 1, 2021.

(i) Notwithstanding a business' obligations to respond to and honor consumer rights requests pursuant to this title:

(1) A time period for a business to respond to any verified consumer request may be extended by up to 90 additional days where necessary, taking into account the complexity and number of the requests. The business shall inform the consumer of any such extension within 45 days of receipt of the request, together with the reasons for the delay.

(2) If the business does not take action on the request of the consumer, the business shall inform the consumer, without delay and at the latest within the time period permitted of response by this section, of the reasons for not taking action and any rights the consumer may have to appeal the decision to the business.

(3) If requests from a consumer are manifestly unfounded or excessive, in particular because of their repetitive character, a business may either charge a reasonable fee, taking into account the administrative costs of providing the information or communication or taking the action requested, or refuse to act on the request and notify the consumer of the reason for refusing the request. The business shall bear the burden of demonstrating that any verified consumer request is manifestly unfounded or excessive.

(j) A business that discloses personal information to a service provider shall not be liable under this title if the service provider receiving the personal information uses it in violation of the restrictions set forth in the title, provided that, at the time of disclosing the personal information, the business does not have actual knowledge, or reason to believe, that the service provider intends to commit such a violation. A service provider shall likewise not be liable under this title for the obligations of a business for which it provides services as set forth in this title.

(k) This title shall not be construed to require a business to collect personal information that it would not otherwise collect in the ordinary course of its business, retain personal information for longer than it would otherwise retain such information in the ordinary course of its business, or reidentify or otherwise link information that is not maintained in a manner that would be considered personal information.

(l) The rights afforded to consumers and the obligations imposed on the business in this title shall not adversely affect the rights and freedoms of other consumers.

(m) The rights afforded to consumers and the obligations imposed on any business under this title shall not apply to the extent that they infringe on the noncommercial activities of a person or entity described in subdivision (b) of Section 2 of Article I of the California Constitution.

(n) (1) The obligations imposed on businesses by Sections 1798.100, 1798.105, 1798.110, 1798.115, 1798.130, and 1798.135 shall not apply to personal information reflecting a written or verbal communication or a transaction between the business and the consumer, where the consumer is a natural person who is acting as an employee, owner, director, officer, or contractor of a company, partnership, sole proprietorship, non-profit, or government agency and whose communications or transaction with the business occur solely within the context of the business conducting due diligence regarding, or providing or receiving a product or service to or from such company, partnership, sole proprietorship, non-profit, or government agency.

(2) For purposes of this subdivision:

(A) "Contractor" means a natural person who provides any service to a business pursuant to a written contract.

(B) "Director" means a natural person designated in the articles of incorporation as such or elected by the incorporators and natural persons designated, elected, or appointed by any other name or title to act as directors, and their successors.

(C) "Officer" means a natural person elected or appointed by the board of directors to manage the daily operations of a corporation, such as a chief executive officer, president, secretary, or treasurer.

(D) "Owner" means a natural person who meets one of the following:

(i) Has ownership of, or the power to vote, more than 50 percent of the outstanding shares of any class of voting security of a business.

(ii) Has control in any manner over the election of a majority of the directors or of individuals exercising similar functions.

(iii) Has the power to exercise a controlling influence over the management of a company.

(3) This subdivision shall become inoperative on January 1, 2021.

*(Amended by Stats. 2019, Ch. 763, Sec. 2.3. (AB 25) Effective January 1, 2020.)*

**1798.150.** (a) (1) Any consumer whose nonencrypted and nonredacted personal information, as defined in subparagraph (A) of paragraph (1) of subdivision (d) of Section 1798.81.5, 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 any of the following:

(A) To recover damages in an amount not less than one hundred dollars (\$100) and not greater than seven hundred and fifty (\$750) per consumer per incident or actual damages, whichever is greater.

(B) Injunctive or declaratory relief.

(C) Any other relief the court deems proper.

(2) In assessing the amount of statutory damages, the court shall consider any one or more of the relevant circumstances presented by any of the parties to the case, including, but not limited to, the nature and seriousness of the misconduct, the number of violations, the persistence of the misconduct, the length of time over which the misconduct occurred, the willfulness of the defendant's misconduct, and the defendant's assets, liabilities, and net worth.

(b) Actions pursuant to this section may be brought by a consumer if, prior to initiating any action against a business for statutory damages on an individual or class-wide basis, a consumer provides a business 30 days' written notice identifying the specific provisions of this title the consumer alleges have been or are being violated. In the event a cure is possible, if within the 30 days the business actually cures the noticed violation and provides the consumer an express written statement that the violations have been cured and that no further violations shall occur, no action for individual statutory damages or class-wide statutory damages may be initiated against the business. No notice shall be required prior to an individual consumer initiating an action solely for actual pecuniary damages suffered as a result of the alleged violations of this title. If a business continues to violate this title in breach of the express written statement provided to the consumer under this section, the consumer may initiate an action against the business to enforce the written statement and may pursue statutory damages for each breach of the express written statement, as well as any other violation of the title that postdates the written statement.

(c) The cause of action established by this section shall apply only to violations as defined in subdivision (a) and shall not be based on violations of any other section of this title. Nothing in this title shall be interpreted to serve as the basis for a private right of action under any other law. This shall not be construed to relieve any party from any duties or obligations imposed under other law or the United States or California Constitution.

*(Amended by Stats. 2019, Ch. 757, Sec. 9. (AB 1355) Effective January 1, 2020.)*

**1798.155.** (a) Any business or third party may seek the opinion of the Attorney General for guidance on how to comply with the provisions of this title.

(b) A business shall be in violation of this title if it fails to cure any alleged violation within 30 days after being notified of alleged noncompliance. Any business, service provider, or other person that violates this title shall be subject to an injunction and liable for a civil penalty of not more than two thousand five hundred dollars (\$2,500) for each violation or seven thousand five hundred dollars (\$7,500) for each intentional violation, which shall be assessed and recovered in a civil action brought in the name of the people of the State of California by the Attorney General. The civil penalties provided for in this section shall be exclusively assessed and recovered in a civil action brought in the name of the people of the State of California by the Attorney General.

(c) Any civil penalty assessed for a violation of this title, and the proceeds of any settlement of an action brought pursuant to subdivision (b), shall be deposited in the Consumer Privacy Fund, created within the General Fund pursuant to subdivision (a) of Section 1798.160 with the intent to fully offset any costs incurred by the state courts and the Attorney General in connection with this title.

*(Amended (as added by Stats. 2018, Ch. 55, Sec. 3) by Stats. 2018, Ch. 735, Sec. 12. (SB 1121) Effective September 23, 2018. Section operative January 1, 2020, pursuant to Section 1798.198.)*

**1798.160.** (a) A special fund to be known as the "Consumer Privacy Fund" is hereby created within the General Fund in the State Treasury, and is available upon appropriation by the Legislature to offset any costs incurred by the state courts in connection with actions brought to enforce this title and any costs incurred by the Attorney General in carrying out the Attorney General's duties under this title.

(b) Funds transferred to the Consumer Privacy Fund shall be used exclusively to offset any costs incurred by the state courts and the Attorney General in connection with this title. These funds shall not be subject to appropriation or transfer by the Legislature for any other purpose, unless the Director of Finance determines that the funds are in excess of the funding needed to fully offset the costs incurred by the state courts and the Attorney General in connection with this title, in which case the Legislature may appropriate excess funds for other purposes.

*(Added by Stats. 2018, Ch. 55, Sec. 3. (AB 375) Effective January 1, 2019. Section operative January 1, 2020, pursuant to Section 1798.198.)*

**1798.175.** 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 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.

*(Added by Stats. 2018, Ch. 55, Sec. 3. (AB 375) Effective January 1, 2019. Section operative January 1, 2020, pursuant to Section 1798.198.)*

**1798.180.** This title is a matter of statewide concern and supersedes and preempts all rules, regulations, codes, ordinances, and other laws adopted by a city, county, city and county, municipality, or local agency regarding the collection and sale of consumers' personal information by a business.

*(Added by Stats. 2018, Ch. 55, Sec. 3. (AB 375) Effective January 1, 2019. Section operative September 23, 2018, pursuant to Section 1798.199.)*

**1798.185.** (a) On or before July 1, 2020, the Attorney General shall solicit broad public participation and adopt regulations to further the purposes of this title, including, but not limited to, the following areas:

(1) Updating as needed additional categories of personal information to those enumerated in subdivision (c) of Section 1798.130 and subdivision (o) of Section 1798.140 in order to address changes in technology, data collection practices, obstacles to implementation, and privacy concerns.

(2) Updating as needed the definition of unique identifiers to address changes in technology, data collection, obstacles to implementation, and privacy concerns, and additional categories to the definition of designated methods for submitting requests to facilitate a consumer's ability to obtain information from a business pursuant to Section 1798.130.

(3) Establishing any exceptions necessary to comply with state or federal law, including, but not limited to, those relating to trade secrets and intellectual property rights, within one year of passage of this title and as needed thereafter.

(4) Establishing rules and procedures for the following:

(A) To facilitate and govern the submission of a request by a consumer to opt-out of the sale of personal information pursuant to Section 1798.120.

(B) To govern business compliance with a consumer's opt-out request.

(C) For the development and use of a recognizable and uniform opt-out logo or button by all businesses to promote consumer awareness of the opportunity to opt-out of the sale of personal information.

(5) Adjusting the monetary threshold in subparagraph (A) of paragraph (1) of subdivision (c) of Section 1798.140 in January of every odd-numbered year to reflect any increase in the Consumer Price Index.

(6) Establishing rules, procedures, and any exceptions necessary to ensure that the notices and information that businesses are required to provide pursuant to this title are provided in a manner that may be easily understood by the average consumer, are accessible to consumers with disabilities, and are available in the language primarily used to interact with the consumer, including establishing rules and guidelines regarding financial incentive offerings, within one year of passage of this title and as needed thereafter.

(7) Establishing rules and procedures to further the purposes of Sections 1798.110 and 1798.115 and to facilitate a consumer's or the consumer's authorized agent's ability to obtain information pursuant to Section 1798.130, with the goal of minimizing the administrative burden on consumers, taking into account available technology, security concerns, and the burden on the business, to govern a business's determination that a request for information received from a consumer is a verifiable consumer request, including treating a request submitted through a password-protected account maintained by the consumer with the business while the consumer is logged into the account as a verifiable consumer request and providing a mechanism for a consumer who does not maintain an account with the business to request information through the business's authentication of the consumer's identity, within one year of passage of this title and as needed thereafter.

(b) The Attorney General may adopt additional regulations as follows:

(1) To establish rules and procedures on how to process and comply with verifiable consumer requests for specific pieces of personal information relating to a household in order to address obstacles to implementation and privacy concerns.

(2) As necessary to further the purposes of this title.

(c) The Attorney General shall not bring an enforcement action under this title until six months after the publication of the final regulations issued pursuant to this section or July 1, 2020, whichever is sooner.

*(Amended by Stats. 2019, Ch. 757, Sec. 10. (AB 1355) Effective January 1, 2020.)*

**1798.190.** If a series of steps or transactions were component parts of a single transaction intended from the beginning to be taken with the intention of avoiding the reach of this title, including the disclosure of information by a business to a third party in order to avoid the definition of sell, a court shall disregard the intermediate steps or transactions for purposes of effectuating the purposes of this title.

*(Added by Stats. 2018, Ch. 55, Sec. 3. (AB 375) Effective January 1, 2019. Section operative January 1, 2020, pursuant to Section 1798.198.)*

**1798.192.** Any provision of a contract or agreement of any kind that purports to waive or limit in any way a consumer's rights under this title, including, but not limited to, any right to a remedy or means of enforcement, shall be deemed contrary to public policy and shall be void and unenforceable. This section shall not prevent a consumer from declining to request information from a business, declining to opt-out of a business's sale of the consumer's personal information, or authorizing a business to sell the consumer's personal information after previously opting out.

*(Amended (as added by Stats. 2018, Ch. 55, Sec. 3) by Stats. 2018, Ch. 735, Sec. 14. (SB 1121) Effective September 23, 2018. Section operative January 1, 2020, pursuant to Section 1798.198.)*

**1798.194.** This title shall be liberally construed to effectuate its purposes.

*(Added by Stats. 2018, Ch. 55, Sec. 3. (AB 375) Effective January 1, 2019. Section operative January 1, 2020, pursuant to Section 1798.198.)*

**1798.196.** This title is intended to supplement federal and state law, if permissible, but shall not apply if such application is preempted by, or in conflict with, federal law or the United States or California Constitution.

*(Amended (as added by Stats. 2018, Ch. 55, Sec. 3) by Stats. 2018, Ch. 735, Sec. 15. (SB 1121) Effective September 23, 2018. Section operative January 1, 2020, pursuant to Section 1798.198.)*

**1798.198.** (a) Subject to limitation provided in subdivision (b), and in Section 1798.199, this title shall be operative January 1, 2020.

(b) This title shall become operative only if initiative measure No. 17-0039, The Consumer Right to Privacy Act of 2018, is withdrawn from the ballot pursuant to Section 9604 of the Elections Code.

*(Amended (as added by Stats. 2018, Ch. 55, Sec. 3) by Stats. 2018, Ch. 735, Sec. 16. (SB 1121) Effective September 23, 2018.)*

**1798.199.** Notwithstanding Section 1798.198, Section 1798.180 shall be operative on the effective date of the act adding this section.

*(Added by Stats. 2018, Ch. 735, Sec. 17. (SB 1121) Effective September 23, 2018. Operative September 23, 2018.)*



# Appendix F

California Office of the Attorney General

CHAPTER 20. CALIFORNIA CONSUMER PRIVACY ACT REGULATIONS (Aug.  
14, 2020)

# FINAL TEXT OF PROPOSED REGULATIONS

## TITLE 11. LAW

### DIVISION 1. ATTORNEY GENERAL

#### **CHAPTER 20. CALIFORNIA CONSUMER PRIVACY ACT REGULATIONS**

##### **Article 1. GENERAL PROVISIONS**

###### **§ 999.300. Title and Scope.**

- (a) This Chapter shall be known as the California Consumer Privacy Act Regulations. It may be cited as such and will be referred to in this Chapter as “these regulations.” These regulations govern compliance with the California Consumer Privacy Act and do not limit any other rights that consumers may have.
- (b) A violation of these regulations shall constitute a violation of the CCPA and be subject to the remedies provided for therein.

*Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.100, 1798.105, 1798.110, 1798.115, 1798.120, 1798.125, 1798.130, 1798.135, 1798.140, 1798.145, 1798.150, 1798.155 and 1798.185, Civil Code.*

###### **§ 999.301. Definitions.**

In addition to the definitions set forth in Civil Code section 1798.140, for purposes of these regulations:

- (a) “Affirmative authorization” means an action that demonstrates the intentional decision by the consumer to opt-in to the sale of personal information. Within the context of a parent or guardian acting on behalf of a consumer under 13 years of age, it means that the parent or guardian has provided consent to the sale of the consumer’s personal information in accordance with the methods set forth in section 999.330. For consumers 13 years of age and older, it is demonstrated through a two-step process whereby the consumer shall first, clearly request to opt-in and then second, separately confirm their choice to opt-in.
- (b) “Attorney General” means the California Attorney General or any officer or employee of the California Department of Justice acting under the authority of the California Attorney General.
- (c) “Authorized agent” means a natural person or a business entity registered with the Secretary of State to conduct business in California that a consumer has authorized to act on their behalf subject to the requirements set forth in section 999.326.
- (d) “Categories of sources” means types or groupings of persons or entities from which a business collects personal information about consumers, described with enough particularity to provide consumers with a meaningful understanding of the type of person or entity. They

may include the consumer directly, advertising networks, internet service providers, data analytics providers, government entities, operating systems and platforms, social networks, and data brokers.

- (e) “Categories of third parties” means types or groupings of third parties with whom the business shares personal information, described with enough particularity to provide consumers with a meaningful understanding of the type of third party. They may include advertising networks, internet service providers, data analytics providers, government entities, operating systems and platforms, social networks, and data brokers.
- (f) “CCPA” means the California Consumer Privacy Act of 2018, Civil Code sections 1798.100 *et seq.*
- (g) “COPPA” means the Children’s Online Privacy Protection Act, 15 U.S.C. sections 6501 to 6508 and 16 Code of Federal Regulations part 312.5.
- (h) “Employment benefits” means retirement, health, and other benefit programs, services, or products to which consumers and their dependents or their beneficiaries receive access through the consumer’s employer.
- (i) “Employment-related information” means personal information that is collected by the business about a natural person for the reasons identified in Civil Code section 1798.145, subdivision (h)(1). The collection of employment-related information, including for the purpose of administering employment benefits, shall be considered a business purpose.
- (j) “Financial incentive” means a program, benefit, or other offering, including payments to consumers, related to the collection, deletion, or sale of personal information.
- (k) “Household” means a person or group of people who: (1) reside at the same address, (2) share a common device or the same service provided by a business, and (3) are identified by the business as sharing the same group account or unique identifier.
- (l) “Notice at collection” means the notice given by a business to a consumer at or before the point at which a business collects personal information from the consumer as required by Civil Code section 1798.100, subdivision (b), and specified in these regulations.
- (m) “Notice of right to opt-out” means the notice given by a business informing consumers of their right to opt-out of the sale of their personal information as required by Civil Code sections 1798.120 and 1798.135 and specified in these regulations.
- (n) “Notice of financial incentive” means the notice given by a business explaining each financial incentive or price or service difference as required by Civil Code section 1798.125, subdivision (b), and specified in these regulations.
- (o) “Price or service difference” means (1) any difference in the price or rate charged for any goods or services to any consumer related to the collection, retention, or sale of personal information, including through the use of discounts, financial payments, or other benefits or penalties; or (2) any difference in the level or quality of any goods or services offered to any consumer related to the collection, retention, or sale of personal information, including the denial of goods or services to the consumer.

- (p) “Privacy policy,” as referred to in Civil Code section 1798.130, subdivision (a)(5), means the statement that a business shall make available to consumers describing the business’s practices, both online and offline, regarding the collection, use, disclosure, and sale of personal information, and of the rights of consumers regarding their own personal information.
- (q) “Request to delete” means a consumer request that a business delete personal information about the consumer that the business has collected from the consumer, pursuant to Civil Code section 1798.105.
- (r) “Request to know” means a consumer request that a business disclose personal information that it has collected about the consumer pursuant to Civil Code sections 1798.100, 1798.110, or 1798.115. It includes a request for any or all of the following:
- (1) Specific pieces of personal information that a business has collected about the consumer;
  - (2) Categories of personal information it has collected about the consumer;
  - (3) Categories of sources from which the personal information is collected;
  - (4) Categories of personal information that the business sold or disclosed for a business purpose about the consumer;
  - (5) Categories of third parties to whom the personal information was sold or disclosed for a business purpose; and
  - (6) The business or commercial purpose for collecting or selling personal information.
- (s) “Request to opt-in” means the affirmative authorization that the business may sell personal information about the consumer by a parent or guardian of a consumer less than 13 years of age, by a consumer at least 13 and less than 16 years of age, or by a consumer who had previously opted out of the sale of their personal information.
- (t) “Request to opt-out” means a consumer request that a business not sell the consumer’s personal information to third parties, pursuant to Civil Code section 1798.120, subdivision (a).
- (u) “Signed” means that the written attestation, declaration, or permission has either been physically signed or provided electronically in accordance with the Uniform Electronic Transactions Act, Civil Code section 1633.1 et seq.
- (v) “Third-party identity verification service” means a security process offered by an independent third party that verifies the identity of the consumer making a request to the business. Third-party identity verification services are subject to the requirements set forth in Article 4 regarding requests to know and requests to delete.
- (w) “Value of the consumer’s data” means the value provided to the business by the consumer’s data as calculated under section 999.337.

- (x) “Verify” means to determine that the consumer making a request to know or request to delete is the consumer about whom the business has collected information, or if that consumer is less than 13 years of age, the consumer’s parent or legal guardian.

*Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.100, 1798.105, 1798.110, 1798.115, 1798.120, 1798.125, 1798.130, 1798.135, 1798.140, 1798.145 and 1798.185, Civil Code.*

## **Article 2. NOTICES TO CONSUMERS**

### **§ 999.304. Overview of Required Notices.**

- (a) Every business that must comply with the CCPA and these regulations shall provide a privacy policy in accordance with the CCPA and section 999.308.
- (b) A business that collects personal information from a consumer shall provide a notice at collection in accordance with the CCPA and section 999.305.
- (c) A business that sells personal information shall provide a notice of right to opt-out in accordance with the CCPA and section 999.306.
- (d) A business that offers a financial incentive or price or service difference shall provide a notice of financial incentive in accordance with the CCPA and section 999.307.

*Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.100, 1798.105, 1798.115, 1798.120, 1798.125, 1798.130 and 1798.135, Civil Code.*

### **§ 999.305. Notice at Collection of Personal Information.**

#### **(a) Purpose and General Principles**

- (1) The purpose of the notice at collection is to provide consumers with timely notice, at or before the point of collection, about the categories of personal information to be collected from them and the purposes for which the personal information will be used.
- (2) The notice at collection shall be designed and presented in a way that is easy to read and understandable to consumers. The notice shall:
- a. Use plain, straightforward language and avoid technical or legal jargon.
  - b. Use a format that draws the consumer’s attention to the notice and makes the notice readable, including on smaller screens, if applicable.
  - c. Be available in the languages in which the business in its ordinary course provides contracts, disclaimers, sale announcements, and other information to consumers in California.
  - d. Be reasonably accessible to consumers with disabilities. For notices provided online, the business shall follow generally recognized industry standards, such as the Web Content Accessibility Guidelines, version 2.1 of June 5, 2018, from the World Wide Web Consortium, incorporated herein by reference. In other

contexts, the business shall provide information on how a consumer with a disability may access the notice in an alternative format.

(3) The notice at collection shall be made readily available where consumers will encounter it at or before the point of collection of any personal information.

Illustrative examples follow:

- a. When a business collects consumers' personal information online, it may post a conspicuous link to the notice on the introductory page of the business's website and on all webpages where personal information is collected.
  - b. When a business collects personal information through a mobile application, it may provide a link to the notice on the mobile application's download page and within the application, such as through the application's settings menu.
  - c. When a business collects consumers' personal information offline, it may include the notice on printed forms that collect personal information, provide the consumer with a paper version of the notice, or post prominent signage directing consumers to where the notice can be found online.
  - d. When a business collects personal information over the telephone or in person, it may provide the notice orally.
- (4) When a business collects personal information from a consumer's mobile device for a purpose that the consumer would not reasonably expect, it shall provide a just-in-time notice containing a summary of the categories of personal information being collected and a link to the full notice at collection. For example, if the business offers a flashlight application and the application collects geolocation information, the business shall provide a just-in-time notice, such as through a pop-up window when the consumer opens the application, that contains the information required by this subsection.
- (5) A business shall not collect categories of personal information other than those disclosed in the notice at collection. If the business intends to collect additional categories of personal information, the business shall provide a new notice at collection.
- (6) If a business does not give the notice at collection to the consumer at or before the point of collection of their personal information, the business shall not collect personal information from the consumer.

(b) A business shall include the following in its notice at collection:

- (1) A list of the categories of personal information about consumers to be collected. Each category of personal information shall be written in a manner that provides consumers a meaningful understanding of the information being collected.
- (2) The business or commercial purpose(s) for which the categories of personal information will be used.

- (3) If the business sells personal information, the link titled “Do Not Sell My Personal Information” required by section 999.315, subsection (a), or in the case of offline notices, where the webpage can be found online.
  - (4) A link to the business’s privacy policy, or in the case of offline notices, where the privacy policy can be found online.
- (c) If a business collects personal information from a consumer online, the notice at collection may be given to the consumer by providing a link to the section of the business’s privacy policy that contains the information required in subsection (b).
- (d) A business that does not collect personal information directly from the consumer does not need to provide a notice at collection to the consumer if it does not sell the consumer’s personal information.
- (e) A data broker registered with the Attorney General pursuant to Civil Code section 1798.99.80 *et seq.* does not need to provide a notice at collection to the consumer if it has included in its registration submission a link to its online privacy policy that includes instructions on how a consumer can submit a request to opt-out.
- (f) A business collecting employment-related information shall comply with the provisions of section 999.305 except with regard to the following:
  - (1) The notice at collection of employment-related information does not need to include the link or web address to the link titled “Do Not Sell My Personal Information”.
  - (2) The notice at collection of employment-related information is not required to provide a link to the business’s privacy policy.
- (g) Subsection (f) shall become inoperative on January 1, 2021, unless the CCPA is amended otherwise.

*Note: Authority: Section 1798.185, Civil Code. Reference: Sections 1798.99.82, 1798.100, 1798.115 and 1798.185, Civil Code.*

### **§ 999.306. Notice of Right to Opt-Out of Sale of Personal Information.**

#### **(a) Purpose and General Principles**

- (1) The purpose of the notice of right to opt-out is to inform consumers of their right to direct a business that sells their personal information to stop selling their personal information.
- (2) The notice of right to opt-out shall be designed and presented in a way that is easy to read and understandable to consumers. The notice shall:
  - a. Use plain, straightforward language and avoid technical or legal jargon.
  - b. Use a format that draws the consumer’s attention to the notice and makes the notice readable, including on smaller screens, if applicable.

- c. Be available in the languages in which the business in its ordinary course provides contracts, disclaimers, sale announcements, and other information to consumers in California.
  - d. Be reasonably accessible to consumers with disabilities. For notices provided online, the business shall follow generally recognized industry standards, such as the Web Content Accessibility Guidelines, version 2.1 of June 5, 2018, from the World Wide Web Consortium, incorporated herein by reference. In other contexts, the business shall provide information on how a consumer with a disability may access the notice in an alternative format.
- (b) A business that sells the personal information of consumers shall provide the notice of right to opt-out to consumers as follows:
  - (1) A business shall post the notice of right to opt-out on the Internet webpage to which the consumer is directed after clicking on the “Do Not Sell My Personal Information” link on the website homepage or the download or landing page of a mobile application. In addition, a business that collects personal information through a mobile application may provide a link to the notice within the application, such as through the application’s settings menu. The notice shall include the information specified in subsection (c) or link to the section of the business’s privacy policy that contains the same information.
  - (2) A business that does not operate a website shall establish, document, and comply with another method by which it informs consumers of their right to opt-out. That method shall comply with the requirements set forth in subsection (a)(2).
- (c) A business shall include the following in its notice of right to opt-out:
  - (1) A description of the consumer’s right to opt-out of the sale of their personal information by the business;
  - (2) The interactive form by which the consumer can submit their request to opt-out online, as required by section 999.315, subsection (a), or if the business does not operate a website, the offline method by which the consumer can submit their request to opt-out; and
  - (3) Instructions for any other method by which the consumer may submit their request to opt-out.
- (d) A business does not need to provide a notice of right to opt-out if:
  - (1) It does not sell personal information; and
  - (2) It states in its privacy policy that it does not sell personal information.
- (e) A business shall not sell the personal information it collected during the time the business did not have a notice of right to opt-out posted unless it obtains the affirmative authorization of the consumer.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.120, 1798.135 and 1798.185, Civil Code.

### **§ 999.307. Notice of Financial Incentive.**

#### **(a) Purpose and General Principles**

- (1) The purpose of the notice of financial incentive is to explain to the consumer the material terms of a financial incentive or price or service difference the business is offering so that the consumer may make an informed decision about whether to participate. A business that does not offer a financial incentive or price or service difference is not required to provide a notice of financial incentive.
- (2) The notice of financial incentive shall be designed and presented in a way that is easy to read and understandable to consumers. The notice shall:
  - a. Use plain, straightforward language and avoid technical or legal jargon.
  - b. Use a format that draws the consumer's attention to the notice and makes the notice readable, including on smaller screens, if applicable.
  - c. Be available in the languages in which the business in its ordinary course provides contracts, disclaimers, sale announcements, and other information to consumers in California.
  - d. Be reasonably accessible to consumers with disabilities. For notices provided online, the business shall follow generally recognized industry standards, such as the Web Content Accessibility Guidelines, version 2.1 of June 5, 2018, from the World Wide Web Consortium, incorporated herein by reference. In other contexts, the business shall provide information on how a consumer with a disability may access the notice in an alternative format.
  - e. Be readily available where consumers will encounter it before opting-in to the financial incentive or price or service difference.
- (3) If the business offers the financial incentive or price or service difference online, the notice may be given by providing a link to the section of a business's privacy policy that contains the information required in subsection (b).

#### **(b) A business shall include the following in its notice of financial incentive:**

- (1) A succinct summary of the financial incentive or price or service difference offered;
- (2) A description of the material terms of the financial incentive or price or service difference, including the categories of personal information that are implicated by the financial incentive or price or service difference and the value of the consumer's data;
- (3) How the consumer can opt-in to the financial incentive or price or service difference;
- (4) A statement of the consumer's right to withdraw from the financial incentive at any time and how the consumer may exercise that right; and
- (5) An explanation of how the financial incentive or price or service difference is reasonably related to the value of the consumer's data, including:

- a. A good-faith estimate of the value of the consumer's data that forms the basis for offering the financial incentive or price or service difference; and
- b. A description of the method the business used to calculate the value of the consumer's data.

*Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.125 and 1798.130, Civil Code.*

### **§ 999.308. Privacy Policy.**

#### **(a) Purpose and General Principles**

- (1) The purpose of the privacy policy is to provide consumers with a comprehensive description of a business's online and offline practices regarding the collection, use, disclosure, and sale of personal information and of the rights of consumers regarding their personal information.
- (2) The privacy policy shall be designed and presented in a way that is easy to read and understandable to consumers. The policy shall:
  - a. Use plain, straightforward language and avoid technical or legal jargon.
  - b. Use a format that makes the policy readable, including on smaller screens, if applicable.
  - c. Be available in the languages in which the business in its ordinary course provides contracts, disclaimers, sale announcements, and other information to consumers in California.
  - d. Be reasonably accessible to consumers with disabilities. For notices provided online, the business shall follow generally recognized industry standards, such as the Web Content Accessibility Guidelines, version 2.1 of June 5, 2018, from the World Wide Web Consortium, incorporated herein by reference. In other contexts, the business shall provide information on how a consumer with a disability may access the policy in an alternative format.
  - e. Be available in a format that allows a consumer to print it out as a document.
- (b) The privacy policy shall be posted online through a conspicuous link using the word "privacy" on the business's website homepage or on the download or landing page of a mobile application. If the business has a California-specific description of consumers' privacy rights on its website, then the privacy policy shall be included in that description. A business that does not operate a website shall make the privacy policy conspicuously available to consumers. A mobile application may include a link to the privacy policy in the application's settings menu.
- (c) The privacy policy shall include the following information:
  - (1) Right to Know About Personal Information Collected, Disclosed, or Sold.

- a. Explanation that a consumer has the right to request that the business disclose what personal information it collects, uses, discloses, and sells.
- b. Instructions for submitting a verifiable consumer request to know and links to an online request form or portal for making the request, if offered by the business.
- c. General description of the process the business will use to verify the consumer request, including any information the consumer must provide.
- d. Identification of the categories of personal information the business has collected about consumers in the preceding 12 months. The categories shall be described in a manner that provides consumers a meaningful understanding of the information being collected.
- e. Identification of the categories of sources from which the personal information is collected.
- f. Identification of the business or commercial purpose for collecting or selling personal information. The purpose shall be described in a manner that provides consumers a meaningful understanding of why the information is collected or sold.
- g. Disclosure or Sale of Personal Information.
  - 1. Identification of the categories of personal information, if any, that the business has disclosed for a business purpose or sold to third parties in the preceding 12 months.
  - 2. For each category of personal information identified, the categories of third parties to whom the information was disclosed or sold.
  - 3. Statement regarding whether the business has actual knowledge that it sells the personal information of consumers under 16 years of age.

(2) Right to Request Deletion of Personal Information.

- a. Explanation that the consumer has a right to request the deletion of their personal information collected by the business.
- b. Instructions for submitting a verifiable consumer request to delete and links to an online request form or portal for making the request, if offered by the business.
- c. General description of the process the business will use to verify the consumer request, including any information the consumer must provide.

(3) Right to Opt-Out of the Sale of Personal Information.

- a. Explanation that the consumer has a right to opt-out of the sale of their personal information by a business.
- b. Statement regarding whether or not the business sells personal information. If the business sells personal information, include either the contents of the notice of right to opt-out or a link to it in accordance with section 999.306.

- (4) Right to Non-Discrimination for the Exercise of a Consumer's Privacy Rights.
  - a. Explanation that the consumer has a right not to receive discriminatory treatment by the business for the exercise of the privacy rights conferred by the CCPA.
- (5) Authorized Agent.
  - a. Instructions on how an authorized agent can make a request under the CCPA on the consumer's behalf.
- (6) Contact for More Information.
  - a. A contact for questions or concerns about the business's privacy policies and practices using a method reflecting the manner in which the business primarily interacts with the consumer.
- (7) Date the privacy policy was last updated.
- (8) If subject to the requirements set forth in section 999.317, subsection (g), the information compiled in section 999.317, subsection (g)(1), or a link to it.
- (9) If the business has actual knowledge that it sells the personal information of consumers under 16 years of age, a description of the processes required by sections 999.330 and 999.331.

*Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.105, 1798.115, 1798.120, 1798.125 and 1798.130, Civil Code.*

### **Article 3. BUSINESS PRACTICES FOR HANDLING CONSUMER REQUESTS**

#### **§ 999.312. Methods for Submitting Requests to Know and Requests to Delete.**

- (a) A business that operates exclusively online and has a direct relationship with a consumer from whom it collects personal information shall only be required to provide an email address for submitting requests to know. All other businesses shall provide two or more designated methods for submitting requests to know, including, at a minimum, a toll-free telephone number. Other acceptable methods for submitting these requests include, but are not limited to, a designated email address, a form submitted in person, and a form submitted through the mail.
- (b) A business shall provide two or more designated methods for submitting requests to delete. Acceptable methods for submitting these requests include, but are not limited to, a toll-free phone number, a link or form available online through a business's website, a designated email address, a form submitted in person, and a form submitted through the mail.
- (c) A business shall consider the methods by which it primarily interacts with consumers when determining which methods to provide for submitting requests to know and requests to delete. If the business interacts with consumers in person, the business shall consider providing an in-person method such as a printed form the consumer can directly submit or send by mail, a tablet or computer portal that allows the consumer to complete and submit

an online form, or a telephone with which the consumer can call the business's toll-free number.

- (d) A business may use a two-step process for online requests to delete where the consumer must first, submit the request to delete and then second, separately confirm that they want their personal information deleted.
- (e) If a consumer submits a request in a manner that is not one of the designated methods of submission, or is deficient in some manner unrelated to the verification process, the business shall either:
  - (1) Treat the request as if it had been submitted in accordance with the business's designated manner, or
  - (2) Provide the consumer with information on how to submit the request or remedy any deficiencies with the request, if applicable.

*Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.100, 1798.105, 1798.110, 1798.115, 1798.130, 1798.140 and 1798.185, Civil Code.*

### **§ 999.313. Responding to Requests to Know and Requests to Delete.**

- (a) Upon receiving a request to know or a request to delete, a business shall confirm receipt of the request within 10 business days and provide information about how the business will process the request. The information provided shall describe in general the business's verification process and when the consumer should expect a response, except in instances where the business has already granted or denied the request. The confirmation may be given in the same manner in which the request was received. For example, if the request is made over the phone, the confirmation may be given orally during the phone call.
- (b) Businesses shall respond to requests to know and requests to delete within 45 calendar days. The 45-day period will begin on the day that the business receives the request, regardless of time required to verify the request. If the business cannot verify the consumer within the 45-day time period, the business may deny the request. If necessary, businesses may take up to an additional 45 calendar days to respond to the consumer's request, for a maximum total of 90 calendar days from the day the request is received, provided that the business provides the consumer with notice and an explanation of the reason that the business will take more than 45 days to respond to the request.
- (c) Responding to Requests to Know.
  - (1) For requests that seek the disclosure of specific pieces of information about the consumer, if a business cannot verify the identity of the person making the request pursuant to the regulations set forth in Article 4, the business shall not disclose any specific pieces of personal information to the requestor and shall inform the requestor that it cannot verify their identity. If the request is denied in whole or in part, the business shall also evaluate the consumer's request as if it is seeking the disclosure of categories of personal information about the consumer pursuant to subsection (c)(2).

- (2) For requests that seek the disclosure of categories of personal information about the consumer, if a business cannot verify the identity of the person making the request pursuant to the regulations set forth in Article 4, the business may deny the request to disclose the categories and other information requested and shall inform the requestor that it cannot verify their identity. If the request is denied in whole or in part, the business shall provide or direct the consumer to its general business practices regarding the collection, maintenance, and sale of personal information set forth in its privacy policy.
- (3) In responding to a request to know, a business is not required to search for personal information if all of the following conditions are met:
- a. The business does not maintain the personal information in a searchable or reasonably accessible format;
  - b. The business maintains the personal information solely for legal or compliance purposes;
  - c. The business does not sell the personal information and does not use it for any commercial purpose; and
  - d. The business describes to the consumer the categories of records that may contain personal information that it did not search because it meets the conditions stated above.
- (4) A business shall not disclose in response to a request to know a consumer's Social Security number, driver's license number or other government-issued identification number, financial account number, any health insurance or medical identification number, an account password, security questions and answers, or unique biometric data generated from measurements or technical analysis of human characteristics. The business shall, however, inform the consumer with sufficient particularity that it has collected the type of information. For example, a business shall respond that it collects "unique biometric data including a fingerprint scan" without disclosing the actual fingerprint scan data.
- (5) If a business denies a consumer's verified request to know specific pieces of personal information, in whole or in part, because of a conflict with federal or state law, or an exception to the CCPA, the business shall inform the requestor and explain the basis for the denial, unless prohibited from doing so by law. If the request is denied only in part, the business shall disclose the other information sought by the consumer.
- (6) A business shall use reasonable security measures when transmitting personal information to the consumer.
- (7) If a business maintains a password-protected account with the consumer, it may comply with a request to know by using a secure self-service portal for consumers to access, view, and receive a portable copy of their personal information if the portal

fully discloses the personal information that the consumer is entitled to under the CCPA and these regulations, uses reasonable data security controls, and complies with the verification requirements set forth in Article 4.

(8) Unless otherwise specified by the business to cover a longer period of time, the 12-month period covered by a consumer's verifiable request to know referenced in Civil Code section 1798.130, subdivision (a)(2), shall run from the date the business receives the request, regardless of the time required to verify the request.

(9) In responding to a consumer's verified request to know categories of personal information, categories of sources, and/or categories of third parties, a business shall provide an individualized response to the consumer as required by the CCPA. It shall not refer the consumer to the businesses' general practices outlined in its privacy policy unless its response would be the same for all consumers and the privacy policy discloses all the information that is otherwise required to be in a response to a request to know such categories.

(10) In responding to a verified request to know categories of personal information, the business shall provide:

- a. The categories of personal information the business has collected about the consumer in the preceding 12 months;
- b. The categories of sources from which the personal information was collected;
- c. The business or commercial purpose for which it collected or sold the personal information;
- d. The categories of third parties with whom the business shares personal information;
- e. The categories of personal information that the business sold in the preceding 12 months, and for each category identified, the categories of third parties to whom it sold that particular category of personal information; and
- f. The categories of personal information that the business disclosed for a business purpose in the preceding 12 months, and for each category identified, the categories of third parties to whom it disclosed that particular category of personal information.

(11) A business shall identify the categories of personal information, categories of sources of personal information, and categories of third parties to whom a business sold or disclosed personal information, in a manner that provides consumers a meaningful understanding of the categories listed.

(d) Responding to Requests to Delete.

- (1) For requests to delete, if a business cannot verify the identity of the requestor pursuant to the regulations set forth in Article 4, the business may deny the request to delete. The business shall inform the requestor that their identity cannot be verified.
- (2) A business shall comply with a consumer's request to delete their personal information by:

  - a. Permanently and completely erasing the personal information on its existing systems with the exception of archived or back-up systems;
  - b. Deidentifying the personal information; or
  - c. Aggregating the consumer information.
- (3) If a business stores any personal information on archived or backup systems, it may delay compliance with the consumer's request to delete, with respect to data stored on the archived or backup system, until the archived or backup system relating to that data is restored to an active system or next accessed or used for a sale, disclosure, or commercial purpose.
- (4) In responding to a request to delete, a business shall inform the consumer whether or not it has complied with the consumer's request.
- (5) If the business complies with the consumer's request, the business shall inform the consumer that it will maintain a record of the request as required by section 999.317, subsection (b). A business may retain a record of the request for the purpose of ensuring that the consumer's personal information remains deleted from the business's records.
- (6) In cases where a business denies a consumer's request to delete, the business shall do all of the following:

  - a. Inform the consumer that it will not comply with the consumer's request and describe the basis for the denial, including any conflict with federal or state law, or exception to the CCPA, unless prohibited from doing so by law;
  - b. Delete the consumer's personal information that is not subject to the exception; and
  - c. Not use the consumer's personal information retained for any other purpose than provided for by that exception.
- (7) If a business that denies a consumer's request to delete sells personal information and the consumer has not already made a request to opt-out, the business shall ask the consumer if they would like to opt-out of the sale of their personal information and

shall include either the contents of, or a link to, the notice of right to opt-out in accordance with section 999.306.

- (8) In responding to a request to delete, a business may present the consumer with the choice to delete select portions of their personal information only if a global option to delete all personal information is also offered and more prominently presented than the other choices.

*Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.100, 1798.105, 1798.110, 1798.115, 1798.130 and 1798.185, Civil Code.*

#### **§ 999.314. Service Providers.**

- (a) A business that provides services to a person or organization that is not a business, and that would otherwise meet the requirements and obligations of a “service provider” under the CCPA and these regulations, shall be deemed a service provider for purposes of the CCPA and these regulations.
- (b) To the extent that a business directs a second entity to collect personal information directly from a consumer, or about a consumer, on the first business’s behalf, and the second entity would otherwise meet the requirements and obligations of a “service provider” under the CCPA and these regulations, the second entity shall be deemed a service provider of the first business for purposes of the CCPA and these regulations.
- (c) A service provider shall not retain, use, or disclose personal information obtained in the course of providing services except:
- (1) To process or maintain personal information on behalf of the business that provided the personal information or directed the service provider to collect the personal information, and in compliance with the written contract for services required by the CCPA;
  - (2) To retain and employ another service provider as a subcontractor, where the subcontractor meets the requirements for a service provider under the CCPA and these regulations;
  - (3) For internal use by the service provider to build or improve the quality of its services, provided that the use does not include building or modifying household or consumer profiles to use in providing services to another business, or correcting or augmenting data acquired from another source;
  - (4) To detect data security incidents or protect against fraudulent or illegal activity; or
  - (5) For the purposes enumerated in Civil Code section 1798.145, subdivisions (a)(1) through (a)(4).
- (d) A service provider shall not sell data on behalf of a business when a consumer has opted-out of the sale of their personal information with the business.

- (e) If a service provider receives a request to know or a request to delete from a consumer, the service provider shall either act on behalf of the business in responding to the request or inform the consumer that the request cannot be acted upon because the request has been sent to a service provider.
- (f) A service provider that is a business shall comply with the CCPA and these regulations with regard to any personal information that it collects, maintains, or sells outside of its role as a service provider.

*Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.100, 1798.105, 1798.110, 1798.115, 1798.130, 1798.140 and 1798.185, Civil Code.*

### **§ 999.315. Requests to Opt-Out.**

- (a) A business shall provide two or more designated methods for submitting requests to opt-out, including an interactive form accessible via a clear and conspicuous link titled “Do Not Sell My Personal Information,” on the business’s website or mobile application. Other acceptable methods for submitting these requests include, but are not limited to, a toll-free phone number, a designated email address, a form submitted in person, a form submitted through the mail, and user-enabled global privacy controls, such as a browser plug-in or privacy setting, device setting, or other mechanism, that communicate or signal the consumer’s choice to opt-out of the sale of their personal information.
- (b) A business shall consider the methods by which it interacts with consumers, the manner in which the business sells personal information to third parties, available technology, and ease of use by the consumer when determining which methods consumers may use to submit requests to opt-out. At least one method offered shall reflect the manner in which the business primarily interacts with the consumer.
- (c) If a business collects personal information from consumers online, the business shall treat user-enabled global privacy controls, such as a browser plug-in or privacy setting, device setting, or other mechanism, that communicate or signal the consumer’s choice to opt-out of the sale of their personal information as a valid request submitted pursuant to Civil Code section 1798.120 for that browser or device, or, if known, for the consumer.
  - (1) Any privacy control developed in accordance with these regulations shall clearly communicate or signal that a consumer intends to opt-out of the sale of personal information.
  - (2) If a global privacy control conflicts with a consumer’s existing business-specific privacy setting or their participation in a business’s financial incentive program, the business shall respect the global privacy control but may notify the consumer of the conflict and give the consumer the choice to confirm the business-specific privacy setting or participation in the financial incentive program.
- (d) In responding to a request to opt-out, a business may present the consumer with the choice to opt-out of sale for certain uses of personal information as long as a global option to opt-

out of the sale of all personal information is more prominently presented than the other choices.

- (e) A business shall comply with a request to opt-out as soon as feasibly possible, but no later than 15 business days from the date the business receives the request. If a business sells a consumer's personal information to any third parties after the consumer submits their request but before the business complies with that request, it shall notify those third parties that the consumer has exercised their right to opt-out and shall direct those third parties not to sell that consumer's information.
- (f) A consumer may use an authorized agent to submit a request to opt-out on the consumer's behalf if the consumer provides the authorized agent written permission signed by the consumer. A business may deny a request from an authorized agent if the agent cannot provide to the business the consumer's signed permission demonstrating that they have been authorized by the consumer to act on the consumer's behalf. User-enabled global privacy controls, such as a browser plug-in or privacy setting, device setting, or other mechanism, that communicate or signal the consumer's choice to opt-out of the sale of their personal information shall be considered a request directly from the consumer, not through an authorized agent.
- (g) A request to opt-out need not be a verifiable consumer request. If a business, however, has a good-faith, reasonable, and documented belief that a request to opt-out is fraudulent, the business may deny the request. The business shall inform the requestor that it will not comply with the request and shall provide an explanation why it believes the request is fraudulent.

*Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.120, 1798.135, 1798.140 and 1798.185, Civil Code.*

#### **§ 999.316. Requests to Opt-In After Opting-Out of the Sale of Personal Information.**

- (a) Requests to opt-in to the sale of personal information shall use a two-step opt-in process whereby the consumer shall first, clearly request to opt-in and then second, separately confirm their choice to opt-in.
- (b) If a consumer who has opted-out of the sale of their personal information initiates a transaction or attempts to use a product or service that requires the sale of their personal information, a business may inform the consumer that the transaction, product, or service requires the sale of their personal information and provide instructions on how the consumer can opt-in.

*Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.120, 1798.135 and 1798.185, Civil Code.*

#### **§ 999.317. Training; Record-Keeping.**

- (a) All individuals responsible for handling consumer inquiries about the business's privacy practices or the business's compliance with the CCPA shall be informed of all of the

requirements in the CCPA and these regulations and how to direct consumers to exercise their rights under the CCPA and these regulations.

- (b) A business shall maintain records of consumer requests made pursuant to the CCPA and how it responded to the requests for at least 24 months. The business shall implement and maintain reasonable security procedures and practices in maintaining these records.
- (c) The records may be maintained in a ticket or log format provided that the ticket or log includes the date of request, nature of request, manner in which the request was made, the date of the business's response, the nature of the response, and the basis for the denial of the request if the request is denied in whole or in part.
- (d) A business's maintenance of the information required by this section, where that information is not used for any other purpose, does not taken alone violate the CCPA or these regulations.
- (e) Information maintained for record-keeping purposes shall not be used for any other purpose except as reasonably necessary for the business to review and modify its processes for compliance with the CCPA and these regulations. Information maintained for record-keeping purposes shall not be shared with any third party except as necessary to comply with a legal obligation.
- (f) Other than as required by subsection (b), a business is not required to retain personal information solely for the purpose of fulfilling a consumer request made under the CCPA.
- (g) A business that knows or reasonably should know that it, alone or in combination, buys, receives for the business's commercial purposes, sells, or shares for commercial purposes the personal information of 10,000,000 or more consumers in a calendar year shall:

  - (1) Compile the following metrics for the previous calendar year:

    - a. The number of requests to know that the business received, complied with in whole or in part, and denied;
    - b. The number of requests to delete that the business received, complied with in whole or in part, and denied;
    - c. The number of requests to opt-out that the business received, complied with in whole or in part, and denied; and
    - d. The median or mean number of days within which the business substantively responded to requests to know, requests to delete, and requests to opt-out.
  - (2) Disclose, by July 1 of every calendar year, the information compiled in subsection (g)(1) within their privacy policy or posted on their website and accessible from a link included in their privacy policy.

- a. In its disclosure pursuant to subsection (g)(2), a business may choose to disclose the number of requests that it denied in whole or in part because the request was not verifiable, was not made by a consumer, called for information exempt from disclosure, or was denied on other grounds.
- (3) Establish, document, and comply with a training policy to ensure that all individuals responsible for handling consumer requests made under the CCPA or the business's compliance with the CCPA are informed of all the requirements in these regulations and the CCPA.
- (h) A business may choose to compile and disclose the information required by subsection (g)(1) for requests received from all individuals, rather than requests received from consumers. The business shall state whether it has done so in its disclosure and shall, upon request, compile and provide to the Attorney General the information required by subsection (g)(1) for requests received from consumers.

*Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.100, 1798.105, 1798.110, 1798.115, 1798.120, 1798.130, 1798.135 and 1798.185, Civil Code.*

#### **§ 999.318. Requests to Know or Delete Household Information.**

- (a) Where a household does not have a password-protected account with a business, a business shall not comply with a request to know specific pieces of personal information about the household or a request to delete household personal information unless all of the following conditions are satisfied:
  - (1) All consumers of the household jointly request to know specific pieces of information for the household or the deletion of household personal information;
  - (2) The business individually verifies all the members of the household subject to the verification requirements set forth in section 999.325; and
  - (3) The business verifies that each member making the request is currently a member of the household.
- (b) Where a consumer has a password-protected account with a business that collects personal information about a household, the business may process requests to know and requests to delete relating to household information through the business's existing business practices and in compliance with these regulations.
- (c) If a member of a household is a consumer under the age of 13, a business must obtain verifiable parental consent before complying with a request to know specific pieces of information for the household or the deletion of household personal information pursuant to the parental consent provisions in section 999.330.

*Note: Authority cited: Section 1798.185, Civil Code. Reference: Section 1798.100, 1798.105, 1798.110, 1798.115, 1798.120, 1798.130, 1798.140 and 1798.185, Civil Code.*

## **Article 4. VERIFICATION OF REQUESTS**

### **§ 999.323. General Rules Regarding Verification.**

- (a) A business shall establish, document, and comply with a reasonable method for verifying that the person making a request to know or a request to delete is the consumer about whom the business has collected information.
- (b) In determining the method by which the business will verify the consumer's identity, the business shall:

  - (1) Whenever feasible, match the identifying information provided by the consumer to the personal information of the consumer already maintained by the business, or use a third-party identity verification service that complies with this section.
  - (2) Avoid collecting the types of personal information identified in Civil Code section 1798.81.5, subdivision (d), unless necessary for the purpose of verifying the consumer.
  - (3) Consider the following factors:

    - a. The type, sensitivity, and value of the personal information collected and maintained about the consumer. Sensitive or valuable personal information shall warrant a more stringent verification process. The types of personal information identified in Civil Code section 1798.81.5, subdivision (d), shall be considered presumptively sensitive;
    - b. The risk of harm to the consumer posed by any unauthorized access or deletion. A greater risk of harm to the consumer by unauthorized access or deletion shall warrant a more stringent verification process;
    - c. The likelihood that fraudulent or malicious actors would seek the personal information. The higher the likelihood, the more stringent the verification process shall be;
    - d. Whether the personal information to be provided by the consumer to verify their identity is sufficiently robust to protect against fraudulent requests or being spoofed or fabricated;
    - e. The manner in which the business interacts with the consumer; and
    - f. Available technology for verification.
- (c) A business shall generally avoid requesting additional information from the consumer for purposes of verification. If, however, the business cannot verify the identity of the consumer from the information already maintained by the business, the business may request additional information from the consumer, which shall only be used for the purposes of verifying the identity of the consumer seeking to exercise their rights under the CCPA.

security, or fraud-prevention. The business shall delete any new personal information collected for the purposes of verification as soon as practical after processing the consumer's request, except as required to comply with section 999.317.

- (d) A business shall not require the consumer or the consumer's authorized agent to pay a fee for the verification of their request to know or request to delete. For example, a business may not require a consumer to provide a notarized affidavit to verify their identity unless the business compensates the consumer for the cost of notarization.
- (e) A business shall implement reasonable security measures to detect fraudulent identity-verification activity and prevent the unauthorized access to or deletion of a consumer's personal information.
- (f) If a business maintains consumer information that is deidentified, a business is not obligated to provide or delete this information in response to a consumer request or to re-identify individual data to verify a consumer request.

*Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.100, 1798.105, 1798.110, 1798.115, 1798.130, 1798.140 and 1798.185, Civil Code.*

#### **§ 999.324. Verification for Password-Protected Accounts.**

- (a) If a business maintains a password-protected account with the consumer, the business may verify the consumer's identity through the business's existing authentication practices for the consumer's account, provided that the business follows the requirements in section 999.323. The business shall also require a consumer to re-authenticate themselves before disclosing or deleting the consumer's data.
- (b) If a business suspects fraudulent or malicious activity on or from the password-protected account, the business shall not comply with a consumer's request to know or request to delete until further verification procedures determine that the consumer request is authentic and the consumer making the request is the person about whom the business has collected information. The business may use the procedures set forth in section 999.325 to further verify the identity of the consumer.

*Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.100, 1798.105, 1798.110, 1798.115, 1798.130 and 1798.185, Civil Code.*

#### **§ 999.325. Verification for Non-Accountholders.**

- (a) If a consumer does not have or cannot access a password-protected account with a business, the business shall comply with this section, in addition to section 999.323.
- (b) A business's compliance with a request to know categories of personal information requires that the business verify the identity of the consumer making the request to a reasonable degree of certainty. A reasonable degree of certainty may include matching at least two data

points provided by the consumer with data points maintained by the business that it has determined to be reliable for the purpose of verifying the consumer.

- (c) A business's compliance with a request to know specific pieces of personal information requires that the business verify the identity of the consumer making the request to a reasonably high degree of certainty. A reasonably high degree of certainty may include matching at least three pieces of personal information provided by the consumer with personal information maintained by the business that it has determined to be reliable for the purpose of verifying the consumer together with a signed declaration under penalty of perjury that the requestor is the consumer whose personal information is the subject of the request. If a business uses this method for verification, the business shall maintain all signed declarations as part of its record-keeping obligations.
- (d) A business's compliance with a request to delete may require that the business verify the identity of the consumer to a reasonable or reasonably high degree of certainty depending on the sensitivity of the personal information and the risk of harm to the consumer posed by unauthorized deletion. For example, the deletion of family photographs may require a reasonably high degree of certainty, while the deletion of browsing history may require only a reasonable degree of certainty. A business shall act in good faith when determining the appropriate standard to apply when verifying the consumer in accordance with these regulations.
- (e) Illustrative examples follow:
  - (1) Example 1: If a business maintains personal information in a manner associated with a named actual person, the business may verify the consumer by requiring the consumer to provide evidence that matches the personal information maintained by the business. For example, if a retailer maintains a record of purchases made by a consumer, the business may require the consumer to identify items that they recently purchased from the store or the dollar amount of their most recent purchase to verify their identity to a reasonable degree of certainty.
  - (2) Example 2: If a business maintains personal information in a manner that is not associated with a named actual person, the business may verify the consumer by requiring the consumer to demonstrate that they are the sole consumer associated with the personal information. For example, a business may have a mobile application that collects personal information about the consumer but does not require an account. The business may determine whether, based on the facts and considering the factors set forth in section 999.323, subsection (b)(3), it may reasonably verify a consumer by asking them to provide information that only the person who used the mobile application may know or by requiring the consumer to respond to a notification sent to their device.
- (f) A business shall deny a request to know specific pieces of personal information if it cannot verify the identity of the requestor pursuant to these regulations.

- (g) If there is no reasonable method by which a business can verify the identity of the consumer to the degree of certainty required by this section, the business shall state so in response to any request and explain why it has no reasonable method by which it can verify the identity of the requestor. If the business has no reasonable method by which it can verify any consumer, the business shall explain why it has no reasonable verification method in its privacy policy. The business shall evaluate and document whether a reasonable method can be established at least once every 12 months, in connection with the requirement to update the privacy policy set forth in Civil Code section 1798.130, subdivision (a)(5).

*Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.100, 1798.105, 1798.110, 1798.115, 1798.130 and 1798.185, Civil Code.*

#### **§ 999.326. Authorized Agent.**

- (a) When a consumer uses an authorized agent to submit a request to know or a request to delete, a business may require that the consumer do the following:
- (1) Provide the authorized agent signed permission to do so.
  - (2) Verify their own identity directly with the business.
  - (3) Directly confirm with the business that they provided the authorized agent permission to submit the request.
- (b) Subsection (a) does not apply when a consumer has provided the authorized agent with power of attorney pursuant to Probate Code sections 4121 to 4130.
- (c) An authorized agent shall implement and maintain reasonable security procedures and practices to protect the consumer's information.
- (d) An authorized agent shall not use a consumer's personal information, or any information collected from or about the consumer, for any purposes other than to fulfill the consumer's requests, verification, or fraud prevention.

*Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.100, 1798.110, 1798.115, 1798.130 and 1798.185, Civil Code.*

### **Article 5. SPECIAL RULES REGARDING CONSUMERS UNDER 16 YEARS OF AGE**

#### **§ 999.330. Consumers Under 13 Years of Age.**

- (a) Process for Opting-In to Sale of Personal Information
- (1) A business that has actual knowledge that it sells the personal information of a consumer under the age of 13 shall establish, document, and comply with a reasonable method for determining that the person affirmatively authorizing the sale of the personal information about the child is the parent or guardian of that child. This

affirmative authorization is in addition to any verifiable parental consent required under COPPA.

- (2) Methods that are reasonably calculated to ensure that the person providing consent is the child's parent or guardian include, but are not limited to:
- a. Providing a consent form to be signed by the parent or guardian under penalty of perjury and returned to the business by postal mail, facsimile, or electronic scan;
  - b. Requiring a parent or guardian, in connection with a monetary transaction, to use a credit card, debit card, or other online payment system that provides notification of each discrete transaction to the primary account holder;
  - c. Having a parent or guardian call a toll-free telephone number staffed by trained personnel;
  - d. Having a parent or guardian connect to trained personnel via video-conference;
  - e. Having a parent or guardian communicate in person with trained personnel; and
  - f. Verifying a parent or guardian's identity by checking a form of government-issued identification against databases of such information, as long as the parent or guardian's identification is deleted by the business from its records promptly after such verification is complete.
- (b) When a business receives an affirmative authorization pursuant to subsection (a), the business shall inform the parent or guardian of the right to opt-out and of the process for doing so on behalf of their child pursuant to section 999.315, subsections (a)-(f).
- (c) A business shall establish, document, and comply with a reasonable method, in accordance with the methods set forth in subsection (a)(2), for determining that a person submitting a request to know or a request to delete the personal information of a child under the age of 13 is the parent or guardian of that child.

*Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.120, 1798.135 and 1798.185, Civil Code.*

### **§ 999.331. Consumers 13 to 15 Years of Age.**

- (a) A business that has actual knowledge that it sells the personal information of consumers at least 13 years of age and less than 16 years of age shall establish, document, and comply with a reasonable process for allowing such consumers to opt-in to the sale of their personal information, pursuant to section 999.316.
- (b) When a business receives a request to opt-in to the sale of personal information from a consumer at least 13 years of age and less than 16 years of age, the business shall inform the

consumer of the right to opt-out at a later date and of the process for doing so pursuant to section 999.315.

*Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.120, 1798.135 and 1798.185, Civil Code.*

#### **§ 999.332. Notices to Consumers Under 16 Years of Age.**

- (a) A business subject to sections 999.330 and 999.331 shall include a description of the processes set forth in those sections in its privacy policy.
- (b) A business that exclusively targets offers of goods or services directly to consumers under 16 years of age and does not sell the personal information without the affirmative authorization of consumers at least 13 years of age and less than 16 years of age, or the affirmative authorization of their parent or guardian for consumers under 13 years of age, is not required to provide the notice of right to opt-out.

*Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.120, 1798.135 and 1798.185, Civil Code.*

### **Article 6. NON-DISCRIMINATION**

#### **§ 999.336. Discriminatory Practices.**

- (a) A financial incentive or a price or service difference is discriminatory, and therefore prohibited by Civil Code section 1798.125, if the business treats a consumer differently because the consumer exercised a right conferred by the CCPA or these regulations.
- (b) A business may offer a financial incentive or price or service difference if it is reasonably related to the value of the consumer's data. If a business is unable to calculate a good-faith estimate of the value of the consumer's data or cannot show that the financial incentive or price or service difference is reasonably related to the value of the consumer's data, that business shall not offer the financial incentive or price or service difference.
- (c) A business's denial of a consumer's request to know, request to delete, or request to opt-out for reasons permitted by the CCPA or these regulations shall not be considered discriminatory.
- (d) Illustrative examples follow:
  - (1) *Example 1:* A music streaming business offers a free service as well as a premium service that costs \$5 per month. If only the consumers who pay for the music streaming service are allowed to opt-out of the sale of their personal information, then the practice is discriminatory, unless the \$5-per-month payment is reasonably related to the value of the consumer's data to the business.

(2) Example 2: A clothing business offers a loyalty program whereby customers receive a \$5-off coupon by email after spending \$100 with the business. A consumer submits a request to delete all personal information the business has collected about them but also informs the business that they want to continue to participate in the loyalty program. The business may deny their request to delete with regard to their email address and the amount the consumer has spent with the business because that information is necessary for the business to provide the loyalty program requested by the consumer and is reasonably anticipated within the context of the business's ongoing relationship with them pursuant to Civil Code section 1798.105, subdivision (d)(1).

(3) Example 3: A grocery store offers a loyalty program whereby consumers receive coupons and special discounts when they provide their phone numbers. A consumer submits a request to opt-out of the sale of their personal information. The retailer complies with their request but no longer allows the consumer to participate in the loyalty program. This practice is discriminatory unless the grocery store can demonstrate that the value of the coupons and special discounts are reasonably related to the value of the consumer's data to the business.

(4) Example 4: An online bookseller collects information about consumers, including their email addresses. It offers coupons to consumers through browser pop-up windows while the consumer uses the bookseller's website. A consumer submits a request to delete all personal information that the bookseller has collected about them, including their email address and their browsing and purchasing history. The bookseller complies with the request but stops providing the periodic coupons to the consumer. The bookseller's failure to provide coupons is discriminatory unless the value of the coupons is reasonably related to the value provided to the business by the consumer's data. The bookseller may not deny the consumer's request to delete with regard to the email address because the email address is not necessary to provide the coupons or reasonably aligned with the expectations of the consumer based on the consumer's relationship with the business.

(e) A business shall notify consumers of any financial incentive or price or service difference subject to Civil Code section 1798.125 that it offers in accordance with section 999.307.

(f) A business's charging of a reasonable fee pursuant to Civil Code section 1798.145, subdivision (i)(3), shall not be considered a financial incentive subject to these regulations.

(g) A price or service difference that is the direct result of compliance with a state or federal law shall not be considered discriminatory.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.125, 1798.130 and 1798.185, Civil Code.

### **§ 999.337. Calculating the Value of Consumer Data**

- (a) A business offering a financial incentive or price or service difference subject to Civil Code section 1798.125 shall use and document a reasonable and good faith method for calculating the value of the consumer's data. The business shall consider one or more of the following:
- (1) The marginal value to the business of the sale, collection, or deletion of a consumer's data.
  - (2) The average value to the business of the sale, collection, or deletion of a consumer's data.
  - (3) The aggregate value to the business of the sale, collection, or deletion of consumers' data divided by the total number of consumers.
  - (4) Revenue generated by the business from sale, collection, or retention of consumers' personal information.
  - (5) Expenses related to the sale, collection, or retention of consumers' personal information.
  - (6) Expenses related to the offer, provision, or imposition of any financial incentive or price or service difference.
  - (7) Profit generated by the business from sale, collection, or retention of consumers' personal information.
  - (8) Any other practical and reasonably reliable method of calculation used in good faith.
- (b) For the purpose of calculating the value of consumer data, a business may consider the value to the business of the data of all natural persons in the United States and not just consumers.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.125, 1798.130 and 1798.185, Civil Code.

## Appendix G

Alastair Mactaggart

Submission of Amendments to The California Privacy Rights and Enforcement Act of 2020, Version 3, No. 19-0021, and Request to Prepare Circulating Title and Summary (Amendment) (Docketed Nov. 13, 2019)

19 - 0021

Amdt. #

November 4, 2019

**VIA MESSENGER**

Office of the Attorney General  
1300 "I" Street, 17th Floor  
Sacramento, CA 95814

RECEIVED

NOV 13 2019

INITIATIVE COORDINATOR  
ATTORNEY GENERAL'S OFFICE

Attention: Initiative Coordinator

Re: *Submission of Amendments to The California Privacy Rights and Enforcement Act of 2020, Version 3, No. 19-0021, and Request to Prepare Circulating Title and Summary (Amendment)*

Dear Initiative Coordinator:

On October 9, 2019, I submitted a proposed statewide initiative titled "*The California Privacy Rights and Enforcement Act of 2020*," Version 3 ("Initiative") and submitted a request that the Attorney General prepare a circulating title and summary pursuant to section 10(d) of Article II of the California Constitution.

Pursuant to Elections Code section 9002(b), I hereby submit timely amendments to the text of the Initiative. As the proponent of the Initiative, I approve the submission of the amended text to the Initiative and I declare that the amendment is reasonably germane to the theme, purpose, and subject of the Initiative. I respectfully request that the Attorney General prepare a circulating title and summary using the amended Initiative (Amendment).

Sincerely,



Alastair Mactaggart

Enclosures  
(00393930)

**THE CALIFORNIA PRIVACY RIGHTS ACT OF 2020**

**Table of Contents**

<b>Section 1:</b>	<b><i>Title: The California Privacy Rights Act of 2020</i></b>
<b>Section 2:</b>	<b><i>Findings and Declarations</i></b>
<b>Section 3:</b>	<b><i>Purpose and Intent</i></b>
	<b><i>A. Consumer Rights</i></b>
	<b><i>B. The Responsibility of Businesses</i></b>
	<b><i>C. Implementation of the Law</i></b>
<b>Section 4:</b>	<b><i>General Duties of Businesses that Collect Consumers' Personal Information</i></b>
<b>Section 5:</b>	<b><i>Consumers' Right to Delete Personal Information</i></b>
<b>Section 6:</b>	<b><i>Consumers' Right to Correct Inaccurate Personal Information</i></b>
<b>Section 7:</b>	<b><i>Consumers' Right to Know What Personal Information is Being Collected. Right to Access Personal Information. Right to Know if Businesses Are Using Personal Information</i></b>
<b>Section 8:</b>	<b><i>Consumers' Right to Know What Personal Information is Sold and to Whom</i></b>
<b>Section 9:</b>	<b><i>Consumers' Right to Opt-Out of Sale or Sharing of Personal Information</i></b>
<b>Section 10:</b>	<b><i>Consumers' Right to Limit Use of Sensitive Personal Information</i></b>
<b>Section 11:</b>	<b><i>Consumers' Right of No Retaliation Following Opt-Out or Exercise of Other Rights</i></b>
<b>Section 12:</b>	<b><i>Notice, Disclosure, Correction, and Deletion Requirements</i></b>
<b>Section 13:</b>	<b><i>Methods of Limiting Sale, Sharing, and Use of Consumers' Personal Information and Sensitive Personal Information</i></b>
<b>Section 14:</b>	<b><i>Definitions</i></b>
<b>Section 15:</b>	<b><i>Exemptions</i></b>
<b>Section 16:</b>	<b><i>Personal Information Security Breaches</i></b>
<b>Section 17:</b>	<b><i>Administrative Enforcement</i></b>
<b>Section 18:</b>	<b><i>Consumer Privacy Fund</i></b>
<b>Section 19:</b>	<b><i>Conflicting Provisions</i></b>
<b>Section 20:</b>	<b><i>Preemption</i></b>
<b>Section 21:</b>	<b><i>Regulations</i></b>
<b>Section 22:</b>	<b><i>Anti-Avoidance</i></b>
<b>Section 23:</b>	<b><i>Waiver</i></b>

## Amendments to Version 3

***Section 24: Establishment of California Privacy Protection Agency***

***Section 25: Amendment***

***Section 26: Severability***

***Section 27: Conflicting Initiatives***

***Section 28: Standing***

***Section 29: Construction***

***Section 30: Savings Clause***

***Section 31: Effective and Operative Dates***

**SEC. 1. Title.**

This measure shall be known and may be cited as “The California Privacy Rights Act of 2020.”

**SEC. 2. Findings and Declarations.**

The People of the State of California hereby find and declare all of the following:

A. In 1972, California voters amended the California Constitution to include the right of privacy among the “inalienable” rights of all people. Voters acted in response to the accelerating encroachment on personal freedom and security caused by increased data collection and usage in contemporary society. The amendment established a legal and enforceable constitutional right of privacy for every Californian. Fundamental to this right of privacy is the ability of individuals to control the use, including the sale, of their personal information.

B. Since California voters approved the constitutional right of privacy, the California Legislature has adopted specific mechanisms to safeguard Californians’ privacy, including the Online Privacy Protection Act, the Privacy Rights for California Minors in the Digital World Act, and Shine the Light, but consumers had no right to learn what personal information a business had collected about them and how they used it or to direct businesses not to sell the consumer’s personal information.

C. That changed in 2018, when more than 629,000 California voters signed petitions to qualify the California Consumer Privacy Act of 2018 for the ballot. In response to the measure’s qualification, the Legislature enacted the California Consumer Privacy Act of 2018 (CCPA) into law. The CCPA gives California consumers the right to learn what information a business has collected about them, to delete their personal information, to stop businesses from selling their personal information, including using it to target them with ads that follow them as they browse the internet from one website to another, and to hold businesses accountable if they do not take reasonable steps to safeguard their personal information.

D. Even before the CCPA had gone into effect, the Legislature considered many bills in 2019 to amend the law, some of which would have significantly weakened it. Unless California voters take action, the hard-fought rights consumers have won could be undermined by future legislation.

E. Rather than diluting privacy rights, California should strengthen them over time. Many businesses collect and use consumers’ personal information, sometimes without consumers’ knowledge regarding the business’s use and retention of their personal information. In practice, consumers are often entering into a form of contractual arrangement in which while they do not pay money for a good or service, they exchange access to that good or service in return for access to their attention, or access to their personal information. Because the value of the personal information they are exchanging for the good or service is often opaque, depending on the practices of the business, consumers often have no good way to value the transaction. In addition, the terms of agreement or policies in which the arrangements are spelled out, are often complex, unclear, and as a result most consumers never have the time to read or understand them.

F. This asymmetry of information makes it difficult for consumers to understand what they are exchanging and therefore to negotiate effectively with businesses. Unlike in other areas of the economy where consumers can comparison shop, or can understand at a glance if a good or

service is expensive or affordable, it is hard for the consumer to know how much his or her information is worth to any given business, when data use practices vary so widely between businesses.

G. The State therefore has an interest in mandating laws that will allow consumers to understand more fully how their information is being used, and for what purposes. In the same way that ingredient labels on foods help consumers shop more effectively, disclosure around data management practices will help consumers become more informed counterparties in the data economy, and promote competition. Additionally, if a consumer can tell a business not to sell his or her data, then that consumer will not have to scour a privacy policy to see whether the business is, in fact, selling that data, and the resulting savings in time is worth, in the aggregate, a tremendous amount of money.

H. Consumers need stronger laws to place them on a more equal footing when negotiating with businesses in order to protect their rights. Consumers should be entitled to a clear explanation of the uses of their personal information, including how it is used for advertising, and to control, correct, or delete it, including by allowing consumers to limit businesses' use of their sensitive personal information to help guard against identity theft, to opt-out of the sale and sharing of their personal information, and to request that businesses correct inaccurate information about them.

I. California is the world leader in many new technologies that have reshaped our society. The world today is unimaginable without the internet, one of the most momentous inventions in human history, and the new services and businesses that arose on top of it -- many of which were invented here in California. One of the most successful business models for the internet has been services that rely on advertising to make money as opposed to charging consumers a fee. Advertising-supported services have existed for generations, and can be a great model for consumers and businesses alike. However, some advertising businesses today use technologies and tools that are opaque to consumers to collect and trade vast amounts of personal information, to track them across the internet, and to create detailed profiles of their individual interests. Some companies that do not charge consumers a fee, subsidize these services by monetizing consumers' personal information. Consumers should have the information and tools necessary to limit the use of their information to non-invasive, pro-privacy advertising, where their personal information is not sold to or shared with hundreds of businesses they've never heard of, if they choose to do so. Absent these tools, it will be virtually impossible for consumers to fully understand these contracts they are essentially entering into when they interact with various businesses.

J. Children are particularly vulnerable from a negotiating perspective with respect to their privacy rights. Parents should be able to control what information is collected and sold or shared about their young children and should be given the right to demand that companies erase information collected about their children.

K. Business should also be held directly accountable to consumers for data security breaches and notify consumers when their most sensitive information has been compromised.

L. An independent watchdog whose mission is to protect consumer privacy should ensure that businesses and consumers are well-informed about their rights and obligations and should vigorously enforce the law against businesses that violate consumers' privacy rights.

### **SEC. 3. Purpose and Intent.**

In enacting this Act, it is the purpose and intent of the people of the State of California to further protect consumers' rights, including the constitutional right of privacy. The implementation of this Act shall be guided by the following principles:

#### **A. Consumer Rights**

1. Consumers should know who is collecting their personal information and that of their children, how it is being used, and to whom it is disclosed, so that they have the information necessary to exercise meaningful control over businesses' use of their personal information and that of their children.
2. Consumers should be able to control the use of their personal information, including limiting the use of their sensitive personal information, the unauthorized use or disclosure of which creates a heightened risk of harm to the consumer, and they should have meaningful options over how it is collected, used, and disclosed.
3. Consumers should have access to their personal information and should be able to correct it, delete it, and take it with them from one business to another.
4. Consumers or their authorized agents should be able to exercise these options through easily accessible self-serve tools.
5. Consumers should be able to exercise these rights without being penalized for doing so.
6. Consumers should be able to hold businesses accountable for failing to take reasonable precautions to protect their most sensitive personal information from hackers and security breaches.
7. Consumers should benefit from businesses' use of their personal information.
8. The privacy interests of employees and independent contractors should also be protected, taking into account the differences in the relationship between employees or independent contractors and businesses, as compared to the relationship between consumers and businesses. In addition, this law is not intended to interfere with the right to organize and collective bargaining under the National Labor Relations Act. It is the purpose and intent of the Act to extend the exemptions in this title for employee and business to business communications until January 1, 2023.

#### **B. The Responsibilities of Businesses**

1. Businesses should specifically and clearly inform consumers about how they collect and use personal information and how they can exercise their rights and choice.
2. Businesses should only collect consumers' personal information for specific, explicit, and legitimate disclosed purposes, and should not further collect, use, or disclose consumers' personal information for reasons incompatible with those purposes.

3. Businesses should collect consumers' personal information only to the extent that it is relevant and limited to what is necessary in relation to the purposes for which it is being collected, used, and shared.
4. Businesses should provide consumers or their authorized agents with easily accessible means to allow consumers and their children to obtain their personal information, to delete it, or correct it, and to opt-out of its sale and the sharing across business platforms, services, businesses and devices, and to limit the use of their sensitive personal information.
5. Businesses should not penalize consumers for exercising these rights.
6. Businesses should take reasonable precautions to protect consumers' personal information from a security breach.
7. Businesses should be held accountable when they violate consumers' privacy rights, and the penalties should be higher when the violation affects children.

### **C. Implementation of the Law**

1. The rights of consumers and the responsibilities of businesses should be implemented with the goal of strengthening consumer privacy, while giving attention to the impact on business and innovation. Consumer privacy and the development of beneficial new products and services are not necessarily incompatible goals. Strong consumer privacy rights create incentives to innovate and develop new products that are privacy protective.
2. Businesses and consumers should be provided with clear guidance about their responsibilities and rights.
3. The law should place the consumer in a position to knowingly and freely negotiate with a business over the business' use of the consumer's personal information.
4. The law should adjust to technological changes, help consumers exercise their rights, and assist businesses with compliance, with the continuing goal of strengthening consumer privacy.
5. The law should enable pro-consumer new products and services and promote efficiency of implementation for business, provided that the amendments do not compromise or weaken consumer privacy.
6. The law should be amended, if necessary, to improve its operation, provided that the amendments do not compromise or weaken consumer privacy, while giving attention to the impact on business and innovation.
7. Businesses should be held accountable for violating the law through vigorous administrative and civil enforcement.
8. To the extent it advances consumer privacy and business compliance, the law should be compatible with privacy laws in other jurisdictions.

**SEC. 4. Section 1798.100 of the Civil Code is amended to read:**

**1798.100. General Duties of Businesses that Collect Personal Information**

1798.100. (a) ~~A consumer shall 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.~~

(b) A business that ***controls the collection of*** collects a consumer's personal information shall, at or before the point of collection, inform consumers as to:

(1) the categories of personal information to be collected and the purposes for which the categories of personal information ***are collected or used shall be used and whether such information is sold or shared.*** A business shall not collect additional categories of personal information or use personal information collected for additional purposes ***that are incompatible with the disclosed purpose for which the personal information was collected,*** without providing the consumer with notice consistent with this section.

(2) ***if the business collects sensitive personal information, the categories of sensitive personal information to be collected and the purposes for which the categories of sensitive personal information are collected or used and whether such information is sold or shared. A business shall not collect additional categories of sensitive personal information or use sensitive personal information collected for additional purposes that are incompatible with the disclosed purpose for which the sensitive personal information was collected, without providing the consumer with notice consistent with this section.***

(3) ***the length of time the business intends to retain each category of personal information, including sensitive personal information, or if that is not possible, the criteria used to determine such period, provided that a business shall not retain a consumer's personal information or sensitive personal information for each disclosed purpose for which the personal information was collected for longer than is reasonably necessary for that disclosed purpose.***

(b) A business that, acting as a third party, controls the collection of personal information about a consumer may satisfy its obligation under subdivision (a) by providing the required information prominently and conspicuously on the homepage of its internet website. In addition, if such business, acting as a third party, controls the collection of personal information about a consumer on its premises, including in a vehicle, then the business shall, at or before the point of collection, inform consumers as to the categories of personal information to be collected and the purposes for which the categories of personal information are used, and whether such personal information is sold, in a clear and conspicuous manner at such location.

(c) A business's collection, use, retention, and sharing of a consumer's personal information shall be reasonably necessary and proportionate to achieve the purposes for which the personal information was collected or processed, or for another disclosed purpose that is compatible with the context in which the personal information was collected, and not further processed in a manner that is incompatible with those purposes.

(d) A business that collects a consumer's personal information and that sells that personal information to, or shares it with, a third party or that discloses it to a service provider or contractor for a business purpose shall enter into an agreement with such third party, service provider, or contractor, that: (1) specifies that the personal information is sold or disclosed by

*the business only for limited and specified purposes; (2) obligates the third party, service provider, or contractor to comply with applicable obligations under this title and obligate those persons to provide the same level of privacy protection as is required by this title; (3) grants the business rights to take reasonable and appropriate steps to help to ensure that the third party, service provider, or contractor uses the personal information transferred in a manner consistent with the business's obligations under this title; (4) requires the third party, service provider, or contractor to notify the business if it makes a determination that it can no longer meet its obligations under this title; (5) grants the business the right, upon notice, including under paragraph (4), to take reasonable and appropriate steps to stop and remediate unauthorized use of personal information.*

*(e) A business that collects a consumer's personal information shall implement reasonable security procedures and practices appropriate to the nature of the personal information to protect the personal information from unauthorized or illegal access, destruction, use, modification, or disclosure in accordance with Section 1798.81.5.*

*(f) Nothing in this section shall require a business to disclose trade secrets, as specified in regulations adopted pursuant to paragraph (3) of subdivision (a) of Section 1798.185.*

~~(c) A business shall provide the information specified in subdivision (a) to a consumer only upon receipt of a verifiable consumer request.~~

~~(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. The information may be delivered by mail or electronically, and if provided electronically, the information shall be in a portable and, to the extent technically feasible, in a readily useable format that allows the consumer to transmit this information to another entity without hindrance. A business may provide personal information to a consumer at any time, but shall not be required to provide personal information to a consumer more than twice in a 12-month period.~~

~~(e) This section shall not require a business to retain any personal information collected for a single, one-time transaction, if such information is not sold or retained by the business or to reidentify or otherwise link information that is not maintained in a manner that would be considered personal information.~~

**SEC. 5. Section 1798.105 of the Civil Code is amended to read:**

***1798.105. Consumers' Right to Delete Personal Information***

1798.105. (a) 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.

(b) A business that collects personal information about consumers shall disclose, pursuant to Section 1798.130, the consumer's rights to request the deletion of the consumer's personal information.

(c) **(1)** A business that receives a verifiable consumer request from a consumer to delete the consumer's personal information pursuant to subdivision (a) of this section shall delete the consumer's personal information from its records, **and direct *notify* any service providers or contractors to delete the consumer's personal information from their records, and *notify all third parties to whom the business has sold or shared such personal information, to delete the***

*consumer's personal information, unless this proves impossible or involves disproportionate effort.*

*(2) The business may maintain a confidential record of deletion requests solely for the purpose of preventing the personal information of a consumer who has submitted a deletion request from being sold, for compliance with laws, or for other purposes solely to the extent permissible under this title.*

*(3) A service provider or contractor shall cooperate with the business in responding to a verifiable consumer request, and at the direction of the business, shall delete, or enable the business to delete, and shall notify any of its own service providers or contractors to delete, personal information about the consumer collected, used, processed, or retained by the service provider or the contractor. The service provider or contractor shall notify any service providers, contractors or third parties who may have accessed such personal information from or through the service provider or contractor, unless the information was accessed at the direction of the business, to delete the consumer's personal information, unless this proves impossible or involves disproportionate effort. A service provider or contractor shall not be required to comply with a deletion request submitted by the consumer directly to the service provider or contractor to the extent that the service provider or contractor has collected, used, processed, or retained the consumer's personal information in its role as a service provider or contractor to the business.*

*(d) A business, or a service provider or contractor, acting pursuant to its contract with the business, another service provider, or another contractor, shall not be required to comply with a consumer's request to delete the consumer's personal information if it is reasonably necessary for the business, or service provider, or contractor to maintain the consumer's personal information in order to:*

*(1) Complete the transaction for which the personal information was collected, fulfill the terms of a written warranty or product recall conducted in accordance with federal law, provide a good or service requested by the consumer, or reasonably anticipated by the consumer within the context of a business's ongoing business relationship with the consumer, or otherwise perform a contract between the business and the consumer.*

*(2) Detect security incidents, protect against malicious, deceptive, fraudulent, or illegal activity, or prosecute those responsible for that activity. Help to ensure security and integrity to the extent the use of the consumer's personal information is reasonably necessary and proportionate for those purposes.*

*(3) Debug to identify and repair errors that impair existing intended functionality.*

*(4) Exercise free speech, ensure the right of another consumer to exercise his or her that consumer's right of free speech, or exercise another right provided for by law.*

*(5) Comply with the California Electronic Communications Privacy Act pursuant to Chapter 3.6 (commencing with Section 1546) of Title 12 of Part 2 of the Penal Code.*

*(6) Engage in public or peer-reviewed scientific, historical, or statistical research in the public interest that conforms or adheres to all other applicable ethics and privacy laws, when the businesses' business's deletion of the information is likely to render impossible or seriously impair the achievement of ability to complete such research, if the consumer has provided informed consent.*

(7) To enable solely internal uses that are reasonably aligned with the expectations of the consumer based on the consumer's relationship with the business **and compatible with the context in which the consumer provided the information.**

(8) Comply with a legal obligation.

~~(9) Otherwise use the consumer's personal information, internally, in a lawful manner that is compatible with the context in which the consumer provided the information.~~

**SEC. 6. Section 1798.106 is added to the Civil Code to read:**

**1798.106. Consumers' Right to Correct Inaccurate Personal Information**

**1798.106 (a) A consumer shall have the right to request a business that maintains inaccurate personal information about the consumer correct such inaccurate personal information, taking into account the nature of the personal information and the purposes of the processing of the personal information.**

**(b) A business that collects personal information about consumers shall disclose, pursuant to Section 1798.130, the consumer's right to request correction of inaccurate personal information.**

**(c) A business that receives a verifiable consumer request to correct inaccurate personal information shall use commercially reasonable efforts to correct the inaccurate personal information, as directed by the consumer, pursuant to Section 1798.130 and regulations adopted pursuant to paragraph (8) of subdivision (a) of Section 1798.185.**

**SEC. 7. Section 1798.110 of the Civil Code is amended to read:**

**1798.110. Consumers' Right to Know What Personal Information is Being Collected. Right to Access Personal Information**

**1798.110. (a) A consumer shall have the right to request that a business that collects personal information about the consumer disclose to the consumer the following:**

**(1) The categories of personal information it has collected about that consumer.**

**(2) The categories of sources from which the personal information is collected.**

**(3) The business or commercial purpose for collecting, ~~or~~ selling, or sharing personal information.**

**(4) The categories of third parties ~~with~~ to whom the business shares **discloses** personal information.**

**(5) The specific pieces of personal information it has collected about that consumer.**

**(b) A business that collects personal information about a consumer shall disclose to the consumer, pursuant to *subparagraph (B) of* paragraph (3) of subdivision (a) of Section 1798.130, the information specified in subdivision (a) upon receipt of a verifiable consumer request from the consumer, **provided that a business shall be deemed to be in compliance with paragraphs (1) through (4) of subdivision (a) of this Section to the extent that the categories of information and the business or commercial purpose for collecting or selling or sharing personal information it would be required to disclose to the consumer pursuant to paragraphs****

**(1) through (4) of subdivision (a) is the same as the information it has disclosed pursuant to paragraphs (1) through (4) of subdivision (c) of this Section.**

(c) A business that collects personal information about consumers shall disclose, pursuant to subparagraphs (B) of paragraph (5) of subdivision (a) of Section 1798.130:

(1) The categories of personal information it has collected about ~~that consumer~~ **consumers**.

(2) The categories of sources from which the personal information is collected.

(3) The business or commercial purpose for collecting, ~~or selling,~~ **or sharing** personal information.

(4) The categories of third parties ~~with~~ **to** whom the business ~~shares~~ **discloses** personal information.

(5) ~~The~~ **That a consumer has the right to request the** specific pieces of personal information the business has collected about that consumer.

~~(d) This section does not require a business to do the following:~~

~~(1) Retain any personal information about a consumer collected for a single one-time transaction if, in the ordinary course of business, that information about the consumer is not retained.~~

~~(2) Reidentify or otherwise link any data that, in the ordinary course of business, is not maintained in a manner that would be considered personal information.~~

**SEC. 8. Section 1798.115 of the Civil Code is amended to read:**

**1798.115. Consumers' Right to Know What Personal Information is Sold or Shared and to Whom**

1798.115. (a) A consumer shall have the right to request that a business that sells **or shares** the consumer's personal information, or that discloses it for a business purpose, disclose to that consumer:

(1) The categories of personal information that the business collected about the consumer.

(2) The categories of personal information that the business sold **or shared** about the consumer and the categories of third parties to whom the personal information was sold **or shared**, by category or categories of personal information for each **category of** third party ~~parties~~ to whom the personal information was sold **or shared**.

(3) The categories of personal information that the business disclosed about the consumer for a business purpose **and the categories of persons to whom it was disclosed for a business purpose**.

(b) A business that sells **or shares** personal information about a consumer, or that discloses a consumer's personal information for a business purpose, shall disclose, pursuant to paragraph (4) of subdivision (a) of Section 1798.130, the information specified in subdivision (a) to the consumer upon receipt of a verifiable consumer request from the consumer.

(c) A business that sells **or shares** consumers' personal information, or that discloses consumers' personal information for a business purpose, shall disclose, pursuant to subparagraph (C) of paragraph (5) of subdivision (a) of Section 1798.130:

(1) The category or categories of consumers' personal information it has sold **or shared**, or if the business has not sold **or shared** consumers' personal information, it shall disclose that fact.

(2) The category or categories of consumers' personal information it has disclosed for a business purpose, or if the business has not disclosed the consumers' personal information for a business purpose, it shall disclose that fact.

(d) A third party shall not sell **or share** personal information about a consumer that has been sold to, **or shared with**, the third party by a business unless the consumer has received explicit notice and is provided an opportunity to exercise the right to opt-out pursuant to Section 1798.120.

**SEC. 9. Section 1798.120 of the Civil Code is amended to read:**

***1798.120. Consumers' Right to Opt-Out of Sale or Sharing of Personal Information***

1798.120. (a) A consumer shall have the right, at any time, to direct a business that sells **or shares** personal information about the consumer to third parties not to sell **or share** the consumer's personal information. This right may be referred to as the right to opt-out **of sale or sharing**.

(b) A business that sells consumers' personal information to, **or shares it with**, third parties shall provide notice to consumers, pursuant to subdivision (a) of Section 1798.135, that this information may be sold **or shared** and that consumers have the "right to opt-out" of the sale **or sharing** of their personal information.

(c) Notwithstanding subdivision (a), a business shall not sell **or share** the personal information of consumers if the business has actual knowledge that the consumer is less than 16 years of age, unless the consumer, in the case of consumers ~~between~~ **at least 13 years of age and less than** 16 years of age, or the consumer's parent or guardian, in the case of consumers who are less than 13 years of age, has affirmatively authorized the sale **or sharing** of the consumer's personal information. A business that willfully disregards the consumer's age shall be deemed to have had actual knowledge of the consumer's age. ~~This right may be referred to as the "right to opt-in."~~

(d) A business that has received direction from a consumer not to sell **or share** the consumer's personal information or, in the case of a minor consumer's personal information has not received consent to sell **or share** the minor consumer's personal information, shall be prohibited, pursuant to paragraph (4) of subdivision ~~(a)~~ **(c)** of Section 1798.135, from selling **or sharing** the consumer's personal information after its receipt of the consumer's direction, unless the consumer subsequently provides ~~express authorization~~ **consent**, for the sale **or sharing** of the consumer's personal information.

**SEC. 10. Section 1798.121 is added to the Civil Code to read:**

***1798.121. Consumers' Right to Limit Use and Disclosure of Sensitive Personal Information***

***1798.121. (a) A consumer shall have the right, at any time, to direct a business that collects sensitive personal information about the consumer to limit its use of the consumer's sensitive personal information to that use which is necessary to perform the services or provide the***

*goods reasonably expected by an average consumer who requests such goods or services, to perform the services set forth in paragraphs (2), (4), (5), and (8) of subdivision (e) of Section 1798.140, and as authorized by regulations adopted pursuant to subparagraph (C) of paragraph (19) of subdivision (a) of Section 1798.185. A business that uses or discloses a consumer's sensitive personal information for purposes other than those specified in this subdivision shall provide notice to consumers, pursuant to subdivision (a) of Section 1798.135, that this information may be used, or disclosed to a service provider or contractor, for additional, specified purposes and that consumers have the right to limit the use or disclosure of their sensitive personal information.*

*(b) A business that has received direction from a consumer not to use or disclose the consumer's sensitive personal information, except as authorized by subdivision (a), shall be prohibited, pursuant to paragraph (4) of subdivision (c) of Section 1798.135, from using or disclosing the consumer's sensitive personal information for any other purpose after its receipt of the consumer's direction, unless the consumer subsequently provides consent for the use or disclosure of the consumer's sensitive personal information for additional purposes.*

*(c) A service provider or contractor that assists a business in performing the purposes authorized by subdivision (a) may not use the sensitive personal information, after it has received instructions from the business and to the extent it has actual knowledge that the personal information is sensitive personal information for any other purpose. A service provider or contractor is only required to limit its use of sensitive personal information received pursuant to a written contract with the business in response to instructions from the business and only with respect to its relationship with that business.*

*(d) Sensitive Personal information that is collected or processed without the purpose of inferring characteristics about a consumer, is not subject to this Section, as further defined in regulations adopted pursuant to subparagraph (C) of paragraph (19) of subdivision (a) of Section 1798.185, and shall be treated as personal information for purposes of all other sections of this Act, including Section 1798.100.*

**SEC. 11. Section 1798.125 of the Civil Code is amended to read:**

***1798.125. Consumers' Right of No Retaliation Following Opt-Out or Exercise of Other Rights***

**1798.125. (a) (1)** A business shall not discriminate against a consumer because the consumer exercised any of the consumer's rights under this title, including, but not limited to, by:

**(A)** Denying goods or services to the consumer.

**(B)** Charging different prices or rates for goods or services, including through the use of discounts or other benefits or imposing penalties.

**(C)** Providing a different level or quality of goods or services to the consumer.

**(D)** Suggesting that the consumer will receive a different price or rate for goods or services or a different level or quality of goods or services.

**(E)** *Retaliating against an employee, applicant for employment, or independent contractor, as defined in subparagraph (A) of paragraph (2) of subdivision (m) of Section 1798.145, for exercising their rights under this title.*

(2) Nothing in this subdivision prohibits a business, **pursuant to subdivision (b)**, from charging a consumer a different price or rate, or from providing a different level or quality of goods or services to the consumer, if that difference is reasonably related to the value provided to the ~~consumer business~~ by the consumer's data.

**(3) This subdivision does not prohibit a business from offering loyalty, rewards, premium features, discounts, or club card programs consistent with this title.**

(b) (1) A business may offer financial incentives, including payments to consumers as compensation, for the collection of personal information, the sale **or sharing** of personal information, or the ~~deletion~~ **retention** of personal information. A business may also offer a different price, rate, level, or quality of goods or services to the consumer if that price or difference is ~~directly~~ **reasonably** related to the value provided to the ~~consumer business~~ by the consumer's data.

(2) A business that offers any financial incentives pursuant to ~~this~~ subdivision (a), shall notify consumers of the financial incentives pursuant to ~~Section 1798.135~~ **1798.130**.

(3) A business may enter a consumer into a financial incentive program only if the consumer gives the business prior opt-in consent pursuant to ~~Section 1798.135~~ **1798.130** which ~~that~~ clearly describes the material terms of the financial incentive program, and which may be revoked by the consumer at any time. ***If a consumer refuses to provide opt-in consent, then the business shall wait for at least 12 months before next requesting that the consumer provide opt-in consent, or as prescribed by regulations adopted pursuant to Section 1798.185.***

(4) A business shall not use financial incentive practices that are unjust, unreasonable, coercive, or usurious in nature.

**SEC. 12. Section 1798.130 of the Civil Code is amended to read:**

***1798.130. Notice, Disclosure, Correction, and Deletion Requirements***

1798.130. (a) In order to comply with Sections 1798.100, 1798.105, **1798.106**, 1798.110, 1798.115, and 1798.125, a business shall, in a form that is reasonably accessible to consumers:

(1) **(A)** Make available to consumers two or more designated methods for submitting requests for information required to be disclosed pursuant to Sections 1798.110 and 1798.115, **or requests for deletion or correction pursuant to Sections 1798.105 and 1798.106, respectively**, including, at a minimum, a toll-free telephone number, ~~and if the business maintains an Internet Web site, a Web site address.~~ ***A business that operates exclusively online and has a direct relationship with a consumer from whom it collects personal information shall only be required to provide an email address for submitting requests for information required to be disclosed pursuant to Sections 1798.110 and 1798.115, or for requests for deletion or correction pursuant to Sections 1798.105 and 1798.106, respectively.***

***(B) If the business maintains an internet website, make the internet website available to consumers to submit requests for information required to be disclosed pursuant to Sections 1798.110 and 1798.115, or requests for deletion or correction pursuant to Sections 1798.105 and 1798.106, respectively.***

(2) **(A)** Disclose and deliver the required information to a consumer free of charge, **or correct inaccurate personal information, or delete a consumer's personal information, based on the consumer's request**, within 45 days of receiving a verifiable consumer request from the consumer. 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, **or correct inaccurate personal information or delete personal information**, within 45 days of receipt of the consumer's request. The time period to provide the required information, **or to correct inaccurate personal information or delete personal 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 **of the required information** 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 **may require authentication of the consumer that is reasonable in light of the nature of the personal information requested, but** shall not require the consumer to create an account with the business in order to make a verifiable consumer request, **provided that if the consumer has an account with the business, the business may require the consumer to use that account to submit a verifiable consumer request.**

**(B) The disclosure of the required information shall cover the 12-month period preceding the business's receipt of the verifiable consumer request, provided that, upon the adoption of a regulation pursuant to paragraph (9) of subdivision (a) of Section 1798.185, a consumer may request that the business disclose the required information beyond the 12-month period and the business shall be required to provide such information unless doing so proves impossible or would involve a disproportionate effort. A consumer's right to request required information beyond the 12-month period, and a business's obligation to provide such information, shall only apply to personal information collected on or after January 1, 2022. Nothing in this subparagraph shall require a business to keep personal information for any length of time.**

**(3) (A) A business that receives a verifiable consumer request pursuant to sections 1798.110 or 1798.115 shall disclose any personal information it has collected about a consumer, directly or indirectly, including through or by a service provider or contractor, to the consumer. A service provider or contractor shall not be required to comply with a verifiable consumer request received directly from a consumer or a consumer's authorized agent pursuant to sections 1798.110 or 1798.115 to the extent that the service provider or contractor has collected personal information about the consumer in its role as a service provider or contractor. A service provider or contractor shall provide assistance to a business with which it has a contractual relationship with respect to the business's response to a verifiable consumer request, including but not limited to by providing to the business the consumer's personal information in the service provider or contractor's possession, which the service provider or contractor obtained as a result of providing services to the business, and by correcting inaccurate information, or by enabling the business to do the same. A service provider or contractor that collects personal information pursuant to a written contract with a business shall be required to assist the business through appropriate technical and organizational measures in complying with the requirements of subdivisions (d) through (f) of Section 1798.100, taking into account the nature of the processing.**

**(B) For purposes of subdivision (b) of Section 1798.110:**

**(A) To identify the consumer, associate the information provided by the consumer in the verifiable consumer request to any personal information previously collected by the business about the consumer.**

~~(B)~~ **(ii)** Identify by category or categories the personal information collected about the consumer ~~in the preceding 12 months~~ **for the applicable period of time** by reference to the enumerated category or categories in subdivision (c) that most closely describes the personal information collected; **the categories of sources from which the consumer's personal information was collected; the business or commercial purpose for collecting, or selling or sharing the consumer's personal information; and the categories of third parties to whom the business discloses the consumer's personal information.**

**(iii) Provide the specific pieces of personal information obtained from the consumer in a format that is easily understandable to the average consumer, and to the extent technically feasible, in a structured, commonly used, machine-readable format, which also may be transmitted to another entity at the consumer's request without hindrance. "Specific pieces of information" do not include data generated to help ensure security and integrity or as prescribed by regulation. Personal information is not considered to have been disclosed by a business when a consumer instructs a business to transfer the consumer's personal information from one business to another in the context of switching services.**

(4) For purposes of subdivision (b) of Section 1798.115:

(A) Identify the consumer and associate the information provided by the consumer in the verifiable consumer request to any personal information previously collected by the business about the consumer.

(B) Identify by category or categories the personal information of the consumer that the business sold **or shared** ~~in the preceding 12 months~~ **during the applicable period of time** by reference to the enumerated category in subdivision (c) that most closely describes the personal information, and provide the categories of third parties to whom the consumer's personal information was sold **or shared** ~~in the preceding 12 months~~ **during the applicable period of time** by reference to the enumerated category or categories in subdivision (c) that most closely describes the personal information sold **or shared**. The business shall disclose the information in a list that is separate from a list generated for the purposes of subparagraph (C).

(C) Identify by category or categories the personal information of the consumer that the business disclosed for a business purpose ~~in the preceding 12 months~~ **during the applicable period of time** by reference to the enumerated category or categories in subdivision (c) that most closely describes the personal information, and provide the categories of ~~third parties~~ **persons** to whom the consumer's personal information was disclosed for a business purpose ~~in the preceding 12 months~~ **during the applicable period of time** by reference to the enumerated category or categories in subdivision (c) that most closely describes the personal information disclosed. The business shall disclose the information in a list that is separate from a list generated for the purposes of subparagraph (B).

(5) Disclose the following information in its online privacy policy or policies if the business has an online privacy policy or policies and in any California-specific description of consumers' privacy rights, or if the business does not maintain those policies, on its ~~Internet Web site~~ **Internet website**, and update that information at least once every 12 months:

(A) A description of a consumer's rights pursuant to Sections **1798.100, 1798.105, 1798.106, 1798.110, 1798.115, and 1798.125** and ~~one~~ **two** or more designated methods for submitting requests, **except as provided in subparagraph (A) of paragraph (1) of subdivision (a).**

(B) For purposes of subdivision (c) of Section 1798.110: **(i)** a list of the categories of personal information it has collected about consumers in the preceding 12 months by reference to the

enumerated category or categories in subdivision (c) that most closely describe the personal information collected; ***(ii) the categories of sources from which consumers' personal information is collected; (iii) the business or commercial purpose for collecting or selling or sharing consumers' personal information; and (iv) the categories of third parties to whom the business discloses consumers' personal information.***

(C) For purposes of paragraphs (1) and (2) of subdivision (c) of Section 1798.115, two separate lists:

(i) A list of the categories of personal information it has sold ***or shared*** about consumers in the preceding 12 months by reference to the enumerated category or categories in subdivision (c) that most closely describe the personal information sold ***or shared***, or if the business has not sold ***or shared*** consumers' personal information in the preceding 12 months, the business shall ***prominently*** disclose that fact ***in its privacy policy.***

(ii) A list of the categories of personal information it has disclosed about consumers for a business purpose in the preceding 12 months by reference to the enumerated category in subdivision (c) that most closely ~~describe~~ ***describes*** the personal information disclosed, or if the business has not disclosed consumers' personal information for a business purpose in the preceding 12 months, the business shall disclose that fact.

(6) Ensure that all individuals responsible for handling consumer inquiries about the business's privacy practices or the business's compliance with this title are informed of all requirements in Sections ***1798.100, 1798.105, 1798.106,*** 1798.110, 1798.115, 1798.125, and this section, and how to direct consumers to exercise their rights under those sections.

(7) Use any personal information collected from the consumer in connection with the business's verification of the consumer's request solely for the purposes of verification, ***and shall not further disclose the personal information, retain it longer than necessary for purposes of verification, or use it for unrelated purposes.***

(b) A business is not obligated to provide the information required by Sections 1798.110 and 1798.115 to the same consumer more than twice in a 12-month period.

(c) The categories of personal information required to be disclosed pursuant to Sections ***1798.100,*** 1798.110 and 1798.115 shall follow the ~~definition~~ ***definitions*** of personal information ***and sensitive personal information*** in Section 1798.140 ***by describing the categories of personal information using the specific terms set forth in subparagraphs (A) through (K) of paragraph (1) of subdivision (v) of Section 1798.140 and by describing the categories of sensitive personal information using the specific terms set forth in paragraphs (1) through (9) of subdivision (ae) of Section 1798.140.***

SEC. 13. Section 1798.135 of the Civil Code is amended to read:

***1798.135. Methods of Limiting Sale, Sharing, and Use of Personal Information and Use of Sensitive Personal Information***

1798.135. (a) A business that ~~is required to comply with Section 1798.120~~ ***sells or shares consumers' personal information or uses or discloses consumers' sensitive personal information for purposes other than those authorized by subdivision (a) of Section 1798.121*** shall, in a form that is reasonably accessible to consumers:

(1) Provide a clear and conspicuous link on the business's ~~internet~~ ***internet*** homepage(s), titled "Do Not Sell ***or Share*** My Personal Information," to an ~~internet Web page~~ ***internet webpage***

that enables a consumer, or a person authorized by the consumer, to opt-out of the sale or *sharing* of the consumer's personal information.

**(2) Provide a clear and conspicuous link on the business's internet homepage(s), titled "Limit the Use of My Sensitive Personal Information" that enables a consumer, or a person authorized by the consumer, to limit the use or disclosure of the consumer's sensitive personal information to those uses authorized by subdivision (a) of Section 1798.121.**

**(3) At the business's discretion, utilize a single, clearly-labeled link on the business's internet homepage(s), in lieu of complying with paragraphs (1) and (2), if such link easily allows a consumer to opt-out of the sale or sharing of the consumer's personal information and to limit the use or disclosure of the consumer's sensitive personal information.**

**(4) In the event that a business responds to opt-out requests received pursuant to paragraphs (1), (2), or (3) by informing the consumer of a charge for the use of any product or service, present the terms of any financial incentive offered pursuant to subdivision (b) of Section 1798.125 for the retention, use, sale, or sharing of the consumer's personal information.**

**(b) (1) A business shall not be required to comply with subdivision (a) if the business allows consumers to opt-out of the sale or sharing of their personal information and to limit the use of their sensitive personal information through an opt-out preference signal sent with the consumer's consent by a platform, technology, or mechanism, based on technical specifications set forth in regulations adopted pursuant to paragraph (20) of subdivision (a) of Section 1798.185, to the business indicating the consumer's intent to opt-out of the business's sale or sharing of the consumer's personal information or to limit the use or disclosure of the consumer's sensitive personal information, or both.**

**(2) A business that allows consumers to opt-out of the sale or sharing of their personal information and to limit the use of their sensitive personal information pursuant to paragraph (1) may provide a link to a webpage that enables the consumer to consent to the business ignoring the opt-out preference signal with respect to that business's sale or sharing of the consumer's personal information or the use of the consumer's sensitive personal information for additional purposes provided that: (A) the consent webpage also allows the consumer or a person authorized by the consumer to revoke such consent as easily as it is affirmatively provided; (B) the link to the webpage does not degrade the consumer's experience on the webpage the consumer intends to visit and has a similar look, feel, and size relative to other links on the same webpage; and (C) the consent webpage complies with technical specifications set forth in regulations adopted pursuant to paragraph (20) of subdivision (a) of Section 1798.185.**

**(3) A business that complies with subdivision (a) of this Section is not required to comply with subdivision (b). For the purposes of clarity, a business may elect whether to comply with subdivision (a) or subdivision (b).**

**(c) A business that is subject to this Section shall:**

**(1) ~~not~~Not require a consumer to create an account or provide additional information beyond what is necessary in order to direct the business not to sell or share the consumer's personal information or to limit use or disclosure of the consumer's sensitive personal information.**

**(2) Include a description of a consumer's rights pursuant to Section Sections 1798.120 and 1798.121, along with a separate link to the "Do Not Sell or Share My Personal Information" internet webpage and a separate link ~~internet Web page~~ to the "Limit the Use of My Sensitive**

***Personal Information” internet webpage, if applicable, or a single link to both choices, or a statement that the business responds to and abides by opt-out preference signals sent by a platform, technology, or mechanism in accordance with subdivision (b), in:***

(A) Its online privacy policy or policies if the business has an online privacy policy or policies.

(B) Any California-specific description of consumers’ privacy rights.

(3) Ensure that all individuals responsible for handling consumer inquiries about the business’s privacy practices or the business’s compliance with this title are informed of all requirements in **Section Sections 1798.120, 1798.121**, and this section and how to direct consumers to exercise their rights under those sections.

(4) For consumers who exercise their right to opt-out of the sale ***or sharing*** of their personal information ***or limit the use or disclosure of their sensitive personal information***, refrain from selling ***or sharing the consumer’s*** personal information ***or using or disclosing the consumer’s sensitive personal information*** collected by the business about the consumer ***and wait for at least 12 months before requesting that the consumer authorize the sale or sharing of the consumer’s personal information or the use and disclosure of the consumer’s sensitive personal information for additional purposes, or as authorized by regulations.***

(5) ~~For a consumer who has opted out of the sale of the consumer’s personal information, respect the consumer’s decision to opt out for at least 12 months before requesting that the consumer authorize the sale of the consumer’s personal information~~ ***consumers under 16 years of age who do not consent to the sale or sharing of their personal information, refrain from selling or sharing the personal information of the consumer under 16 years of age, and wait for at least 12 months before requesting the consumer’s consent again, or as authorized by regulations or until the consumer attains 16 years of age.***

(6) Use any personal information collected from the consumer in connection with the submission of the consumer’s opt-out request solely for the purposes of complying with the opt-out request.

~~(b)-(d)~~ Nothing in this title shall be construed to require a business to comply with the title by including the required links and text on the homepage that the business makes available to the public generally, if the business maintains a separate and additional homepage that is dedicated to California consumers and that includes the required links and text, and the business takes reasonable steps to ensure that California consumers are directed to the homepage for California consumers and not the homepage made available to the public generally.

~~(e)-(e)~~ A consumer may authorize another person ~~solely~~ to opt-out of the sale ***or sharing*** of the consumer’s personal information, ***and to limit the use of the consumer’s sensitive personal information***, on the consumer’s behalf, ***including through an opt-out preference signal, as defined in paragraph (1) of subdivision (b) of this Section, indicating the consumer’s intent to opt-out***, and a business shall comply with an opt-out request received from a person authorized by the consumer to act on the consumer’s behalf, pursuant to regulations adopted by the Attorney General, ***regardless of whether the business has elected to comply with subdivision (a) or (b) of this Section. For purposes of clarity, a business that elects to comply with subdivision (a) of this Section may respond to the consumer’s opt-out consistent with Section 1798.125.***

***(f) If a business communicates a consumer’s opt-out request to any person authorized by the business to collect personal information, the person shall thereafter only use such consumer’s***

***personal information for a business purpose specified by the business, or as otherwise permitted by this title, and shall be prohibited from: (1) selling or sharing the personal information; or (2) retaining, using, or disclosing such consumer's personal information: (A) for any purpose other than for the specific purpose of performing the services offered to the business, (B) outside of the direct business relationship between the person and the business, or (C) for a commercial purpose other than providing the services to the business.***

***(g) A business that communicates a consumer's opt-out request to a person pursuant to subdivision (f) shall not be liable under this title if the person receiving the opt-out request violates the restrictions set forth in the title, provided that, at the time of communicating the opt-out request, the business does not have actual knowledge, or reason to believe, that the person intends to commit such a violation. Any provision of a contract or agreement of any kind that purports to waive or limit in any way this subdivision shall be void and unenforceable.***

**SEC. 14. Section 1798.140 of the Civil Code is amended to read:**

**1798.140. Definitions**

1798.140. For purposes of this title:

***(a) "Advertising and marketing" means a communication by a business or a person acting on the business's behalf in any medium intended to induce a consumer to obtain goods, services, or employment.***

***~~(a)-(b)~~ "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. "Aggregate consumer information" does not mean one or more individual consumer records that have been deidentified.***

***~~(b)-(c)~~ "Biometric information" means an individual's physiological, biological or behavioral characteristics, including **information pertaining to** an individual's deoxyribonucleic acid (DNA), that ~~can be~~ **is used or intended to be used**, singly or in combination with each other or with other identifying data, to establish individual identity. Biometric information includes, but is not limited to, imagery of the iris, retina, fingerprint, face, hand, palm, vein patterns, and voice recordings, from which an identifier template, such as a faceprint, a minutiae template, or a voiceprint, can be extracted, and keystroke patterns or rhythms, gait patterns or rhythms, and sleep, health, or exercise data that contain identifying information.***

***~~(c)-(d)~~ "Business" means:***

***(1) A sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners, 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:***

***(A) As of January 1 of the calendar year, Has had annual gross revenues in excess of twenty-five million dollars (\$25,000,000) in the preceding calendar year, as adjusted pursuant to paragraph (5) of subdivision (a) of Section 1798.185.***

(B) Alone or in combination, annually buys ~~or, receives for the business's commercial purposes,~~ sells, or shares ~~for commercial purposes, alone or in combination~~ the personal information of ~~50,000~~ **100,000** or more consumers ~~or, households, or devices.~~

(C) Derives 50 percent or more of its annual revenues from selling, **or sharing** consumers' personal information.

(2) Any entity that controls or is controlled by a business, as defined in paragraph (1), and that shares common branding with the business **and with whom the business shares consumers' personal information.** "Control" or "controlled" means ownership of, or the power to vote, more than 50 percent of the outstanding shares of any class of voting security of a business; control in any manner over the election of a majority of the directors, or of individuals exercising similar functions; or the power to exercise a controlling influence over the management of a company. "Common branding" means a shared name, servicemark, or trademark, **such that the average consumer would understand that two or more entities are commonly owned.**

**(3) A joint venture or partnership composed of businesses in which each business has at least a 40 percent interest. For purposes of this title, the joint venture or partnership and each business that composes the joint venture or partnership shall separately be considered a single business, except that personal information in the possession of each business and disclosed to the joint venture or partnership shall not be shared with the other business.**

**(4) A person that does business in California, that is not covered by paragraphs (1), (2), or (3) and that voluntarily certifies to the California Privacy Protection Agency that it is in compliance with, and agrees to be bound by, this title.**

~~(d)~~ **(e)** "Business purpose" means the use of personal information for the business's ~~or a service provider's~~ operational purposes, or other notified purposes, **or for the service provider or contractor's operational purposes, as defined by regulations adopted pursuant to paragraph (11) of subdivision (a) of Section 1798.185,** provided that the use of personal information shall 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) ~~Detecting security incidents, protecting against malicious, deceptive, fraudulent, or illegal activity, and prosecuting those responsible for that activity.~~ **Helping to ensure security and integrity to the extent the use of the consumer's personal information is reasonably necessary and proportionate for these purposes.**

(3) Debugging to identify and repair errors that impair existing intended functionality.

(4) Short-term, transient use, **including but not limited to non-personalized advertising shown as part of a consumer's current interaction with the business,** provided ~~that~~ the consumer's personal information ~~that~~ is not disclosed to another third party and is not used to build a profile about ~~a~~ **the** consumer or otherwise alter ~~an individual~~ **the** consumer's experience outside the current interaction **with the business,** ~~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, **providing storage**, or providing similar services on behalf of the business ~~or service provider~~.

***(6) Providing advertising and marketing services, except for cross-context behavioral advertising, to the consumer, provided that for the purpose of advertising and marketing, a service provider or contractor shall not combine the personal information of opted-out consumers which the service provider or contractor receives from or on behalf of the business with personal information which the service provider or contractor receives from or on behalf of another person or persons, or collects from its own interaction with consumers.***

~~(6)-(7)~~ Undertaking internal research for technological development and demonstration.

~~(7)-(8)~~ Undertaking 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.

~~(e)-(f)~~ "Collects," "collected," or "collection" means 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.

~~(f)-(g)~~ "Commercial purposes" means 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. ~~"Commercial purposes" do not include for the purpose of engaging in speech that state or federal courts have recognized as noncommercial speech, including political speech and journalism.~~

***(h) "Consent" means any freely given, specific, informed and unambiguous indication of the consumer's wishes by which he or she, or his or her legal guardian, by a person who has power of attorney or is acting as a conservator for the consumer, such as by a statement or by a clear affirmative action, signifies agreement to the processing of personal information relating to him or her for a narrowly defined particular purpose. Acceptance of a general or broad terms of use or similar document that contains descriptions of personal information processing along with other, unrelated information, does not constitute consent. Hovering over, muting, pausing, or closing a given piece of content does not constitute consent. Likewise, agreement obtained through use of dark patterns does not constitute consent.***

~~(g)-(i)~~ "Consumer" means a natural person who is a California resident, as defined in Section 17014 of Title 18 of the California Code of Regulations, as that section read on September 1, 2017, however identified, including by any unique identifier.

***(j) (1) "Contractor" means a person to whom the business makes available a consumer's personal information for a business purpose pursuant to a written contract with the business, provided that the contract:***

***(A) Prohibits the contractor from:***

***(i) Selling or sharing the personal information.***

***(ii) Retaining, using, or disclosing the personal information for any purpose other than for the business purposes specified in the contract, including retaining, using, or disclosing the personal information for a commercial purpose other than the business purposes specified in the contract, or as otherwise permitted by this title.***

***(iii) Retaining, using, or disclosing the information outside of the direct business relationship between the contractor and the business.***

***(iv) Combining the personal information which the contractor receives pursuant to a written contract with the business with personal information which it receives from or on behalf of another person or persons, or collects from its own interaction with the consumer, provided that the contractor may combine personal information to perform any business purpose as defined in regulations adopted pursuant to paragraph (10) of subdivision (a) of Section 1798.185, except as provided for in paragraph (6) of subdivision (e) of this Section and in regulations adopted by the California Privacy Protection Agency.***

***(B) Includes a certification made by contractor that the contractor understands the restrictions in subparagraph (A) and will comply with them.***

***(C) Permits, subject to agreement with the contractor, the business to monitor the contractor's compliance with the contract through measures including, but not limited to, ongoing manual reviews and automated scans, and regular assessments, audits, or other technical and operational testing at least once every twelve (12) months.***

***(2) If a contractor engages any other person to assist it in processing personal information for a business purpose on behalf of the business, or if any other person engaged by the contractor engages another person to assist in processing personal information for such business purpose, it shall notify the business of such engagement and the engagement shall be pursuant to a written contract binding the other person to observe all the requirements set forth in paragraph (1).***

***(k) "Cross-context behavioral advertising" means the targeting of advertising to a consumer based on the consumer's personal information obtained from the consumer's activity across businesses, distinctly-branded websites, applications, or services, other than the business, distinctly-branded website, application, or service with which the consumer intentionally interacts.***

***(l) "Dark pattern" means a user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decision-making, or choice, as further defined by regulation.***

***~~(h)~~(m) "Deidentified" means information that cannot reasonably be used to infer information about, or otherwise be linked to, a particular consumer, provided that the business that possesses the information:***

***(A) takes reasonable measures to ensure that the information cannot be associated with a consumer or household;***

***(B) publicly commits to maintain and use the information in deidentified form and not to attempt to reidentify the information, except that the business may attempt to reidentify the information solely for the purpose of determining whether its deidentification processes satisfy the requirements of this subdivision; and***

***(C) contractually obligates any recipients of the information to comply with all provisions of this subdivision. 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.~~

~~(i)-(n)~~ ***(n)*** "Designated methods for submitting requests" means a mailing address, email address, Internet Web page ***internet webpage***, Internet Web ***internet web*** portal, toll-free telephone number, or other applicable contact information, whereby consumers may submit a request or direction under this title, and any new, consumer-friendly means of contacting a business, as approved by the Attorney General pursuant to Section 1798.185.

~~(j)-(o)~~ ***(o)*** "Device" means any physical object that is capable of connecting to the Internet, directly or indirectly, or to another device.

~~(k)~~ ***(k)*** "Health insurance information" means a consumer's insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the consumer, or any information in the consumer's application and claims history, including any appeals records, if the information is linked or reasonably linkable to a consumer or household, including via a device, by a business or service provider.

~~(l)-(p)~~ ***(p)*** "Homepage" means the Introductory page of an Internet Web site ***internet website*** and any Internet Web page ***internet webpage*** 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 the notice ***notices*** required by subdivision (a) of Section 1798.145 ***this title***, including, but not limited to, before downloading the application.

***(q)*** "Household" means a group, however identified, of consumers who cohabitate with one another at the same residential address and share use of common device(s) or service(s).

~~(m)-(r)~~ ***(r)*** "Infer" or "inference" means the derivation of information, data, assumptions, or conclusions from facts, evidence, or another source of information or data.

***(s)*** "Intentionally interacts" means when the consumer intends to interact with a person, or disclose personal information to a person, via one or more deliberate interactions, such as visiting the person's website or purchasing a good or service from the person. Hovering over, muting, pausing, or closing a given piece of content does not constitute a consumer's intent to interact with a person.

***(t)*** "Non-personalized advertising" means advertising and marketing that is based solely on a consumer's personal information derived from the consumer's current interaction with the business, with the exception of the consumer's precise geolocation.

~~(n)-(u)~~ **(u)** "Person" means an individual, proprietorship, firm, partnership, joint venture, syndicate, business trust, company, corporation, limited liability company, association, committee, and any other organization or group of persons acting in concert.

~~(o)-(v)~~ **(v)** (1) "Personal Information" means information that identifies, relates to, describes, is **reasonably** capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household. Personal information includes, but is not limited to, the following if it identifies, relates to, describes, is **reasonably** capable of being associated with, or could be reasonably linked, directly or indirectly, with a particular consumer or household:

- (A) Identifiers such as a real name, alias, postal address, unique personal identifier, online identifier, Internet Protocol address, email address, account name, social security number, driver's license number, passport number, or other similar identifiers.
- (B) Any ~~categories of~~ personal information described in subdivision ~~(e)~~ of Section 1798.80.
- (C) Characteristics of protected classifications under California or federal law.
- (D) Commercial information, including records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies.
- (E) Biometric information.
- (F) Internet or other electronic network activity information, including, but not limited to, browsing history, search history, and information regarding a consumer's interaction with an ~~Internet Web site~~ **internet website**, application, or advertisement.
- (G) Geolocation data.
- (H) Audio, electronic, visual, thermal, olfactory, or similar information.
- (I) Professional or employment-related information.
- (J) Education information, defined as information that is not publicly available personally identifiable information as defined in the Family Educational Rights and Privacy Act (20 U.S.C. section 1232g, 34 C.F.R. Part 99).
- (K) Inferences drawn from any of the information identified in this subdivision to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.

**(L) Sensitive personal information.**

(2) "Personal information" does not include publicly available information **or lawfully obtained, truthful information that is a matter of public concern**. For these purposes ~~of this paragraph~~, "publicly available" means: information that is lawfully made available from federal, state, or local government records, ~~or if any conditions associated with such information~~ **that a business has a reasonable basis to believe is lawfully made available to the general public by the consumer or from widely distributed media, or by the consumer; or information made available by a person to whom the consumer has disclosed the information if the consumer has not restricted the information to a specific audience**. "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 "Personal Information"** does not include consumer information that is deidentified or aggregate consumer information.

**(w) "Precise geolocation" means any data that is derived from a device and that is used or intended to be used to locate a consumer within a geographic area that is equal to or less than the area of a circle with a radius of one thousand, eight hundred and fifty (1,850) feet, except as prescribed by regulations.**

~~(p)-(x)~~ **(x)** "Probabilistic identifier" means the identification of a consumer or a **consumer's** device to a degree of certainty of more probable than not based on any categories of personal information included in, or similar to, the categories enumerated in the definition of personal information.

~~(q)-(y)~~ **(y)** "Processing" means any operation or set of operations that are performed on personal data **information** or on sets of personal data **information**, whether or not by automated means.

**(z) "Profiling" means any form of automated processing of personal information, as further defined by regulations pursuant to paragraph (16) of subdivision (a) of Section 1798.185, to evaluate certain personal aspects relating to a natural person, and in particular to analyze or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements.**

~~(r)-(aa)~~ **(aa)** "Pseudonymize" or "Pseudonymization" means 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.

~~(s)-(ab)~~ **(ab)** "Research" means scientific **analysis**, systematic study and observation, including basic research or applied research that is **designed to develop or contribute to public or scientific knowledge in the public interest** and that adheres **or otherwise conforms** to all other applicable ethics and privacy laws, ~~or including but not limited to~~ studies conducted in the public interest in the area of public health. Research with personal information that may have been collected from a consumer in the course of the consumer's interactions with a business's service or device for other purposes shall be:

- (1) Compatible with the business purpose for which the personal information was collected.
- (2) Subsequently pseudonymized and deidentified, or deidentified and in the aggregate, such that the information cannot reasonably identify, relate to, describe, be capable of being associated with, or be linked, directly or indirectly, to a particular consumer, **by a business.**
- (3) Made subject to technical safeguards that prohibit reidentification of the consumer to whom the information may pertain, **other than as needed to support the research.**
- (4) Subject to business processes that specifically prohibit reidentification of the information, **other than as needed to support the research.**
- (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.~~

~~(9)~~ Subjected by the business conducting the research to additional security controls **that** limit access to the research data to only those individuals ~~in a business~~ as are necessary to carry out the research purpose.

**(ac) "Security and Integrity" means the ability: (1) of a network or an information system to detect security incidents that compromise the availability, authenticity, integrity, and confidentiality of stored or transmitted personal information; (2) to detect security incidents, resist malicious, deceptive, fraudulent, or illegal actions, and to help prosecute those responsible for such actions; and (3) a business to ensure the physical safety of natural persons.**

~~(t)-(ad)~~ (1) "Sell," "selling," "sale," or "sold," means 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.

(2) For purposes of this title, a business does not sell personal information when:

(A) A consumer uses or directs the business to: **(i)** intentionally disclose personal information; or **(ii)** ~~uses the business to~~ intentionally interact with a **one or more** third party **parties**; ~~provided the third party does not also sell the personal information, unless that disclosure would be consistent with the provisions of this title. An intentional interaction occurs when the consumer intends to interact with the third party, via one or more deliberate interactions. Hovering over, muting, pausing, or closing a given piece of content does not constitute a consumer's intent to interact with a third party.~~

(B) The business uses or shares an identifier for a consumer who has opted out of the sale of the consumer's personal information **or limited the use of the consumer's sensitive personal information** for the purposes of alerting ~~third parties~~ **persons** that the consumer has opted out of the sale of the consumer's personal information **or limited the use of the consumer's sensitive personal information**; or

~~(C) The business uses or shares with a service provider personal information of a consumer that is necessary to perform a business purpose if both of the following conditions are met:~~

~~(i) The business has provided notice that information being used or shared in its terms and conditions consistent with Section 1798.135.~~

~~(ii) The service provider does not further collect, sell, or use the personal information of the consumer except as necessary to perform the business purpose.~~

~~(D)~~ **(C)** The business transfers to a third party the personal information of a consumer as an asset that is part of a merger, acquisition, bankruptcy, or other transaction in which the third party assumes control of all or part of the business, provided that information is used or shared consistently with Sections ~~1798.110 and 1798.115~~ **this title**. If a third party materially alters how it uses or shares the personal information of a consumer in a manner that is materially inconsistent with the promises made at the time of collection, it shall provide prior notice of the new or changed practice to the consumer. The notice shall be sufficiently prominent and robust to ensure that existing consumers can easily exercise their choices consistently with Section

~~1798.120~~ **this title.** This subparagraph does not authorize a business to make material, retroactive privacy policy changes or make other changes in their privacy policy in a manner that would violate the Unfair and Deceptive Practices Act (Chapter 5 (commencing with Section 17200) of Part 2 of Division 7 of the Business and Professions Code).

**(ae) "Sensitive personal information" means: (1) personal information that reveals (A) a consumer's social security, driver's license, state identification card, or passport number; (B) a consumer's account log-in, financial account, debit card, or credit card number in combination with any required security or access code, password, or credentials allowing access to an account; (C) a consumer's precise geolocation; (D) a consumer's racial or ethnic origin, religious or philosophical beliefs, or union membership; (E) the contents of a consumer's mail, email and text messages, unless the business is the intended recipient of the communication; (F) a consumer's genetic data; and (2)(A) the processing of biometric information for the purpose of uniquely identifying a consumer; (B) personal information collected and analyzed concerning a consumer's health; or (C) personal information collected and analyzed concerning a consumer's sex life or sexual orientation. Sensitive personal information that is "publicly available" pursuant to paragraph (2) of subdivision (v) of Section 1798.140 shall not be considered sensitive personal information or personal information.**

~~(u)~~ **(af) "Service" or "services" means work, labor, and services, including services furnished in connection with the sale or repair of goods.**

~~(v)~~ **(ag) (1) "Service provider" means a sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners, person that processes personal information on behalf of a business and to which receives from or on behalf of the business discloses a consumer's personal information for a business purpose pursuant to a written contract, provided that the contract prohibits the entity receiving the information person from: (A) selling or sharing the personal information; (B) retaining, using, or disclosing the personal information for any purpose other than for the specific purpose of performing the services business purposes specified in the contract for the business, or as otherwise permitted by this title, including retaining, using, or disclosing the personal information for a commercial purpose other than providing the services the business purposes specified in the contract with the business, or as otherwise permitted by this title; (C) retaining, using, or disclosing the information outside of the direct business relationship between the service provider and the business; and (D) combining the personal information which the service provider receives from or on behalf of the business, with personal information which it receives from or on behalf of another person or persons, or collects from its own interaction with the consumer, provided that the service provider may combine personal information to perform any business purpose as defined in regulations adopted pursuant to paragraph (10) of subdivision (a) of Section 1798.185, except as provided for in paragraph (6) of subdivision (e) of this Section and in regulations adopted by the California Privacy Protection Agency. The contract may, subject to agreement with the service provider, permit the business to monitor the service provider's compliance with the contract through measures including, but not limited to, ongoing manual reviews and automated scans, and regular assessments, audits, or other technical and operational testing at least once every twelve (12) months.**

**(2) If a service provider engages any other person to assist it in processing personal information for a business purpose on behalf of the business, or if any other person engaged by the service provider engages another person to assist in processing personal information for such business purpose, it shall notify the business of such engagement, and the**

***engagement shall be pursuant to a written contract binding the other person to observe all the requirements set forth in paragraph (1).***

***(ah) (1) "Share," "shared," or "sharing" means sharing, 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 a third party for cross-context behavioral advertising, whether or not for monetary or other valuable consideration, including transactions between a business and a third party for cross-context behavioral advertising for the benefit of a business in which no money is exchanged.***

***(2) For purposes of this title, a business does not share personal information when:***

***(A) A consumer uses or directs the business to: (i) intentionally disclose personal information; or (ii) intentionally interact with one or more third parties;***

***(B) The business uses or shares an identifier for a consumer who has opted out of the sharing of the consumer's personal information or limited the use of the consumer's sensitive personal information for the purposes of alerting persons that the consumer has opted out of the sharing of the consumer's personal information or limited the use of the consumer's sensitive personal information; or***

***(C) The business transfers to a third party the personal information of a consumer as an asset that is part of a merger, acquisition, bankruptcy, or other transaction in which the third party assumes control of all or part of the business, provided that information is used or shared consistently with this title. If a third party materially alters how it uses or shares the personal information of a consumer in a manner that is materially inconsistent with the promises made at the time of collection, it shall provide prior notice of the new or changed practice to the consumer. The notice shall be sufficiently prominent and robust to ensure that existing consumers can easily exercise their choices consistently with this title. This subparagraph does not authorize a business to make material, retroactive privacy policy changes or make other changes in their privacy policy in a manner that would violate the Unfair and Deceptive Practices Act (Chapter 5 (commencing with Section 17200) of Part 2 of Division 7 of the Business and Professions Code).***

***~~(w)-(ai)~~ "Third party" means a person who is not any of the following:***

***(1) The business with whom the consumer intentionally interacts and that collects personal information from the consumer as part of the consumer's current interaction with the business consumers under this title;***

***(2) A service provider to the business; or***

***(3) A contractor.***

***~~(A) A person to whom the business discloses a consumer's personal information for a business purpose pursuant to a written contract, provided that the contract:~~***

***~~(i) Prohibits the person receiving the personal information from:~~***

***~~(i) Selling the personal information.~~***

***~~(ii) Retaining, using, or disclosing the personal information for any purpose other than for the specific purpose of performing the services specified in the contract, including retaining, using,~~***

~~or disclosing the personal information for a commercial purpose other than providing the services specified in the contract.~~

~~(iii) Retaining, using, or disclosing the information outside of the direct business relationship between the person and the business.~~

~~(ii) Includes a certification made by the person receiving the personal information that the person understands the restrictions in subparagraph (A) and will comply with them.~~

~~(B) A person covered by this paragraph that violates any of the restrictions set forth in this title shall be liable for the violations. A business that discloses personal information to a person covered by this paragraph in compliance with this paragraph shall not be liable under this title if the person receiving the personal information uses it in violation of the restrictions set forth in this title, provided that, at the time of disclosing the personal information, the business does not have actual knowledge, or reason to believe, that the person intends to commit such a violation.~~

~~(x)~~ **(aj)** "Unique identifier" or "Unique personal identifier" means a persistent identifier that can be used to recognize a consumer, a family, or a device that is linked to a consumer or family, over time and across different services, including, but not limited to, a device identifier; an Internet Protocol address; cookies, beacons, pixel tags, mobile ad identifiers, or similar technology; customer number, unique pseudonym, or user alias; telephone numbers, or other forms of persistent or probabilistic identifiers that can be used to identify a particular consumer or device **that is linked to a consumer or family**. For purposes of this subdivision, "family" means a custodial parent or guardian and any ~~minor~~ children **under 18 years of age** over which the parent or guardian has custody.

~~(y)~~ **(ak)** "Verifiable 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, or by a person who has power of attorney or is acting as a conservator for the consumer,~~ and that the business can reasonably verify, **using commercially reasonable methods**, pursuant to regulations adopted by the Attorney General pursuant to paragraph (7) of subdivision (a) of Section 1798.185 to be the consumer about whom the business has collected personal information. A business is not obligated to provide information to the consumer pursuant to Sections 1798.110 and 1798.115, **to delete personal information pursuant to Section 1798.105, or to correct inaccurate personal information pursuant to Section 1798.106**, if the business cannot verify, pursuant to this subdivision and regulations adopted by the Attorney General pursuant to paragraph (7) of subdivision (a) of Section 1798.185, that the consumer making the request is the consumer about whom the business has collected information or is a person authorized by the consumer to act on such consumer's behalf.

**SEC. 15. Section 1798.145 of the Civil Code is amended to read:**

**1798.145. Exemptions**

1798.145. (a) The obligations imposed on businesses by this title shall not restrict a business's ability to:

(1) Comply with federal, state, or local laws **or comply with a court order or subpoena to provide information.**

(2) Comply with a civil, criminal, or regulatory inquiry, investigation, subpoena, or summons by federal, state, or local authorities. **Law enforcement agencies, including police and sheriff's**

***departments, may direct a business pursuant to a law enforcement agency-approved investigation with an active case number not to delete a consumer's personal information and upon receipt of such direction a business shall not delete the personal information for 90 days, in order to allow the law enforcement agency to obtain a court-issued subpoena, order, or warrant to obtain a consumer's personal information. For good cause and only to the extent necessary for investigatory purposes, a law enforcement agency may direct a business not to delete the consumer's personal information for additional 90 day periods. A business that has received direction from a law enforcement agency not to delete the personal information of a consumer who has requested deletion of the consumer's personal information shall not use the consumer's personal information for any purpose other than retaining it to produce to law enforcement in response to a court-issued subpoena, order, or warrant, unless the consumer's deletion request is subject to an exemption from deletion under this title.***

(3) Cooperate with law enforcement agencies concerning conduct or activity that the business, service provider, or third party reasonably and in good faith believes may violate federal, state, or local law.

***(4) Cooperate with a government agency request for emergency access to a consumer's personal information if a natural person is at risk or danger of death or serious physical injury, provided that: (A) the request is approved by a high-ranking agency officer for emergency access to a consumer's personal information; (B) the request is based on the agency's good faith determination that it has a lawful basis to access the information on a non-emergency basis; and (C) the agency agrees to petition a court for an appropriate order within three days and to destroy the information if that order is not granted.***

~~(4)-(5)~~ Exercise or defend legal claims.

~~(5)-(6)~~ Collect, use, retain, sell, ***share***, or disclose consumer ~~consumers'~~ ***personal*** information that is deidentified or in the aggregate consumer information.

~~(6)-(7)~~ Collect, ~~or sell~~, ***or share*** a consumer's personal information if every aspect of that commercial conduct takes place wholly outside of California. For purposes of this title, commercial conduct takes place wholly outside of California if the business collected that information while the consumer was outside of California, no part of the sale of the consumer's personal information occurred in California, and no personal information collected while the consumer was in California is sold. This paragraph shall not ~~permit~~ ***prohibit*** a business from storing, including on a device, personal information about a consumer when the consumer is in California and then collecting that personal information when the consumer and stored personal information is outside of California.

(b) The obligations imposed on businesses by Sections 1798.110, ***1798.115, 1798.120, 1798.121, 1798.130, and to 1798.135***, inclusive, shall not apply where compliance by the business with the title would violate an evidentiary privilege under California law and shall not prevent a business from providing the personal information of a consumer to a person covered by an evidentiary privilege under California law as part of a privileged communication.

(c) (1) This title shall not apply to any of the following:

(A) Medical information governed by the Confidentiality of Medical Information Act (Part 2.6 (commencing with Section 56) of Division 1) or protected health information that is collected by a covered entity or business associate governed by the privacy, security, and breach notification rules issued by the United States Department of Health and Human Services, Parts 160 and 164 of Title 45 of the Code of Federal Regulations, established pursuant to the Health Insurance

Portability and Accountability Act of 1996 (Public Law 104-191) and the Health Information Technology for Economic and Clinical Health Act (Public Law 111-5).

(B) A provider of health care governed by the Confidentiality of Medical Information Act (Part 2.6 (commencing with Section 56) of Division 1) or a covered entity governed by the privacy, security, and breach notification rules issued by the United States Department of Health and Human Services, Parts 160 and 164 of Title 45 of the Code of Federal Regulations, established pursuant to the Health Insurance Portability and Accountability Act of 1996 (Public Law 104-191), to the extent the provider or covered entity maintains patient information in the same manner as medical information or protected health information as described in subparagraph (A) of this section.

(C) ***Personal*** Information collected as part of a clinical trial ***or other biomedical research study*** subject to ***or conducted in accordance with*** the Federal Policy for the Protection of Human Subjects, also known as the Common Rule, pursuant to good clinical practice guidelines issued by the International Council for Harmonisation or pursuant to human subject protection requirements of the United States Food and Drug Administration, ***provided that such information is not sold or shared in a manner not permitted by this subparagraph, and if it is inconsistent, that participants be informed of such use and provide consent.***

(2) For purposes of this subdivision, the definitions of "medical information" and "provider of health care" in Section 56.05 shall apply and the definitions of "business associate," "covered entity," and "protected health information" in Section 160.103 of Title 45 of the Code of Federal Regulations shall apply.

(d) ~~(1) This title 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 as defined by subdivision (d) of Section 1681a of Title 15 of the United States Code and use of that information is limited by the federal Fair Credit Reporting Act (15 U.S.C. Sec. 1681 et seq.).~~ ***activity involving the collection, maintenance, disclosure, sale, communication, or use of any personal information bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living by a consumer reporting agency, as defined in subdivision (f) of Section 1681a of Title 15 of the United States Code, by a furnisher of information, as set forth in Section 1681s-2 of Title 15 of the United States Code, who provides information for use in a consumer report, as defined in subdivision (d) of Section 1681a of Title 15 of the United States Code, and by a user of a consumer report as set forth in Section 1681b of Title 15 of the United States Code.***

***(2) Paragraph (1) shall apply only to the extent that such activity involving the collection, maintenance, disclosure, sale, communication or use of such information by that agency, furnisher, or user is subject to regulation under the Fair Credit Reporting Act, section 1681 et seq., Title 15 of the United States Code and the information is not collected, maintained, used, communicated, disclosed or sold except as authorized by the Fair Credit Reporting Act.***

***(3) This subdivision (d) shall not apply to Section 1798.150.***

(e) This title shall not apply to personal information collected, processed, sold, or disclosed pursuant ~~subject~~ to the federal Gramm-Leach-Bliley Act (Public Law 106-102), and implementing regulations, or the California Financial Information Privacy Act (Division 1.4 (commencing with Section 4050) of the Financial Code), ***or the Federal Farm Credit Act of 1971 (as amended in 12 U.S.C. Sections 2001 -- 2279cc and implementing regulations, 12 Code of Federal Regulations, Parts 600, et seq.).*** This subdivision shall not apply to Section 1798.150.

(f) This title shall not apply to personal information collected, processed, sold, or disclosed pursuant to the Driver's Privacy Protection Act of 1994 (18 U.S.C. Sec. 2721 et seq.). This subdivision shall not apply to Section 1798.150.

***(g) (1) Section 1798.120 shall not apply to vehicle information or ownership information retained or shared between a new motor vehicle dealer, as defined in Section 426 of the Vehicle Code, and the vehicle's manufacturer, as defined in Section 672 of the Vehicle Code, if the vehicle or ownership information is shared for the purpose of effectuating, or in anticipation of effectuating, a vehicle repair covered by a vehicle warranty or a recall conducted pursuant to Sections 30118 to 30120, inclusive, of Title 49 of the United States Code, provided that the new motor vehicle dealer or vehicle manufacturer with which that vehicle information or ownership information is shared does not sell, share, or use that information for any other purpose.***

***(2) For purposes of this subdivision:***

***(A) "Vehicle information" means the vehicle information number, make, model, year, and odometer reading.***

***(B) "Ownership information" means the name or names of the registered owner or owners and the contact information for the owner or owners.***

~~(g)~~ ***(h)*** Notwithstanding a business's obligations to respond to and honor consumer rights requests pursuant to this title:

(1) A time period for a business to respond to ***a consumer*** for any ~~verified~~ ***verifiable*** consumer request may be extended by up to ***a total of 90*** additional days where necessary, taking into account the complexity and number of the requests. The business shall inform the consumer of any such extension within 45 days of receipt of the request, together with the reasons for the delay.

(2) If the business does not take action on the request of the consumer, the business shall inform the consumer, without delay and at the latest within the time period permitted of response by this section, of the reasons for not taking action and any rights the consumer may have to appeal the decision to the business.

(3) If requests from a consumer are manifestly unfounded or excessive, in particular because of their repetitive character, a business may either charge a reasonable fee, taking into account the administrative costs of providing the information or communication or taking the action requested, or refuse to act on the request and notify the consumer of the reason for refusing the request. The business shall bear the burden of demonstrating that any ~~verified~~ ***verifiable*** consumer request is manifestly unfounded or excessive.

~~(h)~~ ***(i) (1) A business that discloses personal information to a service provider or contractor in compliance with this title shall not be liable under this title if the service provider or contractor receiving the personal information uses it in violation of the restrictions set forth in the title, provided that, at the time of disclosing the personal information, the business does not have actual knowledge, or reason to believe, that the service provider or contractor intends to commit such a violation. A service provider or contractor shall likewise not be liable under this title for the obligations of a business for which it provides services as set forth in this title, provided that the service provider or contractor shall be liable for its own violations of this title.***

***(2) A business that discloses personal information of a consumer, with the exception of consumers who have exercised their right to opt-out of the sale or sharing of their personal information, consumers who have limited the use or disclosure of their sensitive personal information, and minor consumers who have not opted-in to the collection or sale of their personal information, to a third party pursuant to a written contract that requires the third party to provide the same level of protection of the consumer's rights under this title as provided by the business shall not be liable under this title if the third party receiving the personal information uses it in violation of the restrictions set forth in the title, provided that, at the time of disclosing the personal information, the business does not have actual knowledge, or reason to believe, that the third party intends to commit such a violation.***

***~~(j)~~ (j) This title shall not be construed to require a business, service provider, or contractor to: (1) reidentify or otherwise link information that, in the ordinary course of business, is not maintained in a manner that would be considered personal information; (2) retain any personal information about a consumer if, in the ordinary course of business, that information about the consumer would not be retained; or (3) maintain information in identifiable, linkable or associable form, or collect, obtain, retain, or access any data or technology, in order to be capable of linking or associating a verifiable consumer request with personal information.***

***~~(k)~~ (k) The rights afforded to consumers and the obligations imposed on the business in this title shall not adversely affect the rights and freedoms of other consumers natural persons. A verifiable consumer request for specific pieces of personal information pursuant to Section 1798.110, to delete a consumer's personal information pursuant to Section 1798.105, or to correct inaccurate personal information pursuant to Section 1798.106, shall not extend to personal information about the consumer that belongs to, or the business maintains on behalf of, another natural person. A business may rely on representations made in a verifiable consumer request as to rights with respect to personal information and is under no legal requirement to seek out other persons that may have or claim to have rights to personal information, and a business is under no legal obligation under this title or any other provision of law to take any action under this title in the event of a dispute between or among persons claiming rights to personal information in the business's possession.***

***~~(l)~~ (l) The rights afforded to consumers and the obligations imposed on any business under this title shall not apply to the extent that they infringe on the noncommercial activities of a person or entity described in subdivision (b) of Section 2 of Article I of the California Constitution.***

***(m) (1) This title shall not apply to any of the following:***

***(A) Personal information that is collected by a business about a natural person in the course of the natural person acting as a job applicant to, an employee of, owner of, director of, officer of, medical staff member of, or independent contractor of that business to the extent that the natural person's personal information is collected and used by the business solely within the context of the natural person's role or former role as a job applicant to, an employee of, owner of, director of, officer of, medical staff member of, or an independent contractor of that business.***

***(B) Personal information that is collected by a business that is emergency contact information of the natural person acting as a job applicant to, an employee of, owner of, director of, officer of, medical staff member of, or independent contractor of that business to the extent that the personal information is collected and used solely within the context of having an emergency contact on file.***

*(C) Personal information that is necessary for the business to retain to administer benefits for another natural person relating to the natural person acting as a job applicant to, an employee of, owner of, director of, officer of, medical staff member of, or independent contractor of that business to the extent that the personal information is collected and used solely within the context of administering those benefits.*

*(2) For purposes of this subdivision:*

*(A) "Independent contractor" means a natural person who provides any service to a business pursuant to a written contract.*

*(B) "Director" means a natural person designated in the articles of incorporation as such or elected by the incorporators and natural persons designated, elected, or appointed by any other name or title to act as directors, and their successors.*

*(C) "Medical staff member" means a licensed physician and surgeon, dentist, or podiatrist, licensed pursuant to Division 2 (commencing with Section 500) of the Business and Professions Code and a clinical psychologist as defined in Section 1316.5 of the Health and Safety Code.*

*(D) "Officer" means a natural person elected or appointed by the board of directors to manage the daily operations of a corporation, such as a chief executive officer, president, secretary, or treasurer.*

*(E) "Owner" means a natural person who meets one of the following:*

*(i) Has ownership of, or the power to vote, more than 50 percent of the outstanding shares of any class of voting security of a business.*

*(ii) Has control in any manner over the election of a majority of the directors or of individuals exercising similar functions.*

*(iii) Has the power to exercise a controlling influence over the management of a company.*

*(3) This subdivision shall not apply to subdivision (a) of Section 1798.100 or Section 1798.150.*

*(4) This subdivision shall become inoperative on January 1, 2023.*

*(n) (1) The obligations imposed on businesses by Sections 1798.100, 1798.105, 1798.106, 1798.110, 1798.115, 1798.121, 1798.130, and 1798.135 shall not apply to personal information reflecting a written or verbal communication or a transaction between the business and the consumer, where the consumer is a natural person who acted or is acting as an employee, owner, director, officer, or independent contractor of a company, partnership, sole proprietorship, non-profit, or government agency and whose communications or transaction with the business occur solely within the context of the business conducting due diligence regarding, or providing or receiving a product or service to or from such company, partnership, sole proprietorship, non-profit, or government agency.*

*(2) For purposes of this subdivision:*

*(A) "Independent contractor" means a natural person who provides any service to a business pursuant to a written contract.*

*(B) "Director" means a natural person designated in the articles of incorporation as such or elected by the incorporators and natural persons designated, elected, or appointed by any other name or title to act as directors, and their successors.*

**(C) "Officer" means a natural person elected or appointed by the board of directors to manage the daily operations of a corporation, such as a chief executive officer, president, secretary, or treasurer.**

**(D) "Owner" means a natural person who meets one of the following:**

**(i) Has ownership of, or the power to vote, more than 50 percent of the outstanding shares of any class of voting security of a business.**

**(ii) Has control in any manner over the election of a majority of the directors or of individuals exercising similar functions.**

**(iii) Has the power to exercise a controlling influence over the management of a company.**

**(3) This subdivision shall become inoperative on January 1, 2023.**

**(o) (1) Sections 1798.105 and 1798.120 shall not apply to a commercial credit reporting agency's collection, processing, sale, or disclosure of business controller information to the extent the commercial credit reporting agency uses the business controller information solely to identify the relationship of a consumer to a business which the consumer owns or contact the consumer only in the consumer's role as the owner, director, officer, or management employee of the business.**

**(2) For the purposes of this subdivision:**

**(A) "Business controller information" means the name or names of the owner or owners, director, officer, or management employee of a business, and the contact information, including a business title, for the owner or owners, director, officer, or management employee.**

**(B) "Commercial credit reporting agency" has the meaning set forth subdivision (b) of Section 1785.42.**

**(C) "Owner or owners" means a natural person that meets one of the following:**

**(i) Has ownership of, or the power to vote, more than 50 percent of the outstanding shares of any class of voting security of a business.**

**(ii) Has control in any manner over the election of a majority of the directors, or of individuals exercising similar functions.**

**(iii) Has the power to exercise a controlling influence over the management of a company.**

**(C) "Director" means a natural person designated in the articles of incorporation of a business as such or elected by the incorporators and natural persons designated, elected or appointed by any other name or title to act as directors, and their successors.**

**(D) "Officer" means a natural person elected or appointed by the board of directors of a business to manage the daily operations of a corporation, such as a chief executive officer, president, secretary, or treasurer.**

**(E) "Management employee" means a natural person whose name and contact information is reported to or collected by a commercial credit reporting agency as the primary manager of a business and used solely within the context of the natural person's role as the primary manager of the business.**

***(p) The obligations imposed on businesses in Sections 1798.105, 1798.106, 1798.110, and 1798.115 inclusive, shall not apply to household data.***

***(q) (1) This title does not require a business to comply with a verifiable consumer request to delete a consumer's personal information under Section 1798.105 to the extent the verifiable consumer request applies to a student's grades, educational scores, or educational test results that the business holds on behalf of a local educational agency, as defined in subdivision (d) of Section 49073.1 of the Education Code, at which the student is currently enrolled. If a business does not comply with a request pursuant to this section, it shall notify the consumer that it is acting pursuant to this exception.***

***(2) This title does not require, in response to a request pursuant to Section 1798.110, that a business disclose an educational standardized assessment or educational assessment or a consumer's specific responses to the educational standardized assessment or educational assessment where consumer access, possession or control would jeopardize the validity and reliability of that educational standardized assessment or educational assessment. If a business does not comply with a request pursuant to this section, it shall notify the consumer that it is acting pursuant to this exception.***

***(3) For purposes of this subdivision:***

***(A) "Educational standardized assessment or educational assessment" means a standardized or non-standardized quiz, test, or other assessment used to evaluate students in or for entry to K-12 schools, post-secondary institutions, vocational programs, and postgraduate programs which are accredited by an accrediting agency or organization recognized by the state of California or the United States Department of Education, as well as certification and licensure examinations used to determine competency and eligibility to receive certification or licensure from a government agency or government certification body.***

***(B) "Jeopardize the validity and reliability of that educational standardized assessment or educational assessment" means releasing information that would provide an advantage to the consumer who has submitted a verifiable consumer request or to another natural person.***

***(r) Sections 1798.105 and 1798.120 shall not apply to a business's use, disclosure, or sale of particular pieces of a consumer's personal information if the consumer has consented to the business's use, disclosure, or sale of that information to produce a physical item such as a school yearbook containing the consumer's photograph if:***

***(1) The business has incurred significant expense in reliance on the consumer's consent;***

***(2) Compliance with the consumer's request to opt-out of the sale of the consumer's personal information or to delete the consumer's personal information would not be commercially reasonable; and***

***(3) The business complies with the consumer's request as soon as it is commercially reasonable to do so.***

**SEC. 16. Section 1798.150 of the Civil Code is amended to read:**

**1798.150. Personal Information Security Breaches**

**1798.150. (a) (1) Any consumer whose nonencrypted ~~or~~ **and** nonredacted personal information, as defined in subparagraph (A) of paragraph (1) of subdivision (d) of Section 1798.81.5, **or whose****

***email address in combination with a password or security question and answer that would permit access to the account***, 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 any of the following:

(A) To recover damages in an amount not less than one hundred dollars (\$100) and not greater than seven hundred and fifty (\$750) per consumer per incident or actual damages, whichever is greater.

(B) Injunctive or declaratory relief.

(C) Any other relief the court deems proper.

(2) In assessing the amount of statutory damages, the court shall consider any one or more of the relevant circumstances presented by any of the parties to the case, including, but not limited to, the nature and seriousness of the misconduct, the number of violations, the persistence of the misconduct, the length of time over which the misconduct occurred, the willfulness of the defendant's misconduct, and the defendant's assets, liabilities, and net worth.

(b) Actions pursuant to this section may be brought by a consumer if, prior to initiating any action against a business for statutory damages on an individual or class-wide basis, a consumer provides a business 30 days' written notice identifying the specific provisions of this title the consumer alleges have been or are being violated. In the event a cure is possible, if within the 30 days the business actually cures the noticed violation and provides the consumer an express written statement that the violations have been cured and that no further violations shall occur, no action for individual statutory damages or class-wide statutory damages may be initiated against the business. ***The implementation and maintenance of reasonable security procedures and practices pursuant to Section 1798.81.5 following a breach does not constitute a cure with respect to that breach.*** No notice shall be required prior to an individual consumer initiating an action solely for actual pecuniary damages suffered as a result of the alleged violations of this title. If a business continues to violate this title in breach of the express written statement provided to the consumer under this section, the consumer may initiate an action against the business to enforce the written statement and may pursue statutory damages for each breach of the express written statement, as well as any other violation of the title that postdates the written statement.

(c) The cause of action established by this section shall apply only to violations as defined in subdivision (a) and shall not be based on violations of any other section of this title. Nothing in this title shall be interpreted to serve as the basis for a private right of action under any other law. This shall not be construed to relieve any party from any duties or obligations imposed under other law or the United States or California Constitution.

**SEC. 17. Section 1798.155 of the Civil Code is amended to read:**

***1798.155. Administrative Enforcement***

~~1798.155. (a) Any business or third party may seek the opinion of the Attorney General for guidance on how to comply with the provisions of this title.~~

~~(b) A business shall be in violation of this title if it fails to cure any alleged violation within 30 days after being notified of alleged noncompliance.~~ Any business, service provider, ***contractor*** or other person that violates this title shall be ~~subject to an injunction and liable for an~~ ***administrative fine of not more than two thousand five hundred dollars (\$2,500) for each***

*violation, or seven thousand five hundred dollars (\$7,500) for each intentional violation or violations involving the personal information of consumers whom the business, service provider, contractor or other person has actual knowledge is under 16 years of age, as adjusted pursuant to paragraph (5) of subdivision (a) of Section 1798.185, in an administrative enforcement action brought by the California Privacy Protection Agency a civil penalty of not more than two thousand five hundred dollars (\$2,500) for each violation or seven thousand five hundred dollars (\$7,500) for each intentional violation, which shall be assessed and recovered in a civil action brought in the name of the people of the State of California by the Attorney General. The civil penalties provided for in this section shall be exclusively assessed and recovered in a civil action brought in the name of the people of the State of California by the Attorney General.*

~~(e)~~ *(b)* Any civil penalty *administrative fine* assessed for a violation of this title, and the proceeds of any settlement of an action brought pursuant to subdivision ~~(b)~~ *(a)*, shall be deposited in the Consumer Privacy Fund, created within the General Fund pursuant to subdivision (a) of Section 1798.160 with the intent to fully offset any costs incurred by the state courts, ~~and the Attorney General and the California Privacy Protection Agency~~ in connection with this title.

**SEC. 18. Section 1798.160 of the Civil Code is amended to read:**

**1798.160. Consumer Privacy Fund**

1798.160. (a) A special fund to be known as the "Consumer Privacy Fund" is hereby created within the General Fund in the State Treasury, and is available upon appropriation by the Legislature *first* to offset any costs incurred by the state courts in connection with actions brought to enforce this title, ~~and any the~~ costs incurred by the Attorney General in carrying out the Attorney General's duties under this title, *and then for the purposes of establishing an investment fund in the State Treasury, with any earnings or interest from the fund to be deposited in the General Fund, and making grants to promote and protect consumer privacy, educate children in the area of online privacy, and fund cooperative programs with international law enforcement organizations to combat fraudulent activities with respect to consumer data breaches.*

(b) Funds transferred to the Consumer Privacy Fund shall be used exclusively *as follows*:

*(1)* to offset any costs incurred by the state courts and the Attorney General in connection with this title.

*(2)* after satisfying the obligations under paragraph (1), the remaining funds shall be allocated each fiscal year as follows: (A) ninety-one percent (91%) shall be invested by the Treasurer in financial assets with the goal of maximizing long term yields consistent with a prudent level of risk; the principal shall not be subject to transfer or appropriation, provided that any interest and earnings shall be transferred on an annual basis to the General Fund for appropriation by the Legislature for General Fund purposes; and (B) nine percent (9%) shall be made available to the California Privacy Protection Agency for the purposes of making grants in California, with three percent (3%) allocated to each of the following grant recipients: (i) non-profit organizations to promote and protect consumer privacy; (ii) non-profit organizations and public agencies, including school districts, to educate children in the area of online privacy; and (iii) state and local law enforcement agencies to fund cooperative programs with international law enforcement organizations to combat fraudulent activities with respect to consumer data breaches.

~~(c) These funds~~ *Funds in the Consumer Privacy Fund* shall not be subject to appropriation or transfer by the Legislature for any other purpose. ~~unless the Director of Finance determines~~

~~that the funds are in excess of the funding needed to fully offset the costs incurred by the state courts and the Attorney General in connection with this title, in which case the Legislature may appropriate excess funds for other purposes.~~

**SEC. 19. Section 1798.175 of the Civil Code is hereby reenacted to read:**

***1798.175. Conflicting Provisions***

1798.175. 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 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.

**SEC. 20. Section 1798.180 of the Civil Code is hereby reenacted to read:**

***1798.180. Preemption***

1798.180. This title is a matter of statewide concern and supersedes and preempts all rules, regulations, codes, ordinances, and other laws adopted by a city, county, city and county, municipality, or local agency regarding the collection and sale of consumers' personal information by a business.

**SEC. 21. Section 1798.185 of the Civil Code is amended to read:**

***1798.185. Regulations***

1798.185. (a) On or before July 1, 2020, the Attorney General shall solicit broad public participation and adopt regulations to further the purposes of this title, including, but not limited to, the following areas:

- (1) Updating ~~or adding as needed~~ additional categories of personal information to those enumerated in subdivision (c) of Section 1798.130 and subdivision ~~(c)~~ (v) of Section 1798.140, **and updating or adding categories of sensitive personal information to those enumerated in subdivision (ae) of Section 1798.140**, in order to address changes in technology, data collection practices, obstacles to implementation, and privacy concerns.
- (2) Updating as needed the definition **definitions** of "**deidentified**" and unique identifiers "**unique identifier**" to address changes in technology, data collection, obstacles to implementation, and privacy concerns, and additional **adding, modifying, or deleting** categories to the definition of designated methods for submitting requests to facilitate a consumer's ability to obtain information from a business pursuant to Section 1798.130. *The authority to update the definition of "deidentified" shall not apply to deidentification standards set forth in Section 164.514 of Title 45 of the Code of Federal Regulations, where such information previously was "protected health information" as defined in Section 160.103 of that title.*
- (3) Establishing any exceptions necessary to comply with state or federal law, including, but not limited to, those relating to trade secrets and intellectual property rights, within one year of

passage of this title and as needed thereafter, ***with the intention that trade secrets should not be disclosed in response to a verifiable consumer request.***

(4) Establishing rules and procedures for the following:

(A) To facilitate and govern the submission of a request by a consumer to opt-out of the sale ***or sharing*** of personal information pursuant to ~~paragraph (1) of subdivision (a) of Section 1798.145~~ ***1798.120 and to limit the use of a consumer's sensitive personal information pursuant to Section 1798.121 to ensure that consumers have the ability to exercise their choices without undue burden and to prevent business from engaging in deceptive or harassing conduct, including in retaliation against consumers for exercising their rights, while allowing businesses to inform consumers of the consequences of their decision to opt-out of the sale or sharing of their personal information or to limit the use of their sensitive personal information.***

(B) To govern business compliance with a consumer's opt-out request.

(C) For the development and use of a recognizable and uniform opt-out logo or button by all businesses to promote consumer awareness of the opportunity to opt-out of the sale of personal information.

(5) Adjusting the monetary ~~threshold~~ ***thresholds, in January of every odd-numbered year to reflect any increase in the Consumer Price Index, in: subparagraph (A) of paragraph (1) of subdivision (e) (d) of Section 1798.140; subparagraph (A) of paragraph (1) of subdivision (a) of Section 1798.150; subdivision (a) of Section 1798.155; Section 1798.199.25; and subdivision (a) of Section 1798.199.90 in January of every odd-numbered year to reflect any increase in the Consumer Price Index.***

(6) Establishing rules, procedures, and any exceptions necessary to ensure that the notices and information that businesses are required to provide pursuant to this title are provided in a manner that may be easily understood by the average consumer, are accessible to consumers with disabilities, and are available in the language primarily used to interact with the consumer, including establishing rules and guidelines regarding financial ***incentives*** ~~incentive offerings~~, within one year of passage of this title and as needed thereafter.

(7) Establishing rules and procedures to further the purposes of Sections ***1798.105, 1798.106, 1798.110 and 1798.115*** and to facilitate a consumer's or the consumer's authorized agent's ability to ***delete personal information, correct inaccurate personal information pursuant to Section 1798.106, or*** obtain information pursuant to Section 1798.130, with the goal of minimizing the administrative burden on consumers, taking into account available technology, security concerns, and the burden on the business, to govern a business's determination that a request for information received ~~by~~ ***from*** a consumer is a verifiable consumer request, including treating a request submitted through a password-protected account maintained by the consumer with the business while the consumer is logged into the account as a verifiable consumer request and providing a mechanism for a consumer who does not maintain an account with the business to request information through the business's authentication of the consumer's identity, within one year of passage of this title and as needed thereafter.

***(8) Establishing how often, and under what circumstances, a consumer may request a correction pursuant to Section 1798.106, including standards governing: (A) how a business responds to a request for correction, including exceptions for requests to which a response is impossible or would involve disproportionate effort, and requests for correction of accurate information; (B) how concerns regarding the accuracy of the information may be resolved; (C) the steps a business may take to prevent fraud; and (D) if a business rejects a request to***

**correct personal information collected and analyzed concerning a consumer's health, the right of a consumer to provide a written addendum to the business with respect to any item or statement regarding any such personal information that the consumer believes to be incomplete or incorrect. The addendum shall be limited to 250 words per alleged incomplete or incorrect item and shall clearly indicate in writing that the consumer requests the addendum to be made a part of the consumer's record.**

**(9) Establishing the standard to govern a business's determination, pursuant to subparagraph (B) of paragraph (2) of subdivision (a) of Section 1798.130, that providing information beyond the 12-month period in a response to a verifiable consumer request is impossible or would involve a disproportionate effort.**

**(10) Issuing regulations further defining and adding to the business purposes, including other notified purposes, for which businesses, service providers, and contractors may use consumers' personal information consistent with consumers' expectations, and further defining the business purposes for which service providers and contractors may combine consumers' personal information obtained from different sources, except as provided for in paragraph (6) of subdivision (e) of Section 1798.140.**

**(11) Issuing regulations identifying those business purposes, including other notified purposes, for which service providers and contractors may use consumers' personal information received pursuant to a written contract with a business, for the service provider or contractor's own business purposes, with the goal of maximizing consumer privacy.**

**(12) Issuing regulations to further define "intentionally interacts," with the goal of maximizing consumer privacy.**

**(13) Issuing regulations to further define "precise geolocation," such as where the size defined is not sufficient to protect consumer privacy in sparsely populated areas, or when the personal information is used for normal operational purposes, such as billing.**

**(14) Issuing regulations to define the term "specific pieces of information obtained from the consumer" with the goal of maximizing a consumer's right to access relevant personal information while minimizing the delivery of information to a consumer that would not be useful to the consumer, such as system log information and other technical data. For delivery of the most sensitive personal information, the regulations may require a higher standard of authentication, provided that the agency shall monitor the impact of the higher standard on the right of consumers to obtain their personal information to ensure that the requirements of verification do not result in the unreasonable denial of verifiable consumer requests.**

**(15) Issuing regulations requiring businesses whose processing of consumers' personal information presents significant risk to consumers' privacy or security, to: (A) perform a cybersecurity audit on an annual basis, including defining the scope of the audit and establishing a process to ensure that audits are thorough and independent. The factors to be considered in determining when processing may result in significant risk to the security of personal information shall include the size and complexity of the business and the nature and scope of processing activities,**

**(B) submit to the California Privacy Protection Agency on a regular basis a risk assessment with respect to their processing of personal information, including whether the processing involves sensitive personal information, and identifying and weighing the benefits resulting from the processing to the business, the consumer, other stakeholders, and the public, against the potential risks to the rights of the consumer associated with such processing, with the goal**

*of restricting or prohibiting such processing if the risks to privacy of the consumer outweigh the benefits resulting from processing to the consumer, the business, other stakeholders, and the public. Nothing in this section shall require a business to divulge trade secrets.*

*(16) Issuing regulations governing access and opt-out rights with respect to businesses' use of automated decision-making technology, including profiling and requiring businesses' response to access requests to include meaningful information about the logic involved in such decision-making processes, as well as a description of the likely outcome of the process with respect to the consumer.*

*(17) Issuing regulations to further define a "law enforcement agency-approved investigation" for purposes of the exception in paragraph (2) of subdivision (a) of Section 1798.145.*

*(18) Issuing regulations to define the scope and process for the exercise of the agency's audit authority, to establish criteria for selection of persons to audit, and to protect consumers' personal information from disclosure to an auditor, in the absence of a court order, warrant, or subpoena.*

*(19) (A) Issuing regulations to define the requirements and technical specifications for an opt-out preference signal sent by a platform, technology, or mechanism, to indicate a consumer's intent to opt-out of the sale or sharing of the consumer's personal information and to limit the use or disclosure of the consumer's sensitive personal information. The requirements and specifications for the opt-out preference signal should be updated from time to time to reflect the means by which consumers interact with businesses, and should: (i) ensure that the manufacturer of a platform or browser or device that sends the opt-out preference signal cannot unfairly disadvantage another business; (ii) ensure that the opt-out preference signal is consumer-friendly, clearly described, and easy to use by an average consumer, and does not require that the consumer provide additional information beyond what is necessary; (iii) clearly represent a consumer's intent and be free of defaults constraining or presupposing such intent; (iv) ensure that the opt-out preference signal does not conflict with other commonly-used privacy settings or tools that consumers may employ; (v) provide a mechanism for the consumer to selectively consent to a business's sale of the consumer's personal information, or the use or disclosure of the consumer's sensitive personal information, without affecting their preferences with respect to other businesses or disabling the opt-out preference signal globally; and (vi) state that in the case of a page or setting view which the consumer accesses to set the opt-out preference signal, the consumer should see up to three choices, including (a) a global opt-out from sale and sharing of personal information, including a direction to limit the use of sensitive personal information; (b) a choice to "Limit The Use Of My Sensitive Personal Information"; and (c) a choice titled "Do Not Sell/Do Not Share/Do Not Share My Personal Information for Cross-Context Behavioral Advertising."*

*(B) Issuing regulations to establish technical specifications for an opt-out preference signal that allows the consumer, or the consumer's parent or guardian, to specify that the consumer is less than 13 years of age or at least 13 years of age and less than 16 years of age.*

*(C) Issuing regulations, with the goal of strengthening consumer privacy, while considering the legitimate operational interests of businesses, to govern the use or disclosure of a consumer's sensitive personal information, notwithstanding the consumer's direction to limit the use or disclosure of the consumer's sensitive personal information, including: (i) determining any additional purposes for which a business may use or disclose a consumer's sensitive personal information; (ii) determining the scope of activities permitted under paragraph (8) of*

*subdivision (e) of Section 1798.140, as authorized by subdivision (a) of Section 1798.121, to ensure that the activities do not involve health-related research; (iii) ensuring the functionality of the business's operations; and (iv) ensuring that the exemption in subdivision (d) of Section 1798.121 for sensitive personal information applies to information that is collected or processed incidentally, or without the purpose of inferring characteristics about a consumer, while ensuring that businesses do not use the exemption for the purpose of evading consumers' rights to limit the use and disclosure of their sensitive personal information under Section 1798.121.*

*(20) Issuing regulations to govern how a business that has elected to comply with subdivision (b) of Section 1798.135 responds to the opt-out preference signal and provides consumers with the opportunity subsequently to consent to the sale or sharing of their personal information or the use and disclosure of their sensitive personal information for purposes in addition to those authorized by subdivision (a) of Section 1798.121. The regulations should: (A) strive to promote competition and consumer choice and be technology neutral; (B) ensure that the business does not respond to an opt-out preference signal by: (i) intentionally degrading the functionality of the consumer experience; (ii) charging the consumer a fee in response to the consumer's opt-out preferences; (iii) making any products or services not function properly or fully for the consumer, as compared to consumers who do not use the opt-out preference signal; (iv) attempting to coerce the consumer to opt-in to the sale or sharing of their personal information, or the use or disclosure of their sensitive personal information, by stating or implying that the use of the opt-out preference signal will adversely affect the consumer as compared to consumers who do not use the opt-out preference signal, including stating or implying that the consumer will not be able to use the business's products or services, or that such products or services may not function properly or fully; or (v) displaying any notification or pop-up in response to the consumer's opt-out preference signal; and (C) ensure that any link to a webpage or its supporting content that allows the consumer to consent to opt-in: (i) is not part of a popup, notice, banner, or other intrusive design that obscures any part of the webpage the consumer intended to visit from full view, or that interferes with or impedes in any way the consumer's experience visiting or browsing the webpage or website the consumer intended to visit; (ii) does not require or imply that the consumer must click the link to receive full functionality of any products or services, including the website; (iii) does not make use of any dark patterns; and (iv) applies only to the business with which the consumer intends to interact. The regulation should strive to curb coercive or deceptive practices in response to an opt-out preference signal but should not unduly restrict businesses that are trying in good faith to comply with Section 1798.135.*

*(21) Review existing California Insurance Code provisions and regulations relating to consumer privacy, except those relating to insurance rates or pricing, to determine whether any provisions of the Insurance Code provide greater protection to consumers than the provisions of this Title. Upon completing its review, the Agency shall adopt a regulation that applies only the more protective provisions of this Title to insurance companies. For the purpose of clarity, the Insurance Commissioner shall have jurisdiction over insurance rates and pricing.*

*(22) Harmonizing the regulations governing opt-out mechanisms, notices to consumers, and other operational mechanisms in this title to promote clarity and the functionality of this title for consumers.*

*(b) The Attorney General may adopt additional regulations as necessary to further the purposes of this title.*

(c) The Attorney General shall not bring an enforcement action under this title until six months after the publication of the final regulations issued pursuant to this section or July 1, 2020, whichever is sooner.

***(d) Notwithstanding subdivision (a), the timeline for adopting final regulations required by the Act adding this subdivision shall be July 1, 2022. Beginning the later of July 1, 2021, or six months after the Agency provides notice to the Attorney General that it is prepared to begin rulemaking under this title, the authority assigned to the Attorney General to adopt regulations under this section shall be exercised by the California Privacy Protection Agency. Notwithstanding any other law, civil and administrative enforcement of the provisions of law added or amended by this Act shall not commence until July 1, 2023, and shall only apply to violations occurring on or after that date. Enforcement of provisions of law contained in the California Consumer Privacy Act of 2018 amended or reenacted by this Act shall remain in effect and shall be enforceable until the same provisions of this Act become enforceable.***

**SEC. 22. Section 1798.190 of the Civil Code is amended to read:**

***1798.190. Anti-Avoidance***

***1798.190. A court or the Agency shall disregard the intermediate steps or transactions for purposes of effectuating the purposes of this title: (a) if ~~if~~ a series of steps or transactions were component parts of a single transaction intended from the beginning to be taken with the intention of avoiding the reach of this title, including the disclosure of information by a business to a third party in order to avoid the definition of sell or share; or (b) if steps or transactions were taken to purposely avoid the definition of sell or share by eliminating any monetary or other valuable consideration, including by entering into contracts that do not include an exchange for monetary or other valuable consideration, but where a party is obtaining something of value or use a court shall disregard the intermediate steps or transactions for purposes of effectuating the purposes of this title.***

**SEC. 23. Section 1798.192 of the Civil Code is amended to read:**

***1798.192. Waiver***

***1798.192. Any provision of a contract or agreement of any kind, including a representative action waiver, that purports to waive or limit in any way a consumer's rights under this title, including, but not limited to, any right to a remedy or means of enforcement, shall be deemed contrary to public policy and shall be void and unenforceable. This section shall not prevent a consumer from declining to request information from a business, declining to opt-out of a business's sale of the consumer's personal information, or authorizing a business to sell or share the consumer's personal information after previously ~~opting out~~ opting-out.***

**SEC. 24. Section 1798.199.10 et seq. are added to the Civil Code to read as follows:**

***Establishment of California Privacy Protection Agency***

***1798.199.10. (a) There is hereby established in state government the California Privacy Protection Agency, which is vested with full administrative power, authority, and jurisdiction to implement and enforce the California Consumer Privacy Act. The Agency shall be governed by a five-member board, including the Chair. The Chair and one member of the board shall be appointed by the Governor. The Attorney General, Senate Rules Committee, and Speaker of the Assembly shall each appoint one member. These appointments should be made from among Californians with expertise in the areas of privacy, technology, and consumer rights.***

***(b) The initial appointments to the Agency shall be made within 90 days of the effective date of the Act adding this section.***

**1798.199.15. Members of the Agency board shall:**

***(a) have qualifications, experience and skills, in particular in the areas of privacy and technology, required to perform the duties of the Agency and exercise its powers;***

***(b) maintain the confidentiality of information which has come to their knowledge in the course of the performance of their tasks or exercise of their powers, except to the extent that disclosure is required by the Public Records Act;***

***(c) remain free from external influence, whether direct or indirect, and shall neither seek nor take instructions from another;***

***(d) refrain from any action incompatible with their duties and engaging in any incompatible occupation, whether gainful or not, during their term;***

***(e) have the right of access to all information made available by the Agency to the Chair;***

***(f) be precluded, for a period of one year after leaving office, from accepting employment with a business that was subject to an enforcement action or civil action under this Title during the member's tenure or during the five-year period preceding the member's appointment; and***

***(g) be precluded for a period of two years after leaving office, from acting, for compensation, as an agent or attorney for, or otherwise representing any other person in a matter pending before the Agency if the purpose is to influence an action of the Agency.***

**1798.199.20. Members of the Agency board, including the Chair, shall serve at the pleasure of their appointing authority but shall serve for no longer than eight consecutive years.**

**1798.199.25. For each day on which they engage in official duties, members of the Agency board shall be compensated at the rate of one hundred dollars (\$100), adjusted biennially to reflect changes in the cost of living, and shall be reimbursed for expenses incurred in performance of their official duties.**

**1798.199.30. The Agency board shall appoint an executive director who shall act in accordance with Agency policies and regulations and with applicable law. The Agency shall appoint and discharge officers, counsel, and employees, consistent with applicable civil service laws, and shall fix the compensation of employees and prescribe their duties. The Agency may contract for services that cannot be provided by its employees.**

**1798.199.35. The Agency board may delegate authority to the Chair or the executive director to act in the name of the Agency between meetings of the Agency, except with respect to resolution of enforcement actions and rulemaking authority.**

**1798.199.40. The Agency shall perform the following functions:**

***(a) Administer, implement, and enforce through administrative actions, Title 1.81.5 (commencing with Section 1798.100) to Part 4 of Division 3 of the Civil Code.***

***(b) On and after the earlier of July 1, 2021, or within six months of the Agency providing the Attorney General with notice that it is prepared to assume rulemaking responsibilities under this title, adopt, amend, and rescind regulations pursuant to Section 1798.185 to carry out the***

*purposes and provisions of the California Consumer Privacy Act, including regulations specifying record keeping requirements for businesses to ensure compliance with this title.*

*(c) Through the implementation of this title, protect the fundamental privacy rights of natural persons with respect to the use of their personal information.*

*(d) Promote public awareness and understanding of the risks, rules, responsibilities, safeguards, and rights in relation to the collection, use, sale and disclosure of personal information, including the rights of minors with respect to their own information, and provide a public report summarizing the risk assessments filed with the Agency pursuant to paragraph (15) of subdivision (a) of Section 1798.185 while ensuring that data security is not compromised.*

*(e) Provide guidance to consumers regarding their rights under this title.*

*(f) Provide guidance to businesses regarding their duties and responsibilities under this title, and appoint a Chief Privacy Auditor to conduct audits of businesses to ensure compliance with this title pursuant to regulations adopted pursuant to paragraph (18) of subdivision (a) of Section 1798.185.*

*(g) Provide technical assistance and advice to the Legislature, upon request, with respect to privacy-related legislation.*

*(h) Monitor relevant developments relating to the protection of personal information, and in particular, the development of information and communication technologies and commercial practices.*

*(i) Cooperate with other agencies with jurisdiction over privacy laws and with data processing authorities in California, other states, territories, and countries to ensure consistent application of privacy protections.*

*(j) Establish a mechanism pursuant to which persons doing business in California that do not meet the definition of business set forth in paragraphs (1), (2), or (3) of subdivision (d) of section 1798.140 may voluntarily certify that they are in compliance with this title, as set forth in paragraph (4) of subdivision (d) of Section 1798.140, and make a list of such entities available to the public.*

*(k) Solicit, review, and approve applications for grants to the extent funds are available pursuant to paragraph (2) of subdivision (b) of Section 1798.160.*

*(l) Perform all other acts necessary or appropriate in the exercise of its power, authority, and jurisdiction, and seek to balance the goals of strengthening consumer privacy while giving attention to the impact on businesses.*

*1798.199.45. Upon the sworn complaint of any person or on its own initiative, the Agency may investigate possible violations of this title relating to any business, service provider, contractor, or person. The Agency may decide not to investigate a complaint or decide to provide a business with a time-period to cure the alleged violation. In making a decision not to investigate or provide more time to cure, the Agency may consider: (a) the lack of intent to violate this title; and (b) voluntary efforts undertaken by the business, service provider, contractor, or person to cure the alleged violation prior to being notified by the Agency of the complaint. The Agency shall notify in writing the person who made the complaint of the action, if any, the Agency has taken or plans to take on the complaint, together with the reasons for such action or non-action.*

**1798.199.50. No finding of probable cause to believe this title has been violated shall be made by the Agency unless, at least 30 days prior to the Agency's consideration of the alleged violation, the business, service provider, contractor, or person alleged to have violated this title is notified of the violation by service of process or registered mail with return receipt requested, provided with a summary of the evidence, and informed of their right to be present in person and represented by counsel at any proceeding of the Agency held for the purpose of considering whether probable cause exists for believing the person violated this title. Notice to the alleged violator shall be deemed made on the date of service, the date the registered mail receipt is signed, or if the registered mail receipt is not signed, the date returned by the post office. A proceeding held for the purpose of considering probable cause shall be private unless the alleged violator files with the Agency a written request that the proceeding be public.**

**1798.199.55. (a) When the Agency determines there is probable cause for believing this title has been violated, it shall hold a hearing to determine if a violation has or violations have occurred. Notice shall be given and the hearing conducted in accordance with the Administrative Procedure Act (Chapter 5 (commencing with Section 11500), Part 1, Division 3, Title 2, Government Code). The Agency shall have all the powers granted by that chapter. If the Agency determines on the basis of the hearing conducted pursuant to this subdivision that a violation or violations have occurred, it shall issue an order that may require the violator to do all or any of the following:**

**(1) Cease and desist violation of this title.**

**(2) Subject to Section 1798.155, pay an administrative fine of up to two thousand five hundred dollars (\$2,500) for each violation, or up to seven thousand five hundred dollars (\$7,500) for each intentional violation and each violation involving the personal information of minor consumers to the Consumer Privacy Fund within the General Fund of the state. When the Agency determines that no violation has occurred, it shall publish a declaration so stating.**

**(b) If two or more persons are responsible for any violation or violations, they shall be jointly and severally liable.**

**1798.199.60. Whenever the Agency rejects the decision of an administrative law judge made pursuant to Section 11517 of the Government Code, the Agency shall state the reasons in writing for rejecting the decision.**

**1798.199.65. The Agency may subpoena witnesses, compel their attendance and testimony, administer oaths and affirmations, take evidence and require by subpoena the production of any books, papers, records or other items material to the performance of the Agency's duties or exercise of its powers, including but not limited to its power to audit a business's compliance with this title.**

**1798.199.70. No administrative action brought pursuant to this title alleging a violation of any of the provisions of this title shall be commenced more than five years after the date on which the violation occurred.**

**(a) The service of the probable cause hearing notice, as required by Section 1798.199.50, upon the person alleged to have violated this title shall constitute the commencement of the administrative action.**

**(b) If the person alleged to have violated this title engages in the fraudulent concealment of his or her acts or identity, the five-year period shall be tolled for the period of the**

**concealment. For purposes of this subdivision, "fraudulent concealment" means the person knows of material facts related to their duties under this title and knowingly conceals them in performing or omitting to perform those duties, for the purpose of defrauding the public of information to which it is entitled under this title.**

**(c) If, upon being ordered by a superior court to produce any documents sought by a subpoena in any administrative proceeding under this title, the person alleged to have violated this title fails to produce documents in response to the order by the date ordered to comply therewith, the five-year period shall be tolled for the period of the delay from the date of filing of the motion to compel until the date the documents are produced.**

**1798.199.75. (a) In addition to any other available remedies, the Agency may bring a civil action and obtain a judgment in superior court for the purpose of collecting any unpaid administrative fines imposed pursuant to this title after exhaustion of judicial review of the Agency's action. The action may be filed as a small claims, limited civil, or unlimited civil case, depending on the jurisdictional amount. The venue for this action shall be in the county where the administrative fines were imposed by the Agency. In order to obtain a judgment in a proceeding under this section, the Agency shall show, following the procedures and rules of evidence as applied in ordinary civil actions, all of the following:**

**(1) That the administrative fines were imposed following the procedures set forth in this title and implementing regulations.**

**(2) That the defendant or defendants in the action were notified, by actual or constructive notice, of the imposition of the administrative fines.**

**(3) That a demand for payment has been made by the Agency and full payment has not been received.**

**(b) A civil action brought pursuant to subdivision (a) shall be commenced within four years after the date on which the administrative fines were imposed.**

**1798.199.80. (a) If the time for judicial review of a final Agency order or decision has lapsed, or if all means of judicial review of the order or decision have been exhausted, the Agency may apply to the clerk of the court for a judgment to collect the administrative fines imposed by the order or decision, or the order as modified in accordance with a decision on judicial review.**

**(b) The application, which shall include a certified copy of the order or decision, or the order as modified in accordance with a decision on judicial review, and proof of service of the order or decision, constitutes a sufficient showing to warrant issuance of the judgment to collect the administrative fines. The clerk of the court shall enter the judgment immediately in conformity with the application.**

**(c) An application made pursuant to this section shall be made to the clerk of the superior court in the county where the administrative fines were imposed by the Agency.**

**(d) A judgment entered in accordance with this section has the same force and effect as, and is subject to all the provisions of law relating to, a judgment in a civil action and may be enforced in the same manner as any other judgment of the court in which it is entered.**

**(e) The Agency may bring an application pursuant to this section only within four years after the date on which all means of judicial review of the order or decision have been exhausted.**

***(f) The remedy available under this section is in addition to those available under any other law.***

***1798.199.85. Any decision of the Agency with respect to a complaint or administrative fine shall be subject to judicial review in an action brought by an interested party to the complaint or administrative fine and shall be subject to an abuse of discretion standard.***

***1798.199.90. (a) Any business, service provider, contractor, or other person that violates this title shall be subject to an injunction and liable for a civil penalty of not more than two thousand five hundred dollars (\$2,500) for each violation or seven thousand five hundred dollars (\$7,500) for each intentional violation and each violation involving the personal information of minor consumers, as adjusted pursuant to paragraph (5) of subdivision (a) of Section 1798.185, which shall be assessed and recovered in a civil action brought in the name of the people of the State of California by the Attorney General. The court may consider the good faith cooperation of the business, service provider, contractor, or other person in determining the amount of the civil penalty.***

***(b) Any civil penalty recovered by an action brought by the Attorney General for a violation of this title, and the proceeds of any settlement of any said action, shall be deposited in the Consumer Privacy Fund.***

***(c) The Agency shall, upon request by the Attorney General, stay an administrative action or investigation under this title to permit the Attorney General to proceed with an investigation or civil action, and shall not pursue an administrative action or investigation, unless the Attorney General subsequently determines not to pursue an investigation or civil action. The Agency may not limit the authority of the Attorney General to enforce this title.***

***(d) No civil action may be filed by the Attorney General under this Section for any violation of this title after the Agency has issued a decision pursuant to Section 1798.199.85 or an order pursuant to Section 1798.199.55 against that person for the same violation.***

***(e) This section shall not affect the private right of action provided for in Section 1798.150.***

***1798.199.95. (a) There is hereby appropriated from the General Fund of the state to the Agency the sum of five million dollars (\$5,000,000) during the fiscal year 2020-2021, and the sum of ten million dollars (\$10,000,000) adjusted for cost-of-living changes, during each fiscal year thereafter, for expenditure to support the operations of the Agency pursuant to this title. The expenditure of funds under this appropriation shall be subject to the normal administrative review given to other state appropriations. The Legislature shall appropriate such additional amounts to the Commission and other agencies as may be necessary to carry out the provisions of this title.***

***(b) The Department of Finance, in preparing the state budget and the Budget Bill submitted to the Legislature, shall include an item for the support of this title, which item shall indicate all of the following: (1) the amounts to be appropriated to other agencies to carry out their duties under this title, which amounts shall be in augmentation of the support items of such agencies; and (2) the additional amounts required to be appropriated by the Legislature to the Agency to carry out the purposes of this title, as provided for in this section; and (3) in parentheses, for informational purposes, the continuing appropriation during each fiscal year of ten million dollars (\$10,000,000), adjusted for cost-of-living changes made pursuant to this section.***

***(c) The Attorney General shall provide staff support to the Agency until such time as the Agency has hired its own staff. The Attorney General shall be reimbursed by the Agency for these services.***

***1798.199.100. The Agency and any court, as applicable, shall consider the good faith cooperation of the business, service provider, contractor, or other person in determining the amount of any administrative fine or civil penalty for a violation of this title. A business shall not be required by the Agency, a court, or otherwise to pay both an administrative fine and a civil penalty for the same violation.***

#### **SEC. 25. Amendment.**

(a) The provisions of this Act may be amended after its approval by the voters by a statute that is passed by a vote of a majority of the members of each house of the Legislature and signed by the Governor, provided that such amendments are consistent with and further the purpose and intent of this Act as set forth in Section 3, including amendments to the exemptions in Section 1798.145 if the laws upon which the exemptions are based are amended to enhance privacy and are consistent with and further the purposes and intent of this Act and amendments to address a decision of a California state or federal court holding that a provision of the Act is unconstitutional or preempted by federal law, provided that any further amendments to legislation that addresses a court holding shall be subject to this subdivision.

(b) Notwithstanding Section 1798.199.25, the Legislature may authorize additional compensation for members of the California Consumer Privacy Agency, if it determines that it is necessary to carry out the Agency's functions, by a statute that is passed by a vote of a majority of the members of each house of the Legislature and signed by the Governor.

(c) This section applies to all statutes amended or reenacted as part of this Act, and all provisions of such statutes, regardless of whether this Act makes any substantive change thereto.

(d) The provisions of this Act shall prevail over any conflicting legislation enacted after January 1, 2020. Any amendments to this Act or any legislation that conflicts with any provision of this Act shall be null and void upon passage of this Act by the voters, regardless of the code in which it appears. Legislation shall be considered "conflicting" for purposes of this subdivision, unless the legislation is consistent with and furthers the purpose and intent of this Act as set forth in Section 3.

#### **SEC. 26. Severability.**

If any provision of this measure, or part of this measure, or the application of any provision or part to any person or circumstances, is for any reason held to be invalid, the remaining provisions, or applications of provisions, shall not be affected, but shall remain in full force and effect, and to this end the provisions of this measure are severable. If a court were to find in a final, unreviewable judgment that the exclusion of one or more entities or activities from the applicability of the Act renders the Act unconstitutional, those exceptions should be severed and the Act should be made applicable to the entities or activities formerly exempt from the Act. It is the intent of the voters that this Act would have been enacted regardless of whether any invalid provision had been included or any invalid application had been made.

**SEC. 27. Conflicting Initiatives.**

(a) In the event that this measure and another measure addressing consumer privacy shall appear on the same statewide ballot, the provisions of the other measure or measures shall be deemed to be in conflict with this measure. In the event that this measure receives a greater number of affirmative votes than a measure deemed to be in conflict with it, the provisions of this measure shall prevail in their entirety, and the other measure or measures shall be null and void.

(b) If this measure is approved by the voters but superseded by law by any other conflicting measure approved by voters at the same election, and the conflicting ballot measure is later held invalid, this measure shall be self-executing and given full force and effect.

**SEC. 28. Standing.**

Notwithstanding any other provision of law, if the State or any of its officials fail to defend the constitutionality of this Act, following its approval by the voters, any other government agency of this State shall have the authority to intervene in any court action challenging the constitutionality of this Act for the purpose of defending its constitutionality, whether such action is in state or federal trial court, on appeal, or on discretionary review by the Supreme Court of California and/or the Supreme Court of the United States. The reasonable fees and costs of defending the action shall be a charge on funds appropriated to the California Department of Justice, which shall be satisfied promptly.

**SEC. 29. Construction.**

This Act shall be liberally construed to effectuate its purposes.

**SEC. 30. Savings Clause.**

This Act is intended to supplement federal and state law, where permissible, but shall not apply where such application is preempted by, or in conflict with, federal law, or the California Constitution. The provisions of the Act relating to children under 16 years of age shall only apply to the extent not in conflict with Children's Online Privacy Protection Act.

**SEC. 31. Effective and Operative Dates.**

(a) This Act shall become effective as provided in subdivision (a) of section 10 of article II of the California Constitution. Except as provided in subdivision (b), this Act shall become operative January 1, 2023, and with the exception of the right of access, shall only apply to personal information collected by a business on or after January 1, 2022.

(b) Subdivisions (m) and (n) of Section 1798.145, Sections 1798.160, 1798.185, 1798.199.10 through 1798.199.40, and 1798.199.95, shall become operative on the effective date of the Act.

(c) The provisions of the California Consumer Privacy Act of 2018, amended or reenacted by this Act, shall remain in full force and effect and shall be enforceable until the same provisions of this Act become operative and enforceable.

## Appendix H

Colleen Theresa Brown, et al.

The Return of the Mac: “CCPA 2.0 Qualifies for California’s November 2020 Ballot and Could Usher In Sweeping Changes to CCPA” (June 26, 2020)

(Reprinted with permission of the publisher)

## DATA MATTERS


Cybersecurity, Privacy, Data Protection, Internet Law and Policy

# SIDLEY

[HOME PAGE](#)[OUR PRACTICE](#)[CONTACT US](#)[SIDLEY.COM](#)

26  
June  
2020

## The Return of the Mac: CCPA 2.0 Qualifies for California's November 2020 Ballot and Could Usher In Sweeping Changes to CCPA

 COLLEEN THERESA BROWN, CHRISTOPHER FONZONE, KATE HEINZELMAN, ALAN CHARLES RAUL, SHERI PORATH ROCKWELL AND CHRISTOPHER D. JOYCE

 CCPA, CPRA, ENFORCEMENT, LEGISLATION, POLICY, U.S. STATE LAW

The California Privacy Rights Act (CPRA), a proposed initiative to codify far-reaching amendments to the California Consumer Privacy Act (CCPA) and sometimes referred to as "CCPA 2.0", is back in play and heading to the November 2020 ballot. A series of dramatic procedural twists and turns culminated with initiative backers successfully obtaining a writ of mandate directing the Secretary of State to direct counties to verify signatures for the ballot proposal by the June 25th Constitutional deadline. This verification involved each county conducting a random sample of the more than 800,000 signatures that proponents had submitted to place the initiative on the ballot.

Before the California court's ruling, observers were skeptical that signatures could be verified before the

### CONTACTS

**Colleen Theresa Brown**

Washington, D.C.

+1 202 736 8465

[ctbrown@sidley.com](mailto:ctbrown@sidley.com)

**John M. Casanova**

Singapore

London

+65 6230 3907

[jcasanova@sidley.com](mailto:jcasanova@sidley.com)

**Tomoki Ishiara**

Tokyo

+81 3 3218 5014

[tishiara@sidley.com](mailto:tishiara@sidley.com)

**Richard D. Klingler**

Washington, D.C.

+1 202 736 8063

[rklingler@sidley.com](mailto:rklingler@sidley.com)

**William RM Long**

London

+44 20 7360 2061

[wlong@sidley.com](mailto:wlong@sidley.com)

deadline. Initiative proponents were almost two weeks behind the recommended schedule when they delivered signatures to be verified by California's 58 counties. This meant counties had until June 26th to verify signatures — a day *after* the June 25th Constitutional deadline. Experience with other initiatives this year had shown that several large counties were waiting until the deadline to complete verifications, so proponents petitioned the court to push the deadline up by a day in order to meet the Constitutional deadline. The court agreed to do so, finding good cause existed to force counties to complete verifications a day early. And, as it happened, the extra time was not needed, as counties finished the count two days ahead of their initial deadline.

#### *Next Steps – Initiative Likely to Pass, But Critics Have Been Vocal*

CPRA will be on the ballot this November and has a strong chance of passing. According to polls conducted by proponents in late 2019, 88 % of California voters reported they would vote in favor of the initiative. Nevertheless, many oppose the initiative – including some proponents of the original CCPA – because it will rewrite much of the CCPA before Californians and the business community have much of an opportunity to see how it works. The CCPA went into effect on January 1, 2020, regulations have been [proposed as final but not yet been finalized](#), and July 1st is the first day that the Attorney General can bring any enforcement action. Arguments against the initiative were heard at a June 19th hearing in the state Assembly which was required under state initiative law, but is not expected to result in the initiative being pulled from the November 2020 ballot.

#### *Impacts on Businesses if Voters Approve CPRA*

#### **Geeta Malhotra**

Chicago

+1 312 853 7683

[cmalhotra@sidley.com](mailto:cmalhotra@sidley.com)

#### **Alan Charles Raul**

Washington, D.C.

+1 202 736 8477

[araul@sidley.com](mailto:araul@sidley.com)

#### **Yuet Ming Tham**

Hong Kong

Singapore

+852 2509 7645

[yuetming.tham@sidley.com](mailto:yuetming.tham@sidley.com)

#### **John K. Van De Weert**

Washington, D.C.

+1 202 736 8094

[jvandeweert@sidley.com](mailto:jvandeweert@sidley.com)

### **RECENT POSTS**

#### **[The Swiss Parliament Agrees on the Draft Bill of a New Data Protection Act](#)**

 Sep 25 2020

#### **[Swiss Parliament Fails to Reach Agreement on New Swiss Data Protection Act](#)**

 Sep 22 2020

#### **[New Rules on CFIUS Mandatory Filings](#)**

 Sep 21 2020

If the CPRA passes, businesses will need to gear up to comply with several amendments to the CCPA that go into effect January 1, 2023. In the short term, the CPRA will help businesses by preserving through 2022 the employee and business-to-business exemptions that are otherwise scheduled to sunset on December 31, 2020.

Substantively, the CPRA will usher in a new era in California privacy law through the creation of the first state data privacy agency in the United States, with the power to implement and enforce the amended CCPA. It will also change the CCPA in several significant respects, some of which we highlight below:

### **New Duties Imposed on Businesses That Collect Personal Information and Their Service Providers.**

*Data Minimization.* The business's collection, use, retention and sharing of personal information would be required to be "reasonably necessary and proportionate to achieve the purposes for which the personal information was collected or processed." Proposed Cal. Civ. Code § 1798.100(a)(3). **1**

*Data Retention Disclosure.* Businesses would be required, at or before the point of collection, to inform consumers as to the length of time the business intends to retain each category of personal information. *Id.*

*Deletion Requests Sent to Third Parties and Service Providers.* Businesses would be required to communicate deletion requests to third parties to whom the business has sold or shared such personal information, to delete the consumer's personal information, unless this proves impossible or involves disproportionate effort." § 1798.105(c)(1). Service providers would be required to do the same with any of their service providers, contractors, or third parties. § 1798.105(c)(3).

*Data Security and Cooperation with Data Subject Requests Codified for Service Providers and Third Parties.* The CPRA would require businesses to contractually bind service providers, contractors and third parties to cooperate with responses to data subject requests and to maintain the same level of privacy protection (e.g., reasonable security) as is required of businesses under CCPA. § 1798.100(d). This may not be a significant change as a practical matter, as many businesses have already included such provisions in CCPA service provider addendums and related contracts.

### **New Rights for Sensitive Personal Information**

CPRA would add a new category of “sensitive personal information” to the CCPA and give consumers the ability to opt-out of the sharing or sale of that information, in ways similar to the existing CCPA right to opt out of the “sale” of personal information generally.

“Sensitive personal information” is defined under the CPRA with reference to specific categories of data that include, without limitation, precise geolocation data, social security and passport numbers, financial account information, customer log-in data with a password, information revealing racial or ethnic origin, religious or philosophical beliefs, or union membership; health data; and the content of a consumer’s mail, email, and text messages unless the business is the intended recipient. See § 1798.140(v)(L)

Businesses would need to make separate disclosures for sensitive personal information (§ 1798.100(a)(2)) and provide opt-out rights allowing consumers to stop businesses from using or disclosing personal information through an additional opt-out link entitled “Limit the Use of My Sensitive Personal Information.” §§ 1798.121(a) and 1798.135(a)(2).

**Opt-In Consent to Share for Cross-Context Behavioral Advertising or Sell Children's Information.** A business would be prohibited from sharing for cross-context behavioral advertising or selling personal information of children under 16 years old without consent of a parent (under 13) or the child (13 to 15 year olds). Additionally, fines for violations involving the personal information of minors would be increased and would apply to service providers, contractors and others. §§ 1798.120(c), 1798.199.90.

**Behavioral Advertising Opt-Out.** Consumers would be able to opt out of cross-context behavior advertising through an additional opt-out option entitled "Do Not Sell/Do Not Share/Do Not Share My Personal Information for Cross-Context Behavioral Advertising." § 1798.185(a)(19). The CPRA defines cross-context behavioral advertising as the targeting of advertising to a consumer based on the consumer's personal information obtained from the consumer's activity across businesses, distinctly-branded websites, applications, or services, other than the business, distinctly-branded website, application, or service with which the consumer intentionally interacts. § 1798.140(k).

**Annual Cybersecurity Audits and Regular Risk Assessments for High Risk Data Processors.**

Businesses whose processing of consumers' personal information "presents a significant risk to consumers' privacy or security" would be required to perform annual cybersecurity audits and submit to the new California data protection agency, "on a regular basis," risk assessments weighing the benefits of processing personal information to the business, the consumer, other stakeholders, and the public, against the potential risks to the consumer. § 1798.185(a)(15).

**Expands Data Breach Liability to Include Email Addresses With Passwords.** CPRA extends potential

liability for data breaches beyond current California law by expanding the private right of action to include data breaches involving email addresses with a password or other security questions and answers that would permit access to the account. § 1798.150(a)(1). This is a potentially significant expansion, as emails and passwords are often involved in data breaches.

**Businesses Subject to CCPA.** CPRA would modify the definition of, and create the following new categories of, a “business”:

*Joint Venture/Partnerships:* “A joint venture or partnership composed of businesses in which each business has a least a 40 percent interest.” There is no requirement of co-branding. The joint venture or partnership and each business “that composes [sic] the joint venture or partnership shall separately be considered a single business.” However, personal information “in the possession of each business and disclosed to the joint venture or partnership “shall not be shared with the other business.” § 1798.140(d)(3).

*Self-Certifying Entities:* Businesses that do not meet the threshold criteria to qualify as a CCPA business could voluntarily certify that they are compliant with the CCPA and agree to be bound by the law. Their names will be made available to the public. § 1798.140(d)(4).

*Reasonableness Requirement for Common Branding:* The “common branding” element of the existing alternative definition of a “business” that controls or is controlled by another business that does business in California and meets CCPA monetary or data thresholds would be modified to include a requirement that “the average consumer would understand that two or more entities are commonly owned.” § 1798.140(d)(2).

**Compliance Efforts Should Begin Soon After Passage**

While most of the CPRA would not go into effect until January 2023, obligations of businesses with respect to the personal information covered by the amended CCPA would relate to personal information collected beginning in January 2022. § 1798.130(a)(2)(B).

---

<sup>1</sup> All code references hereinafter are to the CPRA's proposed amendments to California Civil Code.



< [French Council of State Upholds €50m CNIL Fine against Google](#)  
[Key Takeaways From Sidley's Privacy and Cybersecurity Monitor-Side Chat](#)  
[Featuring Bruno Gencarelli, Head of International Data Flows and Protection](#)  
[at the European Commission](#) >

## Appendix I

*In Re: Capital One Consumer Data Security Breach Litigation*, MDL No.  
1:19md2915 (AJT/JFA) (E.D. Va. June 25, 2020) (Memorandum Opinion and Order)

IN THE UNITED STATES DISTRICT COURT  
FOR THE EASTERN DISTRICT OF VIRGINIA  
Alexandria Division

IN RE: CAPITAL ONE CONSUMER )  
DATA SECURITY BREACH LITIGATION ) MDL No. 1:19md2915 (AJT/JFA)  
\_\_\_\_\_)

This Document Relates to CONSUMER Cases  
\_\_\_\_\_

**MEMORANDUM OPINION AND ORDER**

Defendants Capital One Financial Corporation, Capital One Bank (USA), N.A., and Capital One, N.A. (collectively, “Capital One”) have filed Rule 72 Objections to Order Granting Plaintiffs’ Motion to Compel Production of Mandiant Report [Doc. 556], together with an accompanying memorandum [Doc. 558] (sealed) (“Objections” or “Objs.”). In its Objections, Capital One objects to the Memorandum Opinion and Order dated May 26, 2020 [Doc. 490] (the “Order”) entered by Magistrate Judge John Anderson, granting Plaintiffs’ Motion to Compel Production of the Mandiant Report [Doc. 412].

Upon plenary, *de novo* review of the Order, the Objections, the memoranda in support thereof and in opposition thereto, and for the reasons stated below, the Court concludes that the Order is neither clearly erroneous nor contrary to law, and the Objections are **OVERRULED**, the Order is **AFFIRMED**, and Capital One will be ordered to produce the Mandiant Report pursuant to the terms of the Protective Order entered in this action.

**I. BACKGROUND**

After a *de novo* review of the record, the Court adopts the factual findings set forth in the Order, summarized herein, and makes such additional findings as reflected in this Memorandum Opinion and Order:

On November 30, 2015, Capital One entered into a Master Services Agreement (“MSA”) with FireEye, Inc., d/b/a Mandiant (“Mandiant”). Under that MSA, Capital One, and Mandiant entered into a series of Statements of Work (“SOWs”), including a Statement of Work dated January 7, 2019 (the “2019 SOW”). A key purpose of the MSA and SOWs was to ensure that, in the event of a cybersecurity incident, Capital One could respond quickly. To that end, the SOWs directed Mandiant to provide incident response services, which are broadly characterized as computer security incident response support; digital forensics, log, and malware analysis support; and incident remediation assistance. In addition, under the SOWs, Mandiant is to provide a final report covering these issues and should one be necessary, a written technical document outlining the results and recommendations for remediation. Capital One paid Mandiant for this work from a Capital One fund denominated “business critical” expenses. [Doc. 416-3] at 13.

In July 2019, Capital One confirmed that it had experienced a data breach, and on July 20, 2019, Capital One retained the law firm Debevoise & Plimpton LLP (“Debevoise”) to provide legal advice in connection with that incident. On July 24, 2019, Capital One and Debevoise signed a Letter Agreement with Mandiant under which Mandiant would provide services and advice, “as directed by counsel,” in the areas of (1) computer security incident response; (2) digital forensics, log, and malware analysis; and (3) incident remediation, reflecting the same scope of work Mandiant had already agreed to provide under the MSA and SOWs. The Letter Agreement also provided that Mandiant would be paid based on the payment terms set out in the 2019 SOW, and “[l]ikewise, unless inconsistent with the terms of this Letter, [Debevoise], [Capital One], and Mandiant will abide by the applicable terms set forth in [the 2019 SOW] and the [MSA],” dated November 30, 2015. On July 26, 2019, Capital One,

Debevoise, and Mandiant executed an Addendum to the Letter Agreement that purported to expand the engagement to include “penetration testing of systems and endpoints.” Unlike the MSA and prior SOWs, however, the Letter Agreement provided that all work completed by Mandiant was to be conducted at the direction of Debevoise (not Capital One) and that any deliverables were to be produced directly to Debevoise (not Capital One).

On September 4, 2019, Mandiant issued its report pursuant to the Letter Agreement and Addendum (the “Report”). Initially, the Report was sent directly to Debevoise and later, by Debevoise or at Debevoise’s direction, to Capital One’s legal department, its Board of Directors, its financial regulators, its outside auditor, and dozens of Capital One employees. Mandiant was paid for the services reflected in the Report from a retainer Mandiant had already received from Capital One under the 2019 SOW, and after that retainer had been exhausted, with funds paid directly by Capital One from its Cyber budget, which payments were later re-designated as legal expenses.

On June 9, 2020, Capital One, pursuant to Federal Rule of Civil Procedure 72, filed its Objections. The sole issue now before the Court is whether the Report is entitled to work product protection.<sup>1</sup>

## **II. LEGAL STANDARD**

### **A. Federal Rule of Civil Procedure 72(a)**

Rule 72(a) permits a party to submit objections to a magistrate judge’s ruling on non-dispositive matters such as discovery orders. Fed. R. Civ. P. 72(a); *see also* 28 U.S.C. § 636(b)(1)(A).

---

<sup>1</sup> As agreed, on June 12, 2020, Plaintiffs submitted their response [Doc. 566] (“Opp.”); and on June 16, 2020, Capital One, who has waived a hearing on the Objections [Doc. 555], submitted a reply [Doc. 577] (“Reply”). Accordingly, the Objections are ripe for review.

When presented with an objection under Rule 72, the district court is to review the objected-to order under the “clearly erroneous or contrary to law” standard. 28 U.S.C. § 636(b)(1)(A); *see Malletier v. Haute Diggity Dog, LLC*, 2007 U.S. Dist. LEXIS 14244, 2007 WL 676222, at \*1 (E.D. Va. Feb. 28, 2007). The Fourth Circuit has held that the “clearly erroneous” standard is deferential and that findings of fact should be affirmed *unless* review of the entire record leaves the reviewing court with “the definite and firm conviction that a mistake has been committed.” *Harman v. Levin*, 772 F.2d 1150, 1153 (4th Cir. 1985) (citing *United States v. U.S. Gypsum Co.*, 333 U.S. 364, 395 (1948)). Meanwhile, a decision is considered “contrary to law” “when it fails to apply or misapplies relevant statutes, case law, or rules of procedure.” *Attard Industries, Inc. v. U.S. Fire Ins. Co.*, 2010 U.S. Dist. LEXIS 80785, 2010 WL 3069799 at \*1 (E.D. Va. Aug. 5, 2010) (citing *DeFazio v. Wallis*, 459 F. Supp. 2d 159, 163 (E.D.N.Y. 2006)). And in this respect, this Court has noted that for questions of law, “there is no practical difference between review under Rule 72(a)’s contrary to law standard and [a] *de novo* standard.” *Bruce v. Hartford*, 21 F. Supp.3d 590, 594 (E.D. Va. 2014) (citing *Robinson v. Quicken Loans Inc.*, 2013 U.S. Dist. LEXIS 56210, 2013 WL 1704839, at \*3 (S.D. W.Va. Apr. 19, 2013)).

In its Objections, Capital One centrally claims that the Magistrate Judge erred as a matter of law with respect to its application of the applicable standard for determining work product protection. Objs. at 12 (“The Magistrate Judge misapplied the Fourth Circuit’s ‘because of’ standard”). Although that application implicates underlying factual findings, none of those facts appear to be materially disputed; and Capital One’s challenge is, in substance, based on an issue

of law. The Court therefore reviews the Objections primarily under the “contrary to law” standard.<sup>2</sup>

### **B. Work Product Protection**

Parties may obtain discovery regarding any nonprivileged matter that is relevant to any party’s claim or defense and is proportional to the needs of the case. Fed. R. Civ. P. 26(b)(1). However, a party may not ordinarily discover documents “that are prepared in anticipation of litigation by or for another party or its representative.” Fed. R. Civ. P. 26(b)(3)(A).

In determining whether a document was created in anticipation of litigation, a court must decide if the document was prepared “*because of* the prospect of litigation when the preparer faces an actual claim or a potential claim following an actual event or series of events that reasonably could result in litigation.” *Nat’l Union Fire Ins. Co. of Pittsburgh, Pa. v. Murray Sheet Metal Co.*, 967 F.2d 980, 984 (4th Cir. 1992) (emphasis added). And where, as here, the relevant document may be used for both litigation and business purposes, the court must determine “the driving force behind the preparation of” the requested document. *Id.* at 984. In that connection, work product that would have otherwise been produced “in the ordinary course of business” does not receive work product immunity. *Nat’l Union*, 967 F.2d at 984 (citing *Goosman v. A. Duie Pyle, Inc.*, 320 F.2d 45, 52 (4th Cir. 1963)).

---

<sup>2</sup> In support of its Objections, Capital One has produced two supplemental declarations, *see* Objs., Exs. A & B; and Plaintiffs challenge whether Capital One can present and the Court should consider new evidence at this point. The Court concludes that it is not precluded from receiving new evidence, *see Harleysville Ins. Co. v. Holding Funeral Home, Inc.*, 2017 U.S. Dist. LEXIS 76486, at \*6, 2017 WL 2210520 (W.D. Va. May 19, 2017) (citing *United States v. Frans*, 697 F.2d 188, 191 n.3 (7th Cir. 1983) (Rule 72(a) “do[es] not necessarily restrict district court review of a magistrate’s findings” and the district court may “receiv[e] additional evidence or conduct[ ] a full review”), and has considered the two recently-submitted declarations. However, as Capital One admits, these declarations only “clarify” the arguments previously raised before the Magistrate Judge and do not introduce either new issues or new arguments not raised below. *See* Objs. at 3, n.2; *see also* Reply at 7 (“Regardless of whether the Court considers the additional evidence, it should still sustain” the Objections); *id.* at 9 (“[W]hile the facts detailed in the . . . declaration sharpen and clarify some of the issues raised in the [May 26 Order], none of the arguments Capital One makes in its Rule 72 Objections relies solely on this new material.”).

In determining the “the driving force behind the preparation of” a particular document, courts have applied what has become known as the *RLI* test, based on the pronouncements in *RLI Insurance Co. v. Conseco, Inc.*, 477 F. Supp. 2d 741, 748 (E.D. Va. 2007). Under the *RLI* test, a court focuses on (1) whether the document at issue was created “when [the] litigation is a real likelihood, [and not] . . . when that litigation is merely a possibility[,]” *RLI*, 477 F. Supp. 2d at 748 (citing *Nat’l Union*, 967 F.2d at 984); and (2) whether the document would have been created in essentially the same form in the absence of litigation, *id.* at 747 (citing *United States v. Adlman*, 134 F.3d 1194, 1195 (2d Cir. 1998) (citing *Nat’l Union*, 967 F.2d at 984)). Ultimately, the party “claiming the protection,” here Capital One, “bears the burden of demonstrating the applicability of the work product doctrine.” *Solis v. Food Employers Labor Relations Ass’n*, 644 F.3d 221, 232 (4th Cir. 2011).

### III. ANALYSIS

In its Objections, Capital One argues that the Magistrate Judge erred as a matter of law because he: (1) applied the second prong of the *RLI* test (whether the document would have been created in essentially the same form absent litigation) as part of the Fourth Circuit’s “driving force” test; (2) relied too heavily on the “pre-existing SOW with Mandiant” to conclude that Mandiant would have performed essentially the same services as “described in the Letter Agreement” with Debevoise; and (3) relied on subsequent regulatory and business uses of the Report in determining that the Report is not entitled work product protection. *Id.* at 7-8. None of these contentions is availing.

As an initial matter, the Court notes that Capital One had previously acknowledged that both prongs of the *RLI* test applied in determining whether work product protection exists for the Report. *See* [Doc. 435] at 10-11 (“To determine whether a document was prepared ‘because of’

the prospect of litigation, this Court must first ask whether Capital One ‘face[d] an actual claim or a potential claim following an actual event or series of events that reasonably could result in litigation. . . [and] [t]he second prong of the Fourth Circuit’s ‘because of’ inquiry asks whether the document ‘would not have been prepared in substantially similar form but for the prospect of that litigation.’”) (quoting *E.I. Du Pont de Nemours & Co. v. Kolon Indus., Inc.*, No. 3:09-cv-58, 2010 WL 1489966, at \*3 (E.D. Va. Apr. 13, 2010) (quoting *RLI*, 477 F. Supp. 2d at 748)). Its current position - that the second prong of the *RLI* test does not apply to the circumstances of this case - is fundamentally at odds with its previous position; and as a result, there is a substantial issue whether Plaintiff is barred from taking that position at this point under the invited error doctrine. *See United States v. Ellis*, 1999 U.S. App. LEXIS 2690, at \*16, 1999 WL 92568 (4th Cir. 1999) (holding that even if the complained-of instructions below were erroneous, defense counsel had invited their use and cannot rely on that error as a basis for relief) (citing *Wilson v. Lindler*, 8 F.3d 173, 175 (4th Cir. 1993) (en banc)).

In any event, Capital One’s view that the second prong of the *RLI* test does not apply in this case is misconceived. In that regard, Capital One contends in substance that where, as here, the work product documents are created only after the prospect of litigation arises, *see* Objs. at 17, the “driving force” test should not include the second prong of the *RLI* test and essentially ends in favor of protection upon determining, as the Magistrate Judge did in this case, that the Report was created in anticipation of litigation. But there is nothing in the “driving force” test that suggests such a limiting gloss. The second prong of the *RLI* test captures one of the core inquiries identified by the Fourth Circuit in *National Union*: whether the work product *would have otherwise been produced* in the ordinary course of business. Indeed, the Fourth Circuit in *Nat’l Union* did not end its analysis upon determining that a document was created in the

presence of foreseeable and likely litigation, but also considered whether the work product would not have been prepared in substantially similar form *but for* the prospect of litigation. *See Nat'l Union*, 967 F.2d at 984. Capital One's argument that the "driving force" test must begin and end with whether litigation was foreseeable ignores the substance of the test articulated in *Nat'l Union*.

As mentioned above, Capital One had previously embraced the *RLI* test as properly reflecting the "because of" or "driving force" standard announced in *Nat'l Union*; and other courts have similarly concluded that the *RLI* test is an appropriate formulation, as does the Court in this case. *See, e.g., In re Dominion Dental Servs. United States*, 429 F. Supp. 3d 190, 192-94 (E.D. Va. 2019) (Nachmanoff, J.); *In re Premiera Blue Cross Customer Data Sec. Breach Litig.*, 296 F. Supp. 3d 1230, 1245 (D. Or. 2017); *see also* Charles Alan Wright, Arthur R. Miller, and Richard L. Marcus, 8 Federal Practice & Procedure § 2024 (2d ed. 1994)) ("The 'because of' standard . . . considers the totality of the circumstances and affords protection when it can fairly be said that the document was created because of anticipated litigation, and would not have been created in substantially similar form but for the prospect of that litigation.") (internal quotations and citations omitted). Therefore, for the above reasons, the Magistrate Judge was correct to apply both prongs of the *RLI* test in assessing Capital One's assertion of work product protection.

In applying the *RLI* test, the Magistrate Judge determined that the first prong was clearly satisfied, finding that "[t]here is no question that at the time Mandiant began its 'incident response services' in July 2019, there was a very real potential that Capital One would be facing substantial claims following its announcement of the data breach." Order at 7. However, as to the second prong of the *RLI* test, the Magistrate Judge determined that Capital One failed to establish that the Report would not have been prepared in substantially similar form but for the prospect of

that litigation. There appears to be no dispute as to the Magistrate’s finding concerning the first prong and, after *de novo* review, the Court concludes, after considering the totality of the evidence, that the Magistrate Judge properly applied the second prong in concluding that the Report did not enjoy work product protection.

Capital One contends that the second prong of the *RLI* test was incorrectly applied as a matter of law because the Magistrate Judge gave dispositive effect to the pre-existing SOW with Mandiant, when in fact, at Debevoise’s instruction, Mandiant changed the nature of its investigation, the scope of work, and its purpose in anticipation of litigation; and as a result, “Mandiant’s investigation and report would have been very different if Capital One had engaged Mandiant to investigate the Cyber Incident for *business* purposes” because, in that scenario, “Mandiant’s investigation would have focused on remediation.” Objs. at 18 (emphasis in original).<sup>3</sup>

But that contention appears hollow in light of the respective scope of services covered under the Letter Agreement and the 2019 SOW,<sup>4</sup> which are identical; and the Addendum [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] *see also*

<sup>3</sup> In this regard, Capital One suggests that a Mandiant report produced at the direction of counsel would pertain to “causation issues pertinent to legal liability determinations.” Objs. at 18. But that explanation does not sufficiently address how such issues fall outside the scope of the 2019 SOW, particularly since issues regarding causation and/or legal liability are grounded in the facts Mandiant was tasked with investigating under the 2019 SOW as part of its incident response services.

<sup>4</sup> [REDACTED]

[REDACTED]

[REDACTED]

Letter Agreement (stating that “unless inconsistent with the terms of this Letter [Agreement], Counsel [Debevoise], Client [Capital One] and Mandiant will abide by the applicable terms set forth in the SOW and Master Services Agreement between Mandiant and Client dated November 30, 2015 . . .”) and Addendum. In fact, the primary difference between the 2019 SOW and the Letter Agreement is a specific reference in the Letter Agreement to the Cyber Incident and the role Debevoise would play. In light of these similarities, the Magistrate Judge found that the Report would have been, in the absence of Debevoise’s involvement, likewise similar, particularly given that the “only significant evidence that Capital One has presented concerning the work Mandiant performed is that the work was at the direction of outside counsel and that the final report was initially delivered to outside counsel.” Order at 8. Those findings were neither clearly erroneous nor contrary to law. In short, no difference between what Mandiant produced and what it would have produced in the ordinary course of business absent Debevoise’s involvement can be reasonably inferred from any differences in substance between the 2019 SOW and Letter Agreement; and Capital One failed to produce evidence sufficient to establish any such likely differences.<sup>5</sup>

---

<sup>5</sup> In support of its position that the Report is substantially different than what Mandiant would have otherwise provided absent the prospect of litigation and Debevoise’s involvement, Capital One points to the relatively short and somewhat conclusory internal report that Capital One’s Cyber Organization team produced in response to the Cyber Incident. [Doc. 558], Ex. 2 (under seal). With this internal report as a backdrop, Capital One cites cases finding work product privilege where there were investigations parallel to counsel-led investigations. But those cases indicate that a parallel investigation was but one factor, among others, in the court’s analysis and generally did not discuss in any detail *how* the parallel investigations materially differed in form or substance from the counsel investigation at issue. *See, e.g., In re Target Corp. Customer Data Sec. Breach Litig.*, 2015 U.S. Dist. LEXIS 151974, 2015 WL 6777384, at \*2 (D. Minn. Oct. 23, 2015) (upholding company’s claim of protection over third-party firm’s investigation when a separate, non-privileged investigation had been conducted to determine “how the breach happened” but only after conducting an *in camera* review); *In re Experian Data Breach Litig.*, 2017 U.S. Dist. LEXIS 162891, 2017 WL 4325583, at \*2 (C.D. Cal. May 18, 2017)). More to the point is that there is nothing in the record in this case that would reasonably suggest that this internal report reflects what Mandiant would have produced absent Debevoise’s involvement. And as the Magistrate Judge correctly concluded, Capital One, who bears the burden, has not provided sufficient evidence to explain whether any parallel investigation by Mandiant *would have been* substantially different in substance than the counsel-led investigation at issue here. Order at 8.

In support of its position that the Magistrate Judge erred as a matter of law in applying the applicable test, Capital One relies on the distinguishing features of two cases denying work product protection to a Mandiant investigative report: *Premera* and *Dominion Dental*. In *Premera*, Mandiant was already conducting a “review [of] Premera’s data management system” when it discovered the data breach at issue, after which it continued its work in investigating the breach; and the court found that Mandiant’s data breach investigation was not protected as work product because “[t]he only thing that appear[ed] to have changed involving Mandiant was the identity of its direct supervisor, from Premera to outside counsel.” *In re Premera*, 296 F. Supp. 3d at 1245. In *Dominion Dental*, Mandiant’s company-client, Mandiant, and the company’s outside counsel had entered into an agreement to do the work done almost a year before discovery of the underlying data breach; and that prior agreement expressly contemplated that Mandiant’s work would be conducted alongside outside counsel. *Dominion Dental*, 429 F. Supp. 3d at 191.

None of the relied upon aspects of either *Premera* or *Dominion Dental* dictates or suggests an opposite result in this case. Although Mandiant did not provide any services pertaining to the data breach incident in this case until after it had entered into the Letter Agreement, unlike in *Premera*, and the MSA and SOWs did not specifically mention working with outside counsel, as in *Dominion Dental*, Capital One failed to establish, like the companies in *Premera* and *Dominion Dental*, that the report Mandiant would have created for Capital One pursuant to its pre-data breach SOW would not have been substantially the same in substance or scope as the report Mandiant prepared for Debevoise. After all, both contractual arrangements were virtually identical; and based on the record in this case, it would be unreasonable to think, given identical contractual obligations under the pre- and post-data breach SOWs, that had

Mandiant not provided to Capital One through Debevoise all the information required under the SOW concerning the breach, it would not have provided that same “business critical” information directly to Capital One in discharge of its obligations under the pre-data breach MSA and SOW. In short, Capital One failed, as did these other companies, to satisfy the “because of” test. *See In re Premera*, 296 F. Supp. 3d at 1244 (“Premera has not shown that . . . the documents would not have been created in substantially similar form but for the prospect of litigation”) (internal quotations omitted); *Dominion Dental*, 429 F. Supp. 3d at 194 (holding that, notwithstanding an affidavit from the company that the Mandiant report would not have been prepared in substantially similar form and may not have been necessary at all without the threat of litigation, Dominion Dental had not carried its burden after noting the “almost identical” description of Mandiant’s services in the statement of work prior to and after the data breach). *Cf. In re Experian Data Breach Litig.*, 2017 WL 4325583, at \*2 (finding that a Mandiant report was entitled to work product protection because “Mandiant’s previous work for Experian was separate from the work it did for Experian regarding this particular data breach,” while not addressing in detail distinctions in the nature and scope of the pre-breach and post-breach Mandiant engagements).

Nor did the Magistrate Judge improperly rely on the Mandiant Report’s post-production distribution.<sup>6</sup> As courts have recognized, post-production disclosures are appropriately probative of the purposes for which the work product was initially produced. *Cf. In re Experian Data Breach Litig.*, 2017 WL 4325583, at \*2 (“If the report was more relevant to Experian’s internal investigation or remediation efforts, as opposed to being relevant to defense of this litigation, then the full report would have been given to that team.”). Here, the Magistrate Judge referenced

---

<sup>6</sup> That distribution was to approximately 50 employees, a “corporate governance office general email box,” Capital One’s Board of Directors, and “four different regulators and to Capital One’s accountant.” Order at 4-5, 8.

that distribution simply to underscore Capital One's business needs for a Mandiant produced report, *see* Order at 8 (the distribution of the Mandiant Report showed "that the results of an independent investigation into the cause and the extent of the data breach was significant for regulatory and business reasons"), not, as Capital One contends, for the purpose of stripping away work product protections from an otherwise protected document.<sup>7</sup> Objs. at 23. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] The Magistrate Judge did not commit legal error when he referred to the Report's post-production disclosures.<sup>8</sup>

In sum, Capital One had determined that it had a business critical need for certain information in connection with a data breach incident, it had contracted with Mandiant to provide that information directly to it in the event of a data breach incident, and after the data breach incident at issue in this action, Capital One then arranged to receive through Debevoise the information it already had contracted to receive directly from Mandiant. The Magistrate

---

<sup>7</sup> Because the Court finds that the Report is not protected work product, it does not address Plaintiffs' alternative positions that Capital One waived protection over the Report or that the Report must be disclosed pursuant to Federal Rule of Civil Procedure 26(b)(3).

<sup>8</sup> Capital One argues that the practical realities created by the Order are "unworkable," especially for heavily-regulated companies like itself. Objs. at 19. Specifically, Capital One contends that the Order "incentivizes companies to either (a) forego keeping an incident response vendor on retainer or (b) hire a new, unfamiliar vendor to investigate any incident from which litigation is expected to result." *Id.* at 19-20; Reply at 11. But that contention ignores the alternatives available to produce and protect work product, either through different vendors, different scopes of work and/or different investigation teams. *See, e.g.,* Objs., Ex. 5 (Ben Kochman, Law360, *It's Getting Harder To Hide Consultants' Data Breach Reports*, available at: <https://www.law360.com/articles/1279264?scroll=1&related=1> (last accessed June 19, 2020) ("[Michael] Phillips [chief claims officer at the cybersecurity analytics company Arceo.ai] agreed that [the Order] still 'provides a road map to preserving privilege in an investigation,' if companies are careful to distinguish data breach investigation reports as a distinct form of communication with their cybersecurity consultants. 'Companies and their security partners should consider creating separate statements of work for breach investigations,' Phillips said, adding that 'a company's data breach investigation process should look and feel different than typical operations with a managed security provider.'")).

Judge, after considering the totality of the evidence, properly concluded that Capital One had not established that the Report was protected work product; and the Order was neither clearly erroneous nor contrary to law.

#### IV. CONCLUSION

For the foregoing reasons, after *de novo* review of the Order, it is hereby

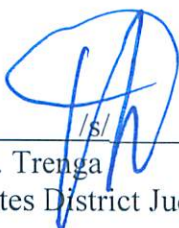
ORDERED that Capital One's Rule 72 Objections to Order Granting Plaintiffs' Motion to Compel Production of Mandiant Report [Doc. 556] be, and the same hereby are,

**OVERRULED** and the Magistrate Judge's Memorandum Opinion and Order [Doc. 490], dated May 26, 2020, be, and the same hereby is, **AFFIRMED**; and it is further

ORDERED that that Capital One provide forthwith a copy of the Mandiant Report to Plaintiffs pursuant to the terms of the Protective Order entered in this action.

The Clerk is directed to docket this Order in the lead case (1:19md2915), as required per PTO-1.

Alexandria, Virginia  
June 25, 2020

  
\_\_\_\_\_  
Anthony J. Trenga  
United States District Judge