

The Sedona Conference WG11 Brainstorming Group Outline - The California Consumer Privacy Act (CCPA): Defining and measuring statutory damages under U.S. privacy laws (Sept. 2019)



The California Consumer Protection Act (CCPA): Defining and Measuring Statutory Damages Under U.S. Privacy Laws (September 2019)

Brainstorming Group:

James J. Pizzirusso (Brainstorming Group Leader)

Mark T. Bailey

Stephen Y. Chow

Alyssa Coon

Stuart A. Davidson

Lydia F. de la Torre

Colton Driver

Eric B. Evans

Eric Goldman

Ross M. Gotler

Amy Keller

Andrew Lucking

Lisa Lukaszewski

Jonathan M. Wilan

Shannon K. Yavorsky

Al Saikali (Steering Committee Liaison)

**The Sedona Conference
WG11 CCPA Brainstorming Group – Question 1**

I. OVERVIEW OF QUESTION 1

Must a consumer show actual harm in addition to a technical violation of the statute before the California Attorney General or a consumer can sue under the California Consumer Protection Act of 2018 (“CCPA”), Cal. Civ. Code §1798.100, *et seq.*? While the CCPA drafters apparently believe that the availability of statutory damages for CCPA violations involving data breaches will satisfy the standing requirement in those situations, it is less clear what, if anything, would satisfy the standing requirement for other types of CCPA violations. A similar issue has arisen in the context of other privacy laws like the Illinois Biometric Information Privacy Act (BIPA). Courts have reached mixed results.

II. ANSWERING THE QUESTION

A. The Statutory Text

1. Scope of the Consumer’s Express Private Right of Action under the CCPA

a. Definition of “Consumer”

The CCPA defines a “Consumer” as “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.” §1798.140(g).

b. The CCPA authorizes a private right of action for Consumers under §1798.150(a) (see attached flowchart at the end of the outline)

“(1) Any consumer whose nonencrypted or 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’ 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."

c. Comments

(1) "Reasonable security procedures and practices"

In §1798.150(a), the CCPA allows a private right of action when there is a breach (see below) of personal information "as a result of the business' 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...." Additional guidance will be necessary to establish what would constitute such "reasonable security procedures and practices." The GDPR ("technical and organisational measures... to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services" Article 32(1)) could provide useful guidance here, as could the Sedona Working Group 11 "Reasonable Security" paper.

(2) "Definition" of breach

The CCPA is narrower than other laws, such as the GDPR, with respect to what constitutes what is colloquially called a "breach" (but is not defined or referred to as such in the CCPA) that may give rise to a cause of action. Mere unauthorized access to information meets the requirements of the GDPR, while the CCPA requires unauthorized access and exfiltration.¹

- (i) CCPA §1798.150(a): "...nonencrypted or nonredacted personal information... subject to an unauthorized access and exfiltration, theft, or disclosure...."
- (ii) GDPR Article 4(12): "'personal data breach' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed[.]"

(3) Notice and Actual Pecuniary Damages

Generally, notice to the AG is required (*inter alia*) before a

¹ Note, however, that in its current format (as of August 22, 2019), the CCPA is unclear if "subject to an unauthorized access and exfiltration, theft, or disclosure" refers to three items: 1) unauthorized access and exfiltration, 2) theft, and 3) disclosure or one item with three options: 1) unauthorized access along with a) exfiltration, b) theft, or c) disclosure.

Consumer may bring a civil action under the CCPA; however, as per §1798.150(b)(1), “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.”

(4) What Constitutes Cure?

CCPA §1798.150(b)(1) allows businesses to avoid an individual action or class action if they “cure” the alleged violations within 30 days of notice.

“Prior to initiating any action against a business for statutory damages on an individual or class-wide basis, a consumer shall provide 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.

What constitutes a “cure” and the meaning of “actually cures” are not detailed in the CCPA, and could be significant questions for ongoing debate, especially in the context of whether the Consumer has cleared the bar to be allowed to bring a private action.

2. Consumer’s Standing Vis-à-vis Other (Non-Breach) Violations of the CCPA

a. Sharing Consumer Information

Cal. Civ. Code §1798.140(d), regulates the “sharing” of information by giving an express exception permitting disclosure of personal information that is “deidentified,” Cal. Civ. Code §1798.145(a)(5).² The statute does

² There is some confusion here as the definition of personal information is broad and, as written, includes essentially everything, even bitstream data. *See* Cal. Civ. Code § 1798.140(o)(1)(f) (Defining “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, application, or advertisement” as personal information.”). Deidentified information, on the other hand, is defined “as information that cannot reasonably identify, relate to, describe, be capable of being associated with, or be linked, directly or indirectly, to a particular consumer.” As a result, it is not clear what can and cannot be shared. For this reason, there is pending legislation AB873 (that has passed some of the preliminary processes before coming up for a vote) that would rectify this drafting error, limit the definition of personal information, and

not confer a private right of action, however, for uses of personal information for the business purposes articulated in the Act, even if the business fails to abide by the rules governing use of personal information for business purposes and/or even if the personal information cannot be considered deidentified because of drafting error.

b. No Private Right of Action for Non-Data Breach Violations.

(1) The use of “Disclosure” in this Statutory Language Does Not Cover Voluntary Disclosure of Personal Information Collected and/or Shared in Violation of the Act

The Act uses the word “disclosure” in two separate and distinct ways. The Act specifically grants “the right of Californians to know whether their personal information is sold *or disclosed* and to whom.” Cal. Civ. Code §1798.150(2)(i)(2). More importantly, the act sets forth a comprehensive statutory regime regulating the “disclosure” of personal information for a business purpose, *See* Cal. Civ. Code §1798.115, granting consumers with certain rights related to this area of “disclosures” for business purposes. The Act also uses the word “disclosure” as a catch-all phrase denoting access to personal information by a nefarious third-party. It is this second use that the legislature was referring to when it described its purpose in passing the CCPA:

The unauthorized disclosure of personal information and the loss of privacy can have devastating effects for individuals, ranging from financial fraud, identity theft, and unnecessary costs to personal time and finances, to destruction of property, harassment, reputational damage, emotional stress, and even potential physical harm.

It is this second purpose that the legislature was referencing in Cal. Civ. Code §1798.81.5, specifically cross-referenced in the section of the CCPA granting a private right of action. And it is this second purpose that the legislature meant in the CCPA itself, including the word “disclosure” as a catch-all at the end of a sentence setting forth the private right of action for “unauthorized access and exfiltration, theft, or disclosure.” Though the act fails to define “disclosure,” the canon of *noscitur a sociis* requires that, in context of the private right

provide a more workable definition of deidentified information as “information that does not identify and is not reasonably linkable, directly or indirectly, to a particular consumer.”

of action, it be read in the context of the surrounding words (all dealing with Data Breach).

(2) Express Rejection of SB 561

The California legislature and the California Attorney General (who has certain enforcement and advisory obligations under the statute) recognized that the private right of action in CCPA was limited to Data Breach. The Attorney General and certain legislators championed a proposal, SB 561, to expand the private right of action to include other CCPA violations, by expanding the private right of action to include the right of “[any consumer whose] “rights under this title are violated...” to file suit. Both the fact that this bill did not pass and, more importantly, that it was proposed in the first place to amend the CCPA indicates that the legislature understands the CCPA’s private right of action to be limited to Data Breaches.

c. Express Rejection of Private Right of Action Under Any Other Law

The Act provides that “nothing in this act shall be interpreted to serve as the basis for a private right of action under any other law.” Cal. Civ. Code §1798.150(c). This language would seemingly suggest that other CCPA violations are of no moment or effect. However, the section also provides that it “shall not be construed to relieve any party from any duties or obligations imposed under other law or the United States or California Constitution.”

It may be the case that even though a violation of other, non-data breach sections of the CCPA are not actionable, a violation thereof may be used in a negligence claim, for instance, to show a duty/standard of care and deviation thereof. *See Johnson v. Honeywell Internat. Inc.*, 179 Cal. App. 4th 549, 558, 101 Cal. Rptr. 3d 726, 732, 2009 (Explaining that a negligence per se claim is not a separate claim, but one in which a plaintiff “borrows” a statute to prove duty and standard of care). In such an action, a plaintiff would need to satisfy the general precepts of standing set forth in this outline.

3. Scope of the Attorney General’s Express Right of Action

The Attorney General’s rights are based on alleged “violations” of the title. Violations would include each obligation a business, service provider, or other person has under CCPA which include the following:

Making disclosures via a privacy policy of the data being collected and how they will use that data (including any potential selling of that data) at the time they collect the data;

Having at least two channels for consumers to make requests relating to their data for free;

Allowing consumers to opt-out of the sale of their information;

Having a “Do Not Sell My Personal Information” button on their website if they sell consumer data;

Honoring consumer requests to prohibit the sale of their personal information;

Having practices in place to verify consumer requests;

Responding to data access requests or deletion requests within the required timeframes;

Having employee training on the handling of consumer data;

Having practices in place that prohibit discrimination of consumers who have exercised their rights under CCPA; and

Notifying third parties of a deletion request by a consumer.

The Attorney General can bring an action against any business, service provider, or other person who: is claimed to have failed to comply with the requirements of CCPA; and who does not cure the alleged noncompliance within 30 days of notification of alleged noncompliance.

In a civil action brought in the name of the people of the State of California by the Attorney General any business, service provider, or other person that violates CCPA 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.

B. When are Statutory Damages Available to Consumers Under the CCPA?

1. Are Actual Damages Required to Recover Statutory Damages?

CCPA §1798.150(a)(1) sets forth the damages and relief available to Consumers.

“...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.”

It is unclear whether (A) represents the only pecuniary relief available to Consumers or if under (C) the court could order additional pecuniary damages, such as punitive damages.

In assessing the amount of statutory damages, courts are bound to consider any one or more relevant circumstances including, but not limited to, the nature and

seriousness of the misconduct, the number of violations, the persistence of misconduct, the length of time over which the misconduct occurred, the willfulness of the misconduct, and the defendant's assets, liabilities, and net worth. Cal. Civ. Code § 1798.150(a)(2).

2. Article III Limitations in Federal Court and Application of *Spokeo* to the CCPA

a. The BIPA Parable

The Biometric Information Privacy Act ("BIPA"), adopted by Illinois in 2008, requires entities to: have a written retention and destruction policy pertaining to biometric data it collects; advise the persons from whom they collect biometric data that such data is being collected; inform them of the purpose of its collection; identify the time frame they will retain the data; obtain from them a written release; and use reasonable care in handling the data. BIPA also prohibits entities from selling or profiting from the biometric data or disclosing it without the person's consent, except for certain specified purposes.

Courts deciding BIPA cases have grappled with whether *Spokeo* requires actual injury in addition to one or more statutory violations to establish Article III standing. This line of jurisprudence clearly parallels the related inquiry concerning the CCPA. Therefore, an analysis of the major decisions interpreting standing requirements under BIPA offers insight into whether or not violation of the CCPA's statutory requirements is sufficient, standing alone, to confer Article III standing under *Spokeo*.

The most recent decisions on this topic indicate that a violation of BIPA's statutory requirements, unaccompanied by allegations of actual harm, establishes a concrete injury sufficient to confer Article III standing:

- (1) *Rosenbach v. Six Flags Entm't Corp.*, No. 123186, 2019 WL 323902 (Ill. Jan. 25, 2019):

Reversing the intermediate appellate court, the Illinois Supreme Court held that a person is not required to sustain actual damage beyond a violation of his or her statutory rights under BIPA.

- (2) *Patel v. Facebook, Inc.*, No. 18-15982, 2019 WL 3727424 (9th Cir. Aug. 8, 2019):

Rejected Facebook's argument that plaintiffs could not establish concrete injury sufficient to confer Article III standing because BIPA's requirements are merely procedural and do not protect substantive rights. Held that plaintiffs' allegations that Facebook violated BIPA's consent and retention requirements went to substantive consumer privacy interests intended by the Illinois Legislature to be protected by the statute, even though plaintiffs' data had not actually been misused or disclosed.

However, not all courts have agreed that actual injury is not necessary to establish Article III standing under BIPA. Prior to *Rosenbach* and the Ninth Circuit's *Facebook* decision, the Second Circuit decided the issue in the opposite direction. Additionally, the Seventh Circuit is poised to address the issue, which could further muddy the waters:

- (3) *Santana v. Take-Two Interactive Software, Inc.*, 717 F. App'x 12 (2d Cir. 2017):

Applying *Spokeo*, the Second Circuit held that mere technical violations of BIPA—*e.g.*, failing to comply with BIPA's notice, consent, and disclosure requirements—that do not result in actual harm are insufficient to confer Article III standing. However, it is worth noting that this decision was made without the benefit of the Illinois Supreme Court's holding in *Rosenbach*.

- (4) *Rivera v. Google, Inc.*, 366 F. Supp. 3d 998 (N.D. Ill. 2018), *appeal pending*, No. 19-1182 (7th Cir.):

Held that Google Photo users had failed to meet the standing bar established by *Spokeo* because they had not shown how Google's creation of face templates had caused them concrete harm.

The *Rivera* decision is currently being reviewed by the Seventh Circuit. Should the Seventh Circuit depart from the interpretations of *Spokeo* as announced in *Facebook* or *Take-Two*, it could result in a three-way circuit split. Such an outcome would likely further entice the Supreme Court to clarify the standing requirements under *Spokeo*.

b. Federal Data Breach Jurisprudence on Risk of Harm Generally

- (1) *Beck v. McDonald*, 848 F.3d 262, 273-74 (4th Cir. 2017):

The Fourth Circuit rejected standing for claims of Veterans Administration violation of the federal Privacy Act and Administrative Procedure Act for a security breach. The Fourth Circuit considered a split among the federal appellate circuit courts of appeal on “whether a plaintiff may establish an Article III injury-in-fact based on an increased risk of future identity theft”:

The Sixth, Seventh, and Ninth Circuits have all recognized, at the pleading stage, that plaintiffs can establish an injury-in-fact based on this threatened injury. *See Galaria v. Nationwide Mut. Ins. Co.*, No. 15-3386, 663 F. App'x 384, 388 (6th Cir. 2016) ([Fair Credit Reporting Act] plaintiff-customers' increased risk of future identity theft theory established injury-in-fact after hackers breached Nationwide Mutual Insurance Company's computer network and stole

their sensitive personal information, because “[t]here is no need for speculation where Plaintiffs allege that their data has already been stolen and is now in the hands of ill-intentioned criminals”); *Remijas v. Neiman Marcus Grp., LLC*, 794 F.3d 688, 692, 694-95 (7th Cir. 2015) (plaintiff-customers’ increased risk of future fraudulent charges and identity theft theory established “certainly impending” injury-in-fact and “substantial risk of harm” after hackers attacked Neiman Marcus with malware to steal credit card numbers, because “[p]resumably, the purpose of the hack is, sooner or later, to make fraudulent charges or assume those consumers’ identities”); *Krottner v. Starbucks Corp.*, 628 F.3d 1139, 1142-43 (9th Cir. 2010) (plaintiff-employees’ increased risk of future identity theft theory a “credible threat of harm” for Article III purposes after theft of a laptop containing the unencrypted names, addresses, and social security numbers of 97,000 Starbucks employees); *Pisciotta v. Old Nat’l Bancorp.*, 499 F.3d 629, 632-34 (7th Cir. 2007) (banking services applicants’ increased risk of harm theory satisfied Article III injury-in-fact requirement after “sophisticated, intentional and malicious” security breach of bank website compromised their information).

By contrast, the First and Third Circuits have rejected such allegations. *See Katz v. Pershing, LLC*, 672 F.3d 64, 80 (1st Cir. 2012) (brokerage account-holder’s increased risk of unauthorized access and identity theft theory insufficient to constitute “actual or impending injury” after defendant failed to properly maintain an electronic platform containing her account information, because plaintiff failed to “identify any incident in which her data has ever been accessed by an unauthorized person”); *Reilly v. Ceridian Corp.*, 664 F.3d 38, 40, 44 (3d Cir. 2011) (plaintiff-employees’ increased risk of identity theft theory too hypothetical and speculative to establish “certainly impending” injury-in-fact after unknown hacker penetrated payroll system firewall, because it was “not known whether the hacker read, copied, or understood” the system’s information and no evidence suggested past or future misuse of employee data or that the “intrusion was intentional or malicious”).

The *Beck* court found that risk of identity theft too speculative from the theft of a laptop with unencrypted health information, distinguishing the intentional hacking cases and laptop cases where there was evidence of misuse. *Beck*, 848 F.3d at 274. *But see Hutton v. Nat’l Bd. of Exam’rs in Optometry, Inc.*, 892 F.3d 613,

622 (4th Cir. 2018) (finding *Beck* distinguishable in data breach case where plaintiffs “allege that they have already suffered actual harm in the form of identity theft and credit card fraud” and noting that the Supreme Court in *Clapper v. Amnesty Int’l USA*, 568 U.S. 398, 414 n.5 (2013) agreed that Article III standing exists “on the basis of costs incurred to mitigate or avoid harm when a substantial risk of harm actually exists”).

(2) *In re U.S. Office of Personnel Mgmt. Data Sec. Breach Litig.*, 928 F.3d 42, 55-56 (D.C. Cir. 2019):

In *OPM*, another Privacy Act case, the District of Columbia Circuit reversed a dismissal for lack of standing, finding substantial risk of future identity theft, where “identity theft ... constitute[s] a concrete and particularized injury.” (quoting *Attias v. Carefirst, Inc.*, 865 F.3d 620, 626-27 (D.C. Cir. 2017), in turn citing *Susan B. Anthony List v. Driehaus*, 134 S. Ct. 2334, 2341 (2014) (establish standing by either “certainly impending” or “substantial risk” test)).

(3) *Robins v. Spokeo, Inc.*, 867 F.3d 1108, 1113 (9th Cir. 2017) (*Spokeo II*):

Upon remand of *Spokeo*, the Ninth Circuit maintained its finding of standing, answering affirmatively:

“In evaluating Robins’s claim of harm, we thus ask: (1) whether the statutory provisions at issue were established to protect his concrete interests (as opposed to purely procedural rights), and if so, (2) whether the specific procedural violations alleged in this case actually harm, or present a material risk of harm to, such interests.”

The Ninth Circuit rejected *Spokeo*’s argument that the “flattering” inaccuracies could only result in speculative, and not concrete, harm, stating “the inaccuracies alleged in this case do not strike us as the sort of ‘mere technical violation[s]’ which are too insignificant to present a sincere risk of harm to the real-world interests that Congress chose to protect with FCRA.” *Id.*

(4) *Patel v. Facebook, Inc.*, No. 18-15982, 2019 WL 3727424 (9th Cir. Aug. 8, 2019):

The Ninth Circuit in *Patel* (at *4) distinguished two federal data breach situations for “concrete injury-in-fact”:

Van Patten v. Vertical Fitness Group, LLC, 847 F.3d 1037, 1041–43 (9th Cir. 2017) found the Telephone Consumer Protection Act (TCPA) was established to protect the plaintiff’s substantive right to privacy and defendant telemarketer’s alleged conduct impacted this privacy right,

therefore on this basis alone a concrete injury-in-fact was alleged sufficient to confer Article III standing.

Bassett v. ABM Parking Servs., Inc., 883 F.3d 776, 777–78, 782-83 (9th Cir. 2018) found failure to allege a concrete injury-in-fact where the plaintiff alleged that a parking garage had violated the FCRA credit card redaction requirement by giving him a receipt displaying his card’s full expiration date “because no one but the plaintiff himself saw the expiration date.” *Cf. Crupar-Weinmann v. Paris Baguette Am., Inc.*, 861 F.3d 76 (2d Cir. 2017) (FACTA one instance of printed credit card expiration date in technical violation of Fair and Accurate Credit Transactions Act [FACTA] did not pose a “material risk of harm” and thus was inadequate to confer standing); *Meyers v. Nicolet Rest. de Perre, LLC*, 843 F.3d 724 (7th Cir. 2017) (same under FACTA).

One synthesis of these cases is that “technical” violations of security procedures will not support standing without some showing of actual injury while breaches such as intentional hacking will. Given that the CCPA appears to require actual data breach, and based on the case law developed to date (particularly in the Ninth Circuit where issues related to CCPA will be decided), it appears that Courts will likely find that actual harm is not required to before a consumer can sue or have standing.

c. California Standing Jurisprudence

The extent to which California’s standing doctrine mirrors its federal jurisprudence is murky at best.

In *People v. Superior Court*, 2018 DJDAR 11217 (Cal. App. Nov. 27, 2018), a group of physicians brought suit against various state officials seeking to enjoin the enforcement of California’s End of Life Option Act, Health and Safety Code, which allowed for physician-assisted suicide. In a split decision, the 4th District Court of Appeal concluded that the plaintiffs could not demonstrate they had standing to challenge the act, which was a jurisdictional defect, because they had failed to plead that they had any “beneficial interest” in the outcome of the dispute. *Id.* at 11220, 11224. Thus, like Article III standing in federal court, the Court found that lack of standing of was a jurisdictional limit on its power.

On the other hand, the California Supreme has recently held that standing is not a jurisdictional prerequisite: “Unlike the federal Constitution, our state Constitution has no case or controversy requirement imposing an independent jurisdictional limitation on our standing doctrine.”

Weatherford v. City of San Rafael, 2 Cal. 5th 1241, 1247-48 (2017). *See also Grosset v. Wenaas*, 42 Cal. 4th 1100, 1117 n.13 (2008). Thus, California courts have recognized that a plaintiff need not have a “personal stake in the outcome of the controversy” to bring suit. *Grosset* at 1117. California courts have also rejected rigid formalism between the various branches of formalism that underlies federal standing doctrine: “[I]t is well understood that the branches share common boundaries and no sharp line between their operations exist.” *People v. Bunn*, 37 P.3d 380, 388 (Cal. 2002).

III. OVERVIEW OF QUESTION 2

How should “each violation” be calculated for purposes of assessing civil penalties under the California Consumer Protection Act of 2018 (“CCPA”), Cal. Civ. Code §1798.100, *et seq.* In particular, Cal. Civ. Code §1798.155(b), provides 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 [of the CCPA], 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 CCPA does not, however, clearly define how “each violation” should be calculated or totaled. For instance, should it be calculated by adding up the total number of consumers affected by the business’ conduct, adding up the number of statutory sections the business violated, or is it limited to one violation of the CCPA generally? A similar issue has arisen in the context of other privacy laws like the Illinois Biometric Information Privacy Act (BIPA) interpretations of which may provide further guidance. This section will also briefly address other critical legal questions implicated by this provision including the meaning of “intentional violation” and whether due process may cap potential civil penalties.

IV. ANSWERING THE QUESTION

A. Statutory Language

Cal. Civ. Code §1798.155(b), provides that, “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.”³

1. Private Right of Action in the CCPA

³ It is not clear whether the Attorney General can pursue claims for administrative fines for violation of Cal. Civ. Code §1798.150 or whether that section is simply a remedy for claims that are limited to a private consumer right of action.

The private right of action discussed *supra* at II.A.1, instructs that “the number of violations” should be considered when determining statutory damages. That suggests, that at least for the individual right of action, multiple violations may constitute only one “incident”

2. Legislative History

The Legislative Counsel’s Digest, with respect to the individual right of action, states: “This bill would clarify that the only private right of action permitted under the act is the private right of action described above for violations of unauthorized access and exfiltration, theft, or disclosure of a consumer’s nonencrypted or nonredacted personal information and would delete the requirement that a consumer bringing a private right of action notify the Attorney General.”

(https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB1121 at paragraph number 3)

B. Possible Methodologies for Calculating Violations

Defendants’ exposure will be determined by the scope of conduct swept into a single “violation.” Narrower definitions of “violation” tend to produce higher civil penalties because more “violations” may occur. Broader definitions tend to produce lower civil penalties because fewer “violations occur.”

These hypothetical scenarios illustrate the damages implications of particular definitions of “violation.”

1. Failure to comply with the Title even across multiple parts of the law is one violation and no more

One approach, similar to the approach adopted in Minnesota and Michigan’s consumer protection laws, is to cap civil penalties by defendant. Minn. Stat. § 8.31(3) (civil penalties capped at \$25,000 per defendant); Mich. Comp. Laws Ann. § 445.905(1) (civil penalties capped at \$25,000 per defendant). This approach would effectively treat all violations of the title as a single violation for purposes of the civil penalty cap.

For example, under this approach, if a major multinational corporation failed to give notice to consumers of categories of data collected under 1798.100(b) AND failed to provide opt-in capability for minors under 1798.120(d), that entire course of conduct would be a single “violation,” with a civil penalty capped at \$2,500 (or \$7,500 for an intentional violation). These amounts would not vary based on the number of consumers affected.

2. Failure to comply with the Title in a particular area (such as failure to develop a program to delete personal information on request) is one violation regardless of number of consumers or records impacted, but there could be multiple violations based on the number of parts of the Title violated.

Another approach would be to treat all conduct that violated a particular subsection

of the title as a “violation.” Given the same fact pattern state above, the major multinational would be liable for two violations: one for all conduct violating 1798.100(b) and another for violating 1798.120(d). Civil penalties would be capped at \$5,000 or \$15,000 if both violations were intentional.

3. Calculate based on the number of consumers impacted by each failure to comply

A third approach treats every affected consumer as a “violation,” regardless of the number of sections implicated. This approach mirrors the approaches adopted by California, Arizona, Maryland, Nebraska, Nevada, New Jersey, and Texas in enforcing their consumer protection laws. *See State ex rel. Corbin v. United Energy Corp. of Am.*, 725 P.2d 752, 759 (1986) (“one violation of the consumer fraud act for each consumer, regardless of the number of misrepresentations made to each consumer.”); *People v. Superior Court*, 9 Cal. 3d 283, 289 (1973) (“the Legislature intended that the number of violations is to be determined by the number of persons to whom the misrepresentations were made.”); *T-UP, Inc. v. Consumer Prot. Div.*, 145 Md. App. 27 (2002); *State ex rel. Stenberg v. Am. Midlands, Inc.*, 244 Neb. 887, 894 (1994); *Landex, Inc. v. State ex rel. List*, 94 Nev. 469, 480 (1978); *Chiesa v. Levine*, No. A-4055-11T3, 2013 WL 3284131, at *2 (2013); *Molano v. State*, 262 S.W.3d 554, 562 (2008).

This approach will result in substantially larger civil penalties. Under the same basic fact pattern above and a population of 500,000 affected minor consumers, civil penalties would be capped at \$1,250,000,000, rising to \$3,750,000,000 for intentional violations.

4. Calculate based on the number of pieces of personal information impacted by each failure to comply

A fourth approach would be to treat each piece of personal information affected by a violation of a statute as a “violation” under the civil penalties cap. Under this approach, each piece of personal information, for each consumer, counts as a “violation” under the civil damages cap. This approach generally tracks the approach adopted by Massachusetts, Mississippi, New Hampshire, Ohio, South Carolina, Washington, and Wisconsin in their consumer fraud laws. *See Com. v. Fall River Motor Sales, Inc.*, 409 Mass. 302, 313-14 (1991); *In re Mississippi Medicaid Pharm. Average Wholesale Price Litig.*, 190 So. 3d 829, 847 (2015); N.H. Rev. Stat. § 358-A:4(III)(b) (“the court shall determine the number of unlawful acts or practices which have occurred without regard to the number of persons affected thereby”); *United States v. Dish Network LLC*, 256 F. Supp. 3d 810, 968 (2017); *State ex rel. Wilson v. Ortho-McNeil-Janssen Pharm., Inc.*, 414 S.C. 33, 86 (2015); *State v. Ralph Williams’ N. W. Chrysler Plymouth, Inc.*, 87 Wash. 2d 298, 325 (1976) (“A single advertisement may include a number of misrepresentations . . . [e]ach of these acts is a separate violation”); *State v. Going Places Travel Corp.*, 362 Wis. 2d 414, 442 (2015) (violations calculated by multiplying the number of misrepresentations by the number of consumers).

In our fact pattern, the two violations per consumer would result in 1,000,000 violations. The aggregate civil penalties cap would be \$2,500,000,000, rising to \$7,500,000,000 for intentional violations.

5. Each day of violation

It is also possible to add another layer. The Attorney General's office might treat each day that a statutory violation continues after a demand to cease as a "violation" for civil penalties purposes. Total civil penalties under this approach would, of course, depend on the underlying definition of "violation." But adding a violation for each day the defendant fails to cure would further increase civil damages.

If, in our fact pattern, the defendant received a demand to cease both practices and did not do so for ten days, its civil penalties exposure would be \$25,000,000,000 before enhancement for intentional violations.

C. Other California Laws that Use Similar Language Related to the Calculation of Civil Penalties

1. Relevant California laws

- a) The California Online Privacy Protection Act (CalOPPA), Cal. Bus. & Prof. Code §§ 22575-22579, which itself lacks an enforcement provision, has been used in tandem with California's Unfair Competition Law on at least one occasion. *See People ex rel. Harris v. Delta Air Lines, Inc.*, 247 Cal. App. 4th 884, 900, 202 Cal. Rptr. 3d 395, 407 (2016).
- b) California's Unfair Competition Law allows for a \$2,500 penalty per violation, much like the CCPA. *See* Cal. Bus. & Prof. Code §17206(a). Given the Attorney General's enforcement powers for both CCPA and CalOPPA, this suit indicates an inclination to define violation in per capita terms.

2. Relevant Caselaw on Calculation Methodologies

Of import in the context of Unfair Competition penalties, California has a longstanding history of calculating the "number" of statutory violations using a "per-victim" methodology. The California Supreme Court has unequivocally held that "[T]he legislature intended that the number of violations is to be determined by the number of persons to whom the misrepresentations were made, and not by the number of separately identifiable misrepresentations involved" *See People v. Sup.Ct. (Jayhill Corp.)* (1973) 9 C3d 283, 289, 107 CR 192, 196. *See also People v. Superior Court (Olson)*, 96 Cal. App. 3d 181, 198, 157 Cal. Rptr. 628, 639 (Ct. App. 1979) (holding that, in the false advertising context, "a reasonable interpretation of the statute in the context of a newspaper advertisement would be that a single publication constitutes a minimum of one violation with as many additional violations as there are persons who read the advertisement or who responded to the advertisement").

D. Other States' Laws that Reflect Similar Language Related to the Calculation

of Civil Penalties

1. Illinois' Biometric Information Privacy Act, ILCS Ch. 740, Act 14

Illinois' Biometric Information Privacy Act, ILCS Ch. 740, Act 14 ("BIPA"), offers an analogy to the CCPA. BIPA authorizes a private right of action and provides, in part:

A prevailing party may recover for each violation:

- (1) against a private entity that negligently violates a provision of this Act, liquidated damages of \$1,000 or actual damages, whichever is greater;
- (2) against a private entity that intentionally or recklessly violates a provision of this Act, liquidated damages of \$5,000 or actual damages, whichever is greater

740 ILCS 14/20.

There does not appear to be definitive legal authority on how the number of violations should be calculated under BIPA. However, the Supreme Court of Illinois has addressed the related question of whether a plaintiff must allege an actual injury or adverse effect in order to receive liquidated damages for violations of BIPA. *See Rosenbach v. Six Flags Entertainment Corporation*, -- N.E. 3d --, 2019 IL 123186, 2019 WL 323902 (Ill. Jan. 25, 2019). While the issue of how to calculate the number of violations was not before the court, the court relied on the statutory language and legislative findings to conclude that BIPA subjects companies "to substantial potential liability, including liquidated damages, injunctions, attorney fees, and litigation expenses 'for each violation' of the law whether or not actual damages, beyond violation of the law's provisions, can be shown. *Id.* at ¶ 36. The court's discussion of BIPA's purposes, along with its characterization of the potential penalties liability as "substantial," could be read to suggest that Illinois courts would take an expansive approach in calculating the number of violations.

One federal district court has considered the calculation of BIPA violations in determining whether the amount in controversy was sufficient to invoke federal jurisdiction. *See Peatry v. Bimbo Bakeries USA, Inc.*, No. 19 C 294, Doc. 31 (N.D. Ill. Aug. 7, 2019). In *Bimbo*, the Plaintiff alleged violations of BIPA relating to Bimbo's practice of requiring employees to give fingerprint scans when clocking in and out of work. Noting a lack of authority on this question, the court concluded that under "an expansive reading of BIPA's damages provision," it was "plausible" that the plaintiff could recover \$5,000 for each time that she scanned her fingerprints as part of Bimbo's process for clocking in and out of work. *Id.* at 4.

2. Other States

Along with Illinois, Washington and Texas have enacted biometric privacy statues

that may provide useful analogies to CCPA.⁴

a. Washington’s “Biometric Identifiers” law, RCWA 19.375, *et seq.*

This law provides for enforcement “solely by the attorney general under the consumer protection act.” RCWA 19.375.030(2). Washington’s consumer protection act authorizes penalties for “each violation.” RCWA 19.86.140. In construing this provision, the Washington Supreme Court has declined to limit penalties to one penalty per consumer. *See State v. Ralph Williams’ N. W. Chrysler Plymouth, Inc.*, 87 Wash. 2d 298, 316–17, 553 P.2d 423, 436 (1976). The court held, in part, “This statute vests the trial court with the power to assess a penalty for each violation. The violations in this case fall within 10 separate classifications, and each classification represents a distinct and separate cause of action. Each cause of action required respondent to prove divergent facts to establish a violation.” *Id.*

b. Texas’ “Capture or Use of Biometric Identifier” law, TX Bus. & Com. § 503.001

This law authorizes the attorney general to bring an action to recover “a civil penalty of not more than \$25,000 for each violation. TX Bus. & Com. § 503.001. While this provision has not been construed in a reported case, Texas’ consumer protection act similarly authorizes penalties “per violation.” TX Bus. & Com § 17.47(c)(1). Under the consumer protection act, it appears that a separate penalty may be assessed for each affected consumer. *See Molano v. State*, 262 S.W.3d 554, 562 (Tx. Ct. App. 2008).

E. The Meaning of “Intentional Violation”

1. Key language: (Section 155)

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. (emphasis added)

2. Legislative History

⁴ As a general matter, state consumer protection acts calculate violations according to the number of transactions, representations, or consumers involved. However, and as discussed further above, two state consumer protection acts – those of Minnesota and Michigan – appear to cap the amount of civil penalties per defendant, irrespective of the number of violations. *See* Minn. Stat. § 8.31(3) (civil penalties capped at \$25,000 per defendant); Mich. Comp. Laws Ann. § 445.905(1) (civil penalties capped at \$25,000 per defendant).

The current language of section 155 was amended by Senate Bill 1121. According to the introductory language to this bill:

“The [then-current CCPA] provides that a business, service provider, or other person who violates its provisions, and fails to cure those violations within 30 days, is liable for a civil penalty under laws relating to unfair competition in an action to be brought by the Attorney General. ... The bill would remove references to laws relating to unfair competition in connection with Attorney General actions described above. The bill would limit the civil penalty to be assessed in an Attorney General action in this context to not more than \$2,500 per violation or \$7,500 per each intentional violation and would specify that an injunction is also available as remedy.”

The concept of enhanced damages for an “intentional” violation exists in the history of the original bill dating back to the original introduction of the CCPA.

3. Comparison with UCL

Because of the interrelatedness of the CCPA and UCL throughout the legislative process, courts may look to the UCL and related cases when interpreting the CCPA. Under the UCL, the “willfulness” of the violation is an element in assessing the amount of damages, but there is otherwise no concept of an intentional violation of the UCL. Section 17206(b). The UCL does address the concept of intentional violation in a similar context, in defining the penalty for the intentional violation of a court order. Section 17207(a).

4. Intentional violation, generally

a. Intent Generally

The Model Penal Code (MPC) presents 4 potential levels of *mens rea*: purposeful, knowing, reckless, and negligent. An actor has “specific intent” if they act knowingly (including purposefully).

(i) Purposeful: an act (or omission) purposefully results in an outcome if the conscious object of the actor to achieve that outcome.

(ii) Knowing: an act (or omission) knowingly results in an outcome if the actor is aware that it is practically certain that the act (or omission) will cause such an outcome.

* Knowledge typically includes constructive knowledge and, in civil contexts, objective knowledge (*i.e.*, “should have known”).

b. California Courts

California courts have addressed the concept of intentionally violating a law in the context of enhanced civil penalties or damages. While the courts are generally consistent as to interpreting intent to mean “knowing”, there is less consistency as to defining the proper object of the *mens rea* (due, primarily, to the fact that the laws and regulations which were the subject

of such cases have vastly different language, legislative objectives, etcetera).

- (i) *PacifiCare Life & Health Ins. Co. v. Jones*, 27 Cal. App. 5th 391 (2018):

In *Jones*, the court upheld certain regulations that separately defined knowing violations (which require knowledge that an action would violate the statute) and willful violations (which relate to whether the action itself was intentional).

- (ii) *Donald v. Cafe Royale, Inc.*, 218 Cal. App. 3d 168 (1990)

In *Donald*, the court opined that an intentional violation of California disability code means an action that intentionally or willfully denies a protected individual their rights. *Accord. Gunther v. Lin*, 144 Cal. App. 4th 223 (2006).

- (iii) *Lopez v. Friant & Associates, LLC*, 15 Cal. App. 5th 773

In *Lopez* the court held that intentional violation of the payroll requirements of California labor law meant intentionally failing to provide the required information.

F. Due Process Caps on Civil Penalties

A number of courts have examined due process rights when confronted with a large, statutory damages award questions including with statutory penalties similar to CCPA, and we look to their previous decisions for guidance.⁵ Appellate courts have predominantly rejected defendants' arguments that statutory damages provisions violate due process when, like here, those statutory damages are offered in lieu of actual damages.

- 1. *Patel v. Facebook, Inc.*, No. 18-15982, 2019 WL 3727424 (9th Cir. Aug. 8, 2019):

In *Patel*, the Ninth Circuit affirmed a district court's order granting class certification to Facebook users who brought claims under the Illinois Biometric Information Privacy Act (BIPA). No. 18-15982, 2019 WL 3727424 (9th Cir. Aug. 8, 2019). The Ninth Circuit rejected Facebook's argument that a large, class-wide statutory damages award under the BIPA would defeat superiority. There, the court reasoned that "whether the potential for enormous liability can justify a denial of

⁵ Although a number of appellate decisions have examined statutory penalties in copyright actions, we have limited our discussion to statutes that are more analogous to the CCPA.

class certification depends on [legislative] intent.” *Id.* at *8 (citations omitted). And neither the statutory language nor the legislative history of the BIPA intended to place a cap on statutory damages, so “denying class certification on that basis would ‘subvert [legislative] intent.’” *Id.* (citations omitted).

2. *Golan v. FreeEats.com*, 930 F.3d 950, 962 (8th Cir. 2019):

Concerning defendants’ due process arguments, most appellate courts have rejected challenges to large statutory awards on that basis, with some exceptions. For example, in *Golan v. FreeEats.com*, for example, the Eighth Circuit reviewed *de novo*⁶ the district court’s determination that Telephone Consumer Protection Act (TCPA)-mandated statutory damages of \$1.6 billion would violate the Due Process Clause. 930 F.3d 950, 962 (8th Cir. 2019). In that case, the court determined that the aggregate—not individual—statutory damages award did, in fact, violate the Due Process Clause because “[to] state the obvious, \$1.6 billion is a shockingly large amount.” *Id.* The court also took into consideration the conduct of the defendant, which “plausibly believed it was not violating the TCPA” because it had prior consent to call the recipients about religious liberty, and a predominant theme of the call which violated the TCPA was about religious liberty. *Id.* at 963.

3. *Perez-Farias v. Global Horizons, Inc.*, 499 Fed. Appx. 735, 737 (9th Cir. 2012):

In *Perez-Farias v. Global Horizons, Inc.*, the Ninth Circuit held that a district court erred when it awarded workers less than the full amount of statutory damages provided for by the Washington Farm Labor Contract Act (“FCLA”). 499 Fed. Appx. 735, 737 (9th Cir. 2012). In that case, the “full amount of statutory damages does not violate federal due process law because it is not ‘so severe and oppressive as to be wholly disproportioned [sic] to the offense and obviously unreasonable.’” *Id.* (citing *St. Louis, I.M. & S. Ry. Co. v. Williams*, 251 U.S. 63, 66 (1919)).

4. *Harris v. Mexican Specialty Foods, Inc.*, 564 F.3d 1301, 1312 (11th Cir. 2009):

In *Harris v. Mexican Specialty Foods, Inc.*, the Eleventh Circuit reviewed a district court’s determination that the Fair Credit Reporting Act’s (FCRA) statutory damages provision “unconstitutionally excessive on its face because the statutory-damages provision is ‘expressly not compensatory in nature.’” 564 F.3d 1301, 1312. According to the district court, “because only litigants that have not suffered any actual harm will avail themselves of statutory damages under § 616(a)(1)(A) [of FACTA], these damages will always be unconstitutionally excessive when compared to the actual harm caused by the violator’s actions.” *Id.* at 1312-13. The

⁶ The circuit court applied the standard of review used in punitive damages awards, which are reviewed *de novo*, rather than copyright awards, which are reviewed for clear error, because the case did “not involve actual damages.” *Id.* at 962, n.12.

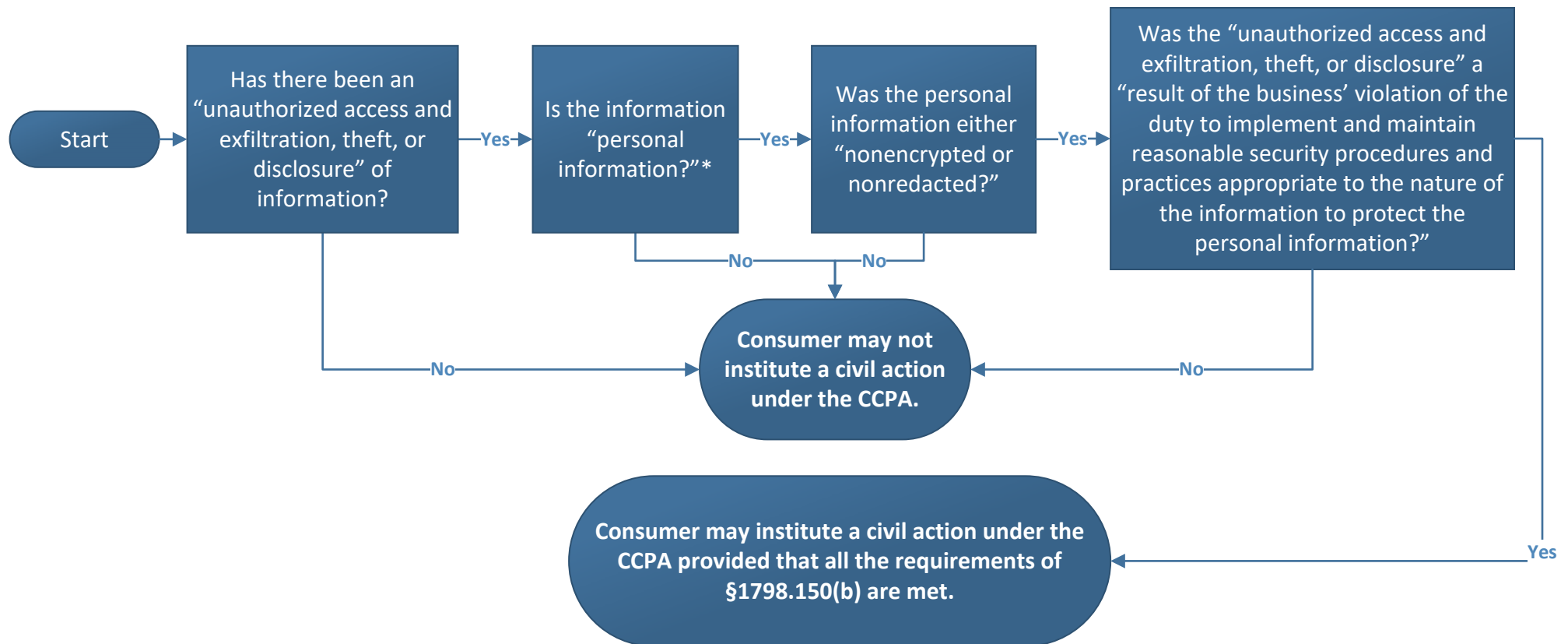
Eleventh Circuit disagreed that the statutory damages were punitive in nature, because the FCRA “provides that plaintiffs may elect to receive actual damages or statutory damages, but not both.” *Id.* Accordingly, the statutory damages provision was not tantamount to a punitive damages award because the statutory damages would only be recoverable in lieu of an individual’s actual damages. As it pertained to the aggregate damages amount, the Eleventh Circuit was clear that the statutory damages provision may even be less than the actual harm that individuals could suffer in the future:

Moreover, even if the statutory damages provision could be construed as punitive, the district court still erred in ruling that § 616(a)(1)(A) always yields unconstitutionally excessive verdicts. As discussed above, *see supra* § III.B, the FCRA does not forbid individuals who suffered actual harm from seeking statutory damages. Even if none of the plaintiffs in the instant case were actually harmed, it is conceivable that in the future a party with actual harm that is difficult to compute will bring a case seeking statutory damages. In such a case, the actual harm might be very close to the statutory damages. This mere possibility of a constitutional application is enough to defeat a facial challenge to the statute.

Id. Accordingly, the district court’s order was vacated and remanded. Similarly here, the CCPA provides both statutory damages *or* actual damages, whichever is greater.

May a Consumer Institute a Civil Action Under the CCPA?

CCPA §1798.150(a)



*"Personal information" means information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household.... "Personal information" does not include publicly available information. For these purposes, 'publicly available' means information that is lawfully made available from federal, state, or local government records...."

**DRAFT FOR DISCUSSION
NOT LEGAL ADVICE**