The Sedona Conference Journal

Volume 22 2021

The Sedona Conference Commentary on Quantifying Violations under U.S. Privacy Laws

The Sedona Conference

Recommended Citation:

The Sedona Conference, *Commentary on Quantifying Violations under U.S. Privacy Laws*, 22 SEDONA CONF. J. 489 (2021).

For this and additional publications see: https://thesedonaconference.org/publications

THE SEDONA CONFERENCE COMMENTARY ON QUANTIFYING VIOLATIONS UNDER U.S. PRIVACY LAWS

A Project of The Sedona Conference Working Group on Data Security and Privacy Liability (WG11)

Author:

The Sedona Conference

Editor-in-Chief:

James J. Pizzirusso

Contributing Editors:

Mark Bailey
Stephen Y. Chow
Ross M. Gotler
Amy E. Keller
Timothy R. Murphy
Kaleigh N. Powell
Jonathan M. Wilan

Steering Committee Liaison:

Al Saikali

Staff Editors:

David Lumia
Michael Pomarico

The opinions expressed in this publication, unless otherwise attributed, represent consensus views of the members of The Sedona Conference Working Group 11. They do not necessarily represent the views of any of the individual participants or their employers, clients, or any other organizations to which any of the participants belong, nor do they necessarily represent official positions of The Sedona Conference.

We thank all of our Working Group Series Annual Sponsors, whose support is essential to our ability to develop Working Group Series publications. For a listing of our sponsors, just click on the "Sponsors" navigation bar on the homepage of our website.

This publication may be cited as follows:

> The Sedona Conference, *Commentary on Quantifying Violations under U.S. Privacy Laws*, 22 Sedona Conf. J. 489 (2021).

PREFACE

Welcome to the July 2021 final version of The Sedona Conference *Commentary on Quantifying Violations under U.S. Privacy Laws* ("*Commentary*"), a project of The Sedona Conference Working Group 11 on Data Security and Privacy Liability (WG11). This is one of a series of Working Group commentaries published by The Sedona Conference, a 501(c)(3) research and educational institute dedicated to the advanced study of law and policy in the areas of antitrust law, complex litigation, intellectual property rights, and data security and privacy law. The mission of The Sedona Conference is to move the law forward in a reasoned and just way.

The mission of WG11 is to identify and comment on trends in data security and privacy law, in an effort to help organizations prepare for and respond to data breaches, and to assist attorneys and judicial officers in resolving questions of legal liability and damages.

The Sedona Conference acknowledges Editor-in-Chief James Pizzirusso for his leadership and commitment to the project. We also thank Contributing Editors Mark Bailey, Stephen Chow, Ross Gotler, Amy Keller, Tim Murphy, Kaleigh Powell, and Jonathan Wilan for their efforts, and Al Saikali for his contributions as Steering Committee liaison to the project. We thank Andrew Lucking for his contributions.

In addition to the drafters, this nonpartisan, consensus-based publication represents the collective effort of other members of WG11 who reviewed, commented on, and proposed edits to early drafts of the *Commentary* that were circulated for feedback from the Working Group membership. Other members provided feedback at WG11 annual and midyear meetings where drafts of the *Commentary* were the subject of the dialogue. The publication was also subject to a period of public comment.

On behalf of The Sedona Conference, I thank both the membership and the public for all of their contributions to the *Commentary*.

We encourage your active engagement in the dialogue. Membership in The Sedona Conference Working Group Series is open to all. The Series includes WG11 and several other Working Groups in the areas of electronic document management and discovery, cross-border discovery and data protection laws, international data transfers, patent litigation, patent remedies and damages, and trade secrets. The Sedona Conference hopes and anticipates that the output of its Working Groups will evolve into authoritative statements of law, both as it is and as it should be. Information on membership and a description of current Working Group activities is available at https://thesedonaconference.org/wgs.

Craig Weinlein
Executive Director
The Sedona Conference
July 2021

TABLE OF CONTENTS

I. INTRODUCTION

Some privacy laws in the United States allow for enforcement authorities and plaintiffs in private actions to seek damages or statutory penalties based on certain violations. Many of these laws, however, do not clearly define how a "violation" should be calculated. This can lead to confusion at best—and due process concerns at worst—when authorities and courts seek to quantify damages or penalties. After an incident that leads to a violation of a U.S. data privacy law that may impact a significant number of victims, should calculations be assessed based on one violation of the law, or is there some other way to measure incidents or violations? For example, should the calculation be based on adding up the total number of consumers affected by the business's conduct, the number of statutory sections the business violated, the number of days the violations in a particular incident occurred, or some combination thereof?

As data privacy receives more attention in the United States and elsewhere—and as new laws in the U.S. take shape and are enacted—The Sedona Conference Working Group 11 (WG11) recognizes that a consistent approach to quantifying violations under U.S. privacy laws could be helpful to impacted parties, courts, authorities, and practitioners, not to mention the general public. With the various jurisdictions and enforcement authorities involved in current and future enforcement of such data privacy laws, however, such consistency can be challenging to reach. WG11 hopes, however, that this *Commentary* will be of use to stakeholders in reaching a fair interpretation of the meaning of a "per violation" measure of damages.

The first section of this *Commentary* reviews at a high level the landscape of existing privacy laws in the United States, addresses certain ambiguities regarding the calculation of penalties and damages that may arise under such laws, and examines

the way in which other somewhat analogous statutes have been enforced across the country. The second section examines possible ways in which violations of privacy laws could be quantified given statutory construction and existing case law. Finally, the last section endeavors to provide a useful test courts can use to evaluate the meaning of a "per violation" measure of damages in the context of data privacy violations in a way that benefits consumers and provides deterrent value to regulators but is fair and provides due process to potential violators.

II. BACKGROUND ON DATA PRIVACY LAWS

The United States has no overarching and preemptive national "privacy law" or "data security law" in place. As a result, different states have passed different laws—some of which provide for significant statutory penalties or damages when the laws at issue are violated. Given this patchwork approach to privacy and security, there is no singular interpretation as to what constitutes a "violation" of any given law. Consumers and regulators often approach these issues on an ad hoc basis through lawsuits in the court system, leaving organizations with little guidance.

A. Ambiguity in Data Privacy Laws

Various U.S. privacy laws permit damages for each "violation" of the law. These statutes, and judicial interpretations thereof, present discrepancies and ambiguities in how to classify and quantify a "violation" upon a failure to comply with a statute, in whole or in part.

1. Classifying Violations

As explained in further detail below, some statutes are explicit in how they are "violated"—for example, by failing to comply with a particular provision of the act.[1] But where statutes are not explicit, how to classify a "violation" becomes a matter of statutory interpretation. Does "violation" mean failure to comply with the title itself, as opposed to some particular provision? Does it mean the number of consumers impacted, or the number of pieces of personal information that are

1. *See, e.g.*, Migrant and Seasonal Agricultural Workers Protection Act, 29 U.S.C. §§ 1801–72 (1983); District of Columbia Consumer Protection Procedures Act, D.C. CODE §§ 28-3901–13 (1975).

implicated? Is there a "violation" for every day that a defendant fails to comply with the statute? The answers may have significant damages implications for potential plaintiffs and due process implications for potential defendants.

2. Quantifying Violations

Further complicating the analysis is how to quantify a violation even where it can be classified. For example, the California Consumer Protection Law (CCPA), which went into effect on January 1, 2020, provides that (1) "[a] person that violates this title shall be . . . 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*" in a civil action brough by the California attorney general.[2] Under the private right of action provided by the Illinois Biometric Information Protection Act (BIPA), "[a] prevailing party may recover for *each violation* [among other remedies] (1) against a private entity that negligently violates a provision of this Act, liquidated damages of $1,000 [or] (2) against a private entity that intentionally or recklessly violates a provision of this Act, liquidated damages of $5,000 . . . ."[3]

These statutes present ambiguities in how one measures a "violation," especially where there are different types of "violations" covered by the prescribed (statutory) damages—in

2. CAL. CIVIL CODE § 1798.155(b) (West 2020) (emphasis added). A separate section of the CCPA provides for statutory damages "in an amount not less than one hundred dollars ($100) and not greater than seven hundred and fifty ($750) *per consumer per incident*" for certain security breaches (emphasis added). CAL. CIVIL CODE § 1798.150(1)(a) (West 2020). The CCPA provides more guidance for what constitutes a violation under the private right of action, which will be addressed in later parts of this paper.

3. 740 ILL. COMP. STAT. ANN. 14/20 (West 2020).

contrast to the more particularized "incident" of a breach of security for which the CCPA allows a limited private right of action.[4] There is a question under the CCPA or the BIPA whether

---

4. CAL. CIVIL CODE § 1798.150(1)(a) (West 2020) (emphasis added). The next subsection calls these "statutory damages" subject to mandatory consideration of factors:

> "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." *Id.* § 1798.150(1)(b) (emphasis added).

The reference to "number of violations" to be considered in the prescribed remedy for an "incident" suggests reference to prior "violations." Compare the Uniform Law Commission's provision in one privacy law directed to unauthorized internet distribution of "intimate images":

> "[*S*]*tatutory damages not to exceed* $[10,000] against each defendant found liable under this [act] for all disclosures and threatened disclosures by the defendant of which the plaintiff knew or reasonably should have known when filing the action or which became known during the pendency of the action. In determining the amount of statutory damages under subsection (a)(1)(B), *consideration must be given to* the age of the parties at the time of the disclosure or threatened disclosure, *the number of disclosures or threatened disclosures made by the defendant*, the breadth of distribution of the image by the defendant, and other exacerbating or mitigating factors[.]" UNIF. CIVIL REMEDIES FOR UNAUTHORIZED DISCLOSURE OF INTIMATE IMAGES ACT § 6(a)(1)(B) (UNIF. LAW COMM'N 2018) (emphasis added) (subsection 6(a)(3) allows for punitive damages under other law of the state). The comments explain the structure:
>
> "The statutory damages provision is unusual in that it

the measuring "violation" is an aggregate or general violation of a particular statutory provision, or a particular action (unauthorized collection of information, single or series of failure to comply with consumer requests, etc.).

Adding to the ambiguity is the blurring in the statutes of the traditional distinction between statutory and liquidated damages as compensatory versus punitive or exemplary damages.[5]

> suggests a range of damages rather than a fixed amount, and is limited to *one statutory recovery for all disclosures by the defendant occurring within a certain time period*. This is due to the unique nature of the problem addressed by this act. *Technology makes it possible for the number of unauthorized disclosures of intimate images to range in the thousands, even millions*. This potential for vast proliferation makes it advisable to establish upper and lower boundaries. . . ." *Id.* § 6 cmt. (emphasis added).

In another privacy act, the Commission did not provide for statutory damages in private suits but allowed (optionally, according to the legislature) the attorney general to seek "a civil penalty of up to $[1000] for *each violation, but not exceeding* $[100,000] *for all violations caused by the same event*." UNIF. EMPLOYEE & STUDENT ONLINE PRIVACY PROTECTION ACT § 5(a)(2) (UNIF. LAW COMM'N 2016) (emphasis added).

5. In international recognition of foreign money judgments, recognition of noncompensatory awards may be limited to the availability of such awards in the State of enforcement. *See, e.g.*, INTELLECTUAL PROPERTY: PRINCIPLES GOVERNING JURISDICTION, CHOICE OF LAW, AND JUDGMENTS IN TRANSNATIONAL DISPUTES § 411 (AM. LAW INST. 2007). "In the United States . . . statutory damages are awarded in lieu of actual damages and profits in copyright cases [and] the enforcement court should enforce the full amount of the damages." *Id.* cmt. b. Relative to "liquidated damage," traditionally contracted, "unless the rendering court specifically characterizes all or part of the liquidated damages as exceeding the amount necessary to compensate, these awards should be regarded as compensatory and fully enforceable." *Id.* cmt. d. It is possible that certain violations of privacy rights in personal information may be compensated under a theory restitution for "use value" as recognized in "reasonable royalties" as statutory damages in

Thus the factors to be considered for some statutory damages awards (for example, as explained in note 4, *supra*) include consideration of defendant conduct relative to third parties, rather than strictly damage to the plaintiff, including unjust enrichment.

Issues also arise in aggregate (class action) litigation:

> Statutes sometimes entitle persons to sue for liquidated or minimum damages—also known as statutory damages—for technical violations of law that result in either no actual loss or an actual loss too small to warrant conventional litigation. . . .
>
> [B]ecause conduct regulated by statutes with minimum-damages provisions often affects large populations, technical violations can foster lawsuits with enormous potential damage awards if aggregation is permitted. . . .
>
> Difficulties arise when statutes providing for minimum damages make no reference to aggregate procedures. In cases brought under such silent statutes, judges have tried to mediate between the risk of under-deterrence, which a denial of aggregation might cause, and the risk of over-compensation and over-deterrence, which a decision allowing aggregation would encourage. . . .[6]

---

patent infringement. *See* RESTATEMENT (THIRD) OF RESTITUTION AND UNJUST ENRICHMENT § 42 (AM. LAW INST. 2011). Reasonable royalties awards are also statutorily available for trade secrets misappropriation. UNIF. TRADE SECRETS ACT § 3(a) (UNIF. LAW COMM'N 1985); 18 U.S.C. § 1836(b)(3)(B)(ii). Trade secrets misappropriation may be characterized as invasion of commercial information privacy.

6. PRINCIPLES OF THE LAW OF AGGREGATE LITIGATION § 1.03 cmt. e (AM.

The ambiguity on the measurement of "violation" affects appropriate aggregation.

B. Clear Context in Privacy Laws

Although rare, there are U.S. and state laws concerning privacy-type issues that provide clear guidance in quantifying the defendants' exposure following a violation of the law. Nevertheless, in some cases, courts have reduced the statutorily mandated "per violation" damages on other grounds such as due process. The following are examples of statues that explicitly define how "each violation" is calculated or totaled.

1. Telephone Consumer Protection Act of 1991

Enacted in 1991, the Telephone Consumer Protection Act of 1991 (TCPA) was a response by Congress to the reactions of American consumers over intrusive and unwanted phone calls to their homes.[7] The TCPA contains a number of restrictions on the use of automated telephone equipment, including prohibiting the "initiat[ion of] any telephone call to any residential telephone line using an artificial or prerecorded voice to deliver a message without the prior express consent of the called party."[8] This subsection of the TCPA includes an express private right of action and statutory damages, permitting "an action to recover for actual monetary loss from such a violation, or to receive $500 in damages for each such violation, whichever is greater."[9] If the court finds that the defendant willfully or

---

LAW INST. 2010).

7. 47 U.S.C. § 227 (1991).

8. *Id*. § 227(b)(1)(B).

9. *Id*. § 227(b)(3)(B). *See also* Section 227(c)(5) of the TCPA, which provides a private right of action on behalf of "[a] person who has received more than one telephone call within any 12-month period by or on behalf of the

knowingly violated, the court may, in its discretion, increase the amount of the award to $1,500 per violation.[10]

The TCPA's plain text makes the defendant strictly liable for any violative calls and can lead to windfall verdicts in a class action. In *Wakefield v. ViSalus Inc.*,[11] for example, an Oregon federal jury returned a verdict finding ViSalus violated Section 227 of the TCPA by placing 1,850,440 calls using an artificial or prerecorded voice without prior express consent of the class members.[12] Since the TCPA provides for statutory damages of $500 per call, the verdict resulted in a total monetary award of more than $925 million.[13]

Though the statutory damages per violation under Section 227 of the TCPA are clear, district courts have reduced the statutory mandated award on other grounds.[14] One of those

---

same entity in violation of the regulations prescribed under this subsection . . . an action to recover for actual monetary loss from such a violation, or to receive *up to $500* in damages for each such violation . . ." *Id*. § 227(c)(5)(B) (emphasis added).

10. *Id*. § 227(b)(3)(C).

11. No. 15-cv-1857, 2019 WL 2578082, at *1 (D. Or. June 24, 2019) (denying plaintiffs' claim for additional trebled damages).

12. *Id*.

13. *Id*.

14. *See* Texas v. American Blastfax, Inc., 164 F. Supp. 2d 892, 900–01 (W.D. Tex. 2001) (finding it would be inequitable and unreasonable to award $500 for each violation); Maryland v. Universal Elections, Inc., 862 F. Supp. 2d 457, 465 (D. Md. 2012) (holding the penalty was disproportionate to the size of the company and the defendants' presumptive ability to pay); United States v. Dish Network LLC, 256 F. Supp. 3d 810, 906 (C.D. Ill. 2017) (awarding civil penalties and statutory damages of $280,000,000—approximately 20 percent of the defendant's after-tax profits for 2016—finding this amount was "appropriate and constitutionally proportionate, reasonable, and consistent with due process").

grounds—due process—is discussed in further detail below.

2. State Data Security Breach Notification Laws

As of March 28, 2018, all 50 states had enacted breach notification laws requiring notification to individuals where there is an unauthorized access or acquisition of the individual's personally identifiable information.[15] While most breach notification statutes do not make clear what "per violation" means, some articulate the overall liability in the enforcement section of the notification statute.

Unlike the CCPA, for example, Florida's breach notification statue crystalizes that civil penalties apply per breach and not per individual affected by the breach.[16] Specifically, an entity that violates the provisions regarding notification of affected individuals or notification to the Florida Department of Legal Affairs is liable for a civil penalty of $1,000 per day up to 30 days following any violation and $50,000 per 30-day period thereafter, up to a maximum total of $500,000.[17] Virginia's Personal Information Breach Notification Statue also caps the civil penalty that the Virginia Attorney General can recover at $150,000 per breach of the security of the system or a series of breaches of a similar nature that are discovered in a single investigation.[18]

Other statutes make apparent that the civil penalty is calculated on a per-resident basis. The District of Columbia's notification statute allows for the Attorney General to recover a modest civil penalty not to exceed $100 for each resident who was

15. *See* Daniel J. Marcus, *The Data Breach Dilemma: Proactive Solutions for Protecting Consumers' Personal Information*, 68 DUKE L.J. 555, 577 (2018).

16. FLA. STAT. ANN. § 501.171(9)(b)(2) (West 2020).

17. FLA. STAT. ANN. § 501.171(9)(b)(1)-(2) (West 2020).

18. VA. CODE ANN. § 18.2-186.6(I) (West 2020).

not provided notice.[19] In South Carolina, a person who is found to have knowingly and willfully violated the state's notification statute is subject to an administrative fine of $1,000 per South Carolina resident affected by a breach.[20]

19. D.C. CODE § 28-3853(b) (West 2020).

20. S.C. CODE ANN. § 39-1-90(H) (2013).

III. POSSIBLE METHODOLOGIES FOR CALCULATING VIOLATIONS

There are several ways to calculate "violations" of the law—below are some of the most common methodologies for calculating violations.

A. Option One: Calculation of Violations Based Singularly on Defendant's Failure to Comply, Regardless of Number of Impacted Consumers or Parts of the Law Violated

Under this approach—which has an attractive simplicity—"violation" requires only one finding: that the defendant failed to comply with the title, regardless of the number of impacted consumers, the length of the breach, the amount of data exposed, or the number of failures.

But this approach almost certainly undermines the purpose of the inclusion of a statutory damages provision at all. Most courts recognize that statutory damages can serve "both a compensatory and punitive purpose," depending on the statutory structure.[21] They can also incentivize private suits to vindicate

21. *See* Los Angeles News Serv. v. Reuters Television Int'l, Ltd., 149 F.3d 987, 996 (9th Cir. 1998); *see also* Bateman v. Am. Multi-Cinema, Inc., 623 F.3d 708, 718 (9th Cir. 2010) ("We further note that Congress provided for punitive damages in addition to any actual or statutory damages, . . . which further suggests that the statutory damages provision has a compensatory, not punitive, purpose."); Schnall v. Amboy Nat'l Bank, 279 F.3d 205, 216 (3d Cir. 2002) ("But the structure of § 4310, which permitted a plaintiff to recover both actual damages and statutory damages, suggests that this provision served the dual purpose of both compensating plaintiffs who have been misled and deterring banks [committing allegedly harmful conduct]."); Dryden v. Lou Budke's Arrow Fin. Co., 661 F.2d 1186, 1191 (8th Cir. 1981) ("[A]lthough we may disagree with Congress's wisdom in providing for statutory damages in an instance such as this, we are bound to recognize the remedial purpose of the act."); Williams v. Pub. Fin. Corp., 598 F.2d 349, 356

the public interest.[22]

If "violation" means only the failure to comply with the title, statutory damages are exceedingly (and likely inappropriately) limited. Whether statutory damages provisions are designed to deter or to compensate victims (or both),[23] such a limited interpretation undermines the statute's likely purpose: to force a defendant to pay an amount that would deter wrongful conduct in the future or to compensate victims who might otherwise have trouble quantifying their damages.[24]

The statutory language across provisions, moreover, may suggest that "violation" means something other than violation of the title only. The portion of the CCPA authorizing private causes of action, for example, contemplates plural "*violations* of

(5th Cir. 1979) ("The remedial scheme in the [Truth in Lending Act] is designed to deter generally illegalities which are only rarely uncovered and punished, and not just to compensate borrowers for their actual injuries in any particular case.").

22. *See* Perrone v. Gen. Motors Acceptance Corp., 232 F.3d 433, 436 (5th Cir. 2000) ("The caselaw confirms that statutory damages may be imposed as a means to encourage private attorneys general to police disclosure compliance even where no actual damages exist."); *Schnall*, 279 F.3d at 217 (". . . Congress may have deemed it more cost-effective to cede [Truth in Savings Act] enforcement to individuals in the private sector who stand to profit from efficiently detecting and prosecuting [Truth in Savings Act] violations.").

23. For the California Consumer Privacy Act, CAL. CIV. CODE § 1798.155(b) (West 2020), the description of the statutory damages provision as a "penalty" in this context on the one hand suggests that the aim is deterrence. The collected penalty, however, is "deposited into the Consumer Privacy Fund . . . with the intent to fully offset any costs incurred by the state courts and the Attorney General in connection with this title," § 1798.155(c), which suggests a remedial aim at least for the public at large.

24. *See* Capital Records, Inc. v. Thomas-Rasset, 692 F.3d 899, 908 (8th Cir. 2012) ("[S]tatutory damages are designed precisely for instances where actual harm is difficult or impossible to calculate.").

this title" by a singular defendant.[25] Indeed, in "assessing the amount of statutory damages," the court is to consider, among other factors, "the number of violations" a defendant made.[26] If "violation" means only a failure to comply with the title as a whole, it is difficult to see how a defendant could have engendered multiple violations.

Ironically, such a limited interpretation may also work against defendants trying to invoke federal court jurisdiction.[27] As discussed further below, courts—and many defendants—often assume that "violation" implies a per-person basis even in the data breach context. In *Attias v. CareFirst, Inc.*,[28] for example, when evaluating whether the plaintiffs had met the amount-in-controversy requirement under the Class Action Fairness Act in a data breach case, the court explained:

> [P]laintiffs have brought claims under the District of Columbia Consumer Protection Procedures Act, D.C. Code Ann. § 28-3901 *et seq.*, which provides statutory damages of $1,500 *per violation*, and the Virginia Consumer Protection Act ("VCPA"), Va. Code Ann. § 59.1-196 *et seq.*, which entitles successful plaintiffs up to $ 500 to $ 1,000 *per violation*. . . . Although plaintiffs do not provide a breakdown of the numbers in each

25. *See* CAL. CIV. CODE § 1798.150(b) (West 2020).

26. *Id.* § 1798.150(a)(2).

27. *See, e.g.*, Peatry v. Bimbo Bakeries USA, Inc., 393 F. Supp. 3d 766, 769 (N.D. Ill. 2019) (explaining in class action under the Illinois Biometric Information Privacy Act, "[f]or jurisdictional purposes, the parties' positions are reversed, with [plaintiff] seeking to limit the potential damages and [defendant] arguing that the complaint provides the possibility of almost unlimited damages against it.").

28. 365 F. Supp. 3d 1, 8 (D.D.C. Jan. 30, 2019) (appeal pending).

> subclass, it's hard to imagine a distribution that would not satisfy the amount-in-controversy requirement based solely on these statutory claims.[29]

B. *Option Two: Calculation of Violations Based on the Number of Parts of the Statute Violated*

"Violation" could also mean each failure to comply with a particular provision within the statute. Arguably, though, if that was the intent of the legislature in enacting a particular statute, it could have said so. Multiple statutes contemplating statutory damages provisions on a "per violation" basis describe when "per violation" means "per provision violated." As noted above, under the Migrant and Seasonal Agricultural Workers Protection Act,[30] for example, statutory damages are available on a per plaintiff "per violation" basis, and the statute expressly contemplates that violations of the same provision constitute one violation—thereby implying that violating different provisions of the same title amounts to different violations.[31]

Likewise, the District of Columbia Consumer Protection Procedures Act provides that in an action by the Department of

---

29. *See also* Edoff v. T-Mobile Ne. LLC, 2019 WL 1459046, No. ELH-18-3777, at *2 (D. Md. Apr. 2, 2019) (explaining in a data breach case that in case involving "approximately 15,280 Maryland residents," amount in controversy requirement met for Class Action Fairness Act where plaintiffs sought "statutory damages of $1,000 'per first-time violation.'").

30. U.S.C. § 1854(c)(1) (1983).

31. *See id*. ("[M]ultiple infractions of a single provision of this chapter or of regulations under this chapter shall constitute only one violation for purposes of determining the amount of statutory damages due a plaintiff."); Elizondo v. Podgorniak, 100 F. Supp. 2d 459, 462 (E.D. Mich. 2000) ("It is also clear that violations of separate provisions of [the Migrant and Seasonal Agricultural Workers Protection Act] are evaluated separately.").

Consumer and Regulatory Affairs, "[a]ny person found to have executed a trade practice in violation of a law of the District within the jurisdiction of the Department may be liable for a civil penalty not exceeding $1,000 for *each failure to adhere to a provision* of an order described in subsection (f), (g), or (j) of this section, or a consent decree described in subsection (h) of this section."[32] Thus if "per violation" meant "per provision violated," the legislature could have said so.

But some statutes may imply, by their language, that "violation" is in fact based on a "per provision" understanding. As noted above, the CCPA, for example, uses the term "violation" not just in the provision authorizing attorney general action, but also in the section authorizing a private right of action.[33] The statute's use of "violation" in Section 1798.150 refers specifically to violations of provisions: before bringing an action for statutory damages, a consumer must provide 30 days' written notice "identifying the specific provisions of this title the consumer alleges have been or are being violated." Since courts are supposed to give words used across a statute the same meaning,[34] one could argue that "violation" for the purpose of the civil penalty provision similarly means each provision violated.

C. *Option Three: Calculation of Violations Based on the Number of Consumers Impacted*

Courts may also look to the number of consumers impacted by a defendant's failure to comply with the statute as a separate "violation." This approach is consistent with the provision for

32. D.C. CODE § 28-3905(i)(3)(A) (1975) (emphasis added).

33. *See* CAL. CIV. CODE § 1798.150 (West 2020).

34. *See* Miranda v. Nat'l Emergency Servs., Inc., 35 Cal. App. 4th 894, 905 (Cal. Ct. App. 1995).

damages in some other consumer protection statutes, including the TCPA.[35] Even the CCPA's private right of action provision provides for a fine of not less than $100 "per consumer per incident."[36] It may also provide some certainty when assessing damages for settlement purposes.[37]

A recent Pennsylvania case is instructive for proponents of this approach: *Taha v. Bucks County Pennsylvania*.[38] In 2011, Bucks County launched an internet-accessible database of individuals who had been incarcerated in the county from 1938 onward—for a total of 66,799 people.[39] The plaintiff had been arrested and processed by the county but had been released the following day and had his arrest record expunged. He alleged that the database was a violation of Pennsylvania's Criminal History Record Information Act (PCHRIA),[40] which authorizes plaintiffs to bring suit for its violation.[41]

Notably, the PCHRIA's private right of action section

35. 47 U.S.C. § 227(b)(3)(B) (1991) (providing for the greater of actual damages or "$500 in damages for each such violation").

36. CAL. CIV. CODE § 1798.150(a)(1) (West 2020).

37. *Cf.* Marcello Antonucci et al., *Post-Spokeo, Data Breach Defendants Can't Get Spooked*, FIRST QUARTER 2017 PLUS JOURNAL, *available at* https://www.wiley.law/media/publication/271_Post-Spokeo-Data-Breach-Defendants-Cant-Get-Spooked-They-Should-Stand-Up-to-the-Class-Action-Plaintiff-Boogeyman.pdf). Notably, some states specifically preclude this type of calculation. *See, e.g.*, N.H. REV. STAT. § 358-A:4(III)(b) (1997) (providing for "civil penalties up to $10,000 for each violation of this chapter" but providing that "the court shall determine the number of unlawful acts or practices which have occurred without regard to the number of persons affected thereby").

38. 367 F. Supp. 3d 320 (E.D. Pa. 2019).

39. *Id*.

40. 18 PA. CON. STATS. ANN. § 9101 *et seq*. (West 1979).

41. *Taha*, 367 F. Supp. 3d at 323.

provides that:

> A person found by the court to have been aggrieved by a violation of this chapter or the rules or regulations promulgated under this chapter, shall be entitled to actual and real damages of not less than $100 for each violation and to reasonable costs of litigation and attorney's fees. *Exemplary and punitive damages of not less than $1,000 nor more than $10,000 shall be imposed for any violation of this chapter, or the rules or regulations adopted under this chapter, found to be willful*.[42]

After the district court certified a class action of individuals whose information was released in the database, the county appealed to the Third Circuit.[43] The county argued, in part, that the district court had improperly certified a punitive damages class under the statute because the named plaintiff had no actual damages.[44] The Third Circuit disagreed and—in reaching its conclusion—noted specifically that "the District Court has not made any decision regarding what conduct constitutes a violation or violations" for the purposes of the PCHRIA's statutory damages provision.[45]

The district court made its ruling on that score on remand.[46] Unsurprisingly, the county argued that "violation" under the statute meant only the dissemination of the database itself—"and therefore punitive damages must be capped at $10,000."[47]

---

42. 18 PA. CON. STATS. ANN. § 9183(b)(2) (emphasis added) (West 1979).
43. *See* Taha v. Cty. of Bucks, 862 F.3d 292 (3d Cir. 2017).
44. *Id.* at 303.
45. *Id.* at 305.
46. *See Taha*, 367 F. Supp. 3d at 333–34.
47. *Id.* at 333.

The plaintiff, on the other hand, argued that "each release of criminal history record information—that is, the releases as to each of the 66,799 class members—constituted a violation of the statute."[48]

The district court agreed with the plaintiff. According to the district court, the defendants' argument was based on a flawed assumption: "that a 'violation' is synonymous with an 'act.'"[49] But violation, according to the court, is more appropriately considered with reference to the number of people whose rights have been violated. It provided this example: "If a tortfeasor breaks into a single computer, obtains private information relating to five different people, and publishes that information, the tortfeasor has violated five different peoples' rights and could give rise to five different causes of action, despite only engaging in one act."[50]

It also distinguished between its case and *Tomasello v. Rubin*,[51] which addressed a violation of the Privacy Act of 1974. [52] In *Tomasello*, the defendant faxed one letter to 4,500 people.[53] The *Tomasello* plaintiff argued he was entitled to statutory damages for each letter.[54] The D.C. Circuit disagreed, finding that—consistent with the concept that waivers of sovereign immunity, as the Privacy Act in this case was, should be narrowly construed—the sending of the letter was the failure for which the

48. *Id*.

49. *Id*.

50. *Id*.

51. 167 F.3d 612 (D.C. Cir. 1999).

52. 5 U.S.C. § 552a (1974).

53. *Tomasello*, 167 F.3d at 616.

54. *Id.* at 617.

defendant was liable.[55] According to the *Taha* court, however, the appropriate analysis under the PCHRIA was the inverse: "Plaintiff's claim does not turn on the number of people to whom private information was impermissibly sent, but rather on the number of class members whose information was published."[56] Ultimately, the jury awarded—and the district court upheld—a statutory damages award of $1,000 per class member, totaling over $60 million in damages.[57]

This approach may raise due process concerns, however. In *Taha*, the district court ruled that due process did not apply because the defendant was a governmental entity.[58] But for private defendants, the calculus is likely different.[59] Indeed, the potential for large damages awards may also make courts reluctant to certify classes.[60] The role due process plays in selecting among

---

55. *Id.* at 617–18.

56. Taha v. Bucks Cty, Pa., 367 F. Supp. 3d 320, 334.

57. Taha v. Bucks Cty. Pa., 408 F. Supp. 3d 628, 646–47.

58. *Id.* at 648–49 ("[T]he Due Process Clause protects persons, not governmental entities such as Bucks County.").

59. *See, e.g.*, Golan v. FreeEats.com, Inc., 930 F.3d 950 (8th Cir 2019) (holding that $1.6 billion in statutory damages for an "innocent" violation violated the Due Process Clause); J. Gregory Sidak, *Does the Telephone Consumer Protection Act Violate Due Process as Applied?*, 68 FLA. L. REV. 1403 (2016) (calculating that a TCPA violation causes only approximately $.70 of harm per violation); Maryland v. Universal Elections, Inc., 862 F. Supp. 2d 457 (D. Md. 2011); *see also* Larson v. Harman-Mgmt. Corp., No. 1:16-cv-00219-DAD-SKO, 2019 U.S. Dist. LEXIS 219294 (E.D. Cal. Dec. 18 2019) (approving settlement agreement of TCPA, in part, because "likelihood that an award of damages in the billions would be deemed unconstitutional").

60. *See, e.g.*, Parker v. Time Warner Entm't Co., L.P., 331 F.3d 13 (2d Cir. 2002) (acknowledging due process concerns for large damages awards in class cases and noting that "[i]t may be that the aggregation in a class action of large numbers of statutory damages distorts the purpose of both statutory damages and class actions.").

the possible methodologies for quantifying violations is set forth below.

D. Option Four: Calculation of Violations Based on the Number of Pieces of Personal Information Impacted By Failure to Comply

A fourth approach would be to treat each piece of personal information, for each consumer, affected by a violation of a statute as a "violation" under the civil penalties cap. In a way, a version of this approach has been adopted in state unfair competition laws insofar as those laws sometimes focus on the pieces of information disseminated for false advertising purposes.[61]

This approach has intuitive appeal. If each piece of personal information is treated as a discrete "thing," and conduct that results in a violation as to a single piece of personal information is a violation, then it makes sense that conduct that results in violations as to ten pieces of personal information would be treated as ten violations. But defining a "piece" of personal information

---

61. *See, e.g.*, Commonwealth v. Fall River Motor Sales, Inc., 565 N.E.2d 1205, 1213 (Mass. 1991) (holding that each advertisement disseminated constituted violation of a consent judgment despite the fact that the advertisements were identical and paid for in a single transaction); *In re* Miss. Medicaid Pharm. Average Wholesale Price Litig., 190 So. 3d 829, 847 (Miss. 2015) (upholding statutory damages based on the number of falsely reported average wholesale prices of medications); State *ex rel.* Wilson v. Ortho-McNeil-Janssen Pharm., Inc., 777 S.E.2d 176, 204 (S.C. 2015) (reducing per violation damages but upholding application of uniform civil penalty to each "sample box" defendant distributed in violation of state unfair trade practices act); State v. Ralph Williams' N. W. Chrysler Plymouth, Inc., 553 P.2d 436 & n.12 (1976) (upholding a per-misrepresentation civil penalty and noting that "[a] single advertisement may include a number of misrepresentations . . . [e]ach of these acts is a separate violation"); State v. Going Places Travel Corp., 864 N.W.2d 885, 898 (2015) (violations calculated by multiplying the number of misrepresentations by the number of consumers).

may be difficult. For example, would a record of a visit to web page that is tied to an IP address be a "piece"? Would the IP address and the address of the web page be "pieces"?

And as with the consumer/statutory section approach, this approach may tend to result in damages calculations that may violate the Due Process Clause. Depending on the definition of "piece" of personal information, amounts calculated under this method may easily be ten, one hundred, or one thousand times amounts calculated under the consumer/statutory section approach, which creates enormous theoretical exposures that may result in overdeterrence or an inefficient overspend on compliance.

E. Option Five: Calculation of Violations Based on the Number of Days Violation Occurred

Finally, "violation" might mean that each day a statutory violation continues after a demand to cease is treated as a separate "violation" for civil penalties purposes. At least one consumer protection statute explicitly provides for this sort of calculation—though with a limit. The Cable Privacy Act[62] permits the court to award actual damages, though those damages cannot be less than the statutory damages of $100 for each day of violation or $1,000, whichever is greater.[63]

---

62. 47 U.S.C. § 551(f)(2)(A) (1984).

63. *See also* 18 U.S.C. § 2520(c) (2018) (providing for "statutory damages of whichever is the greater of $100 a day for each day of violation or $10,000" under the federal Wiretap Act); 33 U.S.C. § 1319(d) (2019) (providing for civil penalty "not to exceed $25,000 per day for each violation" of the Clean Water Act); WASH. REV. CODE ANN. § 42.56.550(5) (West 2017) (permitting trial court to award "an amount not to exceed one hundred dollars for each day that he or she was denied the right to inspect or copy" public records under the public records act).

In theory, unlike the approaches outlined above, this approach creates incentive for violators to cure quickly, because exposure increases linearly with time—which, in turn, brings exposure in line with the public interest in cessation of violations.

But adding a violation for each day the defendant fails to cure would likely further increase civil damages, especially if it is coupled with other "high exposure" methods like per-consumer or per-piece of information. That would likely further deepen due process concerns and a hesitancy to certify class actions.

F. Due Process Concerns and Their Role in a "Per Violation" Analysis

Due process concerns are present in any evaluation of the methodologies set forth above. In many ways statutory damages seem comparable to punitive damages—which are often challenged on due process grounds—especially insofar as both may be disconnected from compensatory damages. As to punitive damages, in the seminal cases of *State Farm Mutual Auto Insurance Co. v. Campbell* and *BMW of North America, Inc. v. Gore,* the Supreme Court instructed courts to consider various factors in determining whether an award of punitive damages comports with due process: "(1) the degree of reprehensibility of the defendant's misconduct; (2) the disparity between the actual or potential harm suffered by the plaintiff and the punitive damages award; and (3) the difference between the punitive damages awarded by the jury and the civil penalties authorized or imposed in comparable cases."[64]

64. State Farm Mut. Auto Ins. Co. v. Campbell, 538 U.S. 408, 418 (2003); *see also* BMW of N. Am., Inc. v. Gore, 517 U.S. 559 (1996).

But courts have also held that the "guideposts" the Supreme Court imposed on punitive damages in the *Campbell* and *Gore* do not apply to statutory damage awards.[65] According to these courts, due process prohibits excessive punitive damages awards because the defendant lacks fair notice of the severity of the penalty it may face for its conduct.[66]

These courts instead follow the Supreme Court's ruling in *St. Louis, I.M. & Southern Railway Co. v. Williams*:[67] A statutory damages award violates due process only when the award is "so severe and oppressive as to be wholly disproportioned to the offense and obviously unreasonable."[68] The standard is "extraordinarily deferential—even more so than in cases applying

65. *See, e.g.*, Capitol Records, Inc. v. Thomas-Rasset, 692 F.3d 899, 907–08 (8th Cir. 2012); *see also* Sony BMG Music Entm't v. Tenenbaum, 719 F.3d 67, 70–71 (1st Cir. 2013) ("[W]e conclude, as have other courts, that the standard articulated in *Williams* governs the review of an award of statutory damages under the Copyright Act."); Zomba Enters., Inc. v. Panorama Records, Inc., 491 F.3d 574, 587 (6th Cir. 2007) ("We know of no case invalidating [an award of statutory damages] under *Gore* or *Campbell*, although we note that some courts have suggested in dicta that these precedents may apply to statutory-damage awards.").

66. *See Capitol Records*, 692 F.3d at 907; *Sony BMG*, 719 F.3d at 70 ("The concerns regarding fair notice to the parties of the range of possible punitive damage awards, which underpin *Gore*, are simply not present in a statutory damages case where the statute itself provides notice of the scope of the potential award.").

67. 251 U.S. 63 (1919).

68. *Zomba*, 491 F.3d at 587 (quoting *Williams*, 251 U.S. at 66–67); *see also* Golan v. FreeEats.com, Inc., 930 F.3d 950, 962 (8th Cir. 2019) (applying *Williams* standard to TCPA claim and upholding finding that $1.6 billion statutory damages award violated due process); Perez-Farias v. Global Horizons, Inc., 499 F. App'x 735, 737 (9th Cir. 2012) (applying *Williams* standard to claim under the Washington Farm Labor Contractors Act and finding statutory damages did not violate due process).

abuse of discretion review."[69] Thus, statutory damages may be even more disconnected from compensatory damages than punitive damages.[70] And when deciding whether the statutory damages award fails to comport with due process, some courts look to the award as a whole—not the awards for individual "violations." That is, "[t]he absolute amount of the award, not just the amount per violation, is relevant to whether the award" violates due process under the reasoning in *Williams*.[71]

One district court, for example, slashed a TCPA-mandated statutory damages award of $1.6 billion to $32 million.[72] In a post-trial motion for reduction of excessive damages, the defendant argued that the statutory damages of $500 per call for 3,242,493 calls—totaling $1,621,246,500—was so excessive it violated the Due Process Clause of the Fifth Amendment.[73] The district court agreed, calling the required damage award "obviously unreasonable and wholly disproportionate to the offense" and awarded the plaintiffs the amount of $10 per call.[74]

On appeal, the class members argued that the statutory damages of $500 per call do not violate the Due Process Clause and should not have been reduced.[75] Although the circuit court agreed with the class members that nothing in the relevant provision of the TCPA allows for the reduction of statutory

---

69. *Zomba*, 491 F.3d at 587.

70. *See, e.g.*, *id.* at 588 (upholding a 44:1 ratio of statutory to compensatory damages); *Williams*, 251 U.S. at 67 (upholding what amounted to a 113:1 ratio of statutory to compensatory damages).

71. *See Capitol Records*, 692 F.3d at 910.

72. Golan v. Veritas Entm't, LLC, No. 4:14CV00069 ERW, 2017 WL 3923162, at *1 (E.D. Mo. Sept. 7, 2017).

73. *Id*.

74. *Id.* at *4.

75. Golan v. FreeEats.com, Inc., 930 F.3d 950, 962 n.11 (8th Cir. 2019).

damages, it held that the district court did not err in concluding the statutory damages of $1.6 billion violated the Due Process Clause.[76] It concluded: "[u]nder [the] facts [of this case], $1.6 billion is 'so severe and oppressive as to be wholly disproportioned to the offense and obviously unreasonable.'"[77]

Not all courts follow this reasoning, however. The district court in *Wakefield v. ViSalus, Inc.*,[78] for example, explicitly rejected this line of thinking. In *Wakefield*, as explained above, a jury found that the defendant ViSalus had violated the TCPA 1,850,440 times, for a total damages award of $925,220,000. The defendant challenged the award as excessive and thus unconstitutional under the standard in *Williams*.[79] The district court—while noting that the Ninth Circuit had not decided the issue—concluded that due process does not require reducing aggregate statutory damages.[80] Because *Williams* analyzed only "the penalty for a *single* statutory violation," according to the district court, it implies that "the Supreme Court construed 'penalty' to mean the fine for a single statutory violation, not for the aggregate amount of damages."[81] And because the TCPA's $500 per violation statutory damages was not so unreasonable or oppressive as to violate due process, it was constitutional—all that was left was the "arithmetic" of multiplying the number of violations by the minimum statutory penalty for each violation.[82]

---

76. *Id*. at 963.

77. *Id*. (quoting St. Louis, I.M. & S. Ry. Co. v. Williams, 251 U.S. 63, 67 (1919)).

78. No. 3:15-cv-1857-SI, 2020 WL 4728878 (D. Or. Aug. 14, 2020).

79. *Id*. at *2.

80. *Id.* at *3.

81. *Id.* (emphasis original).

82. *Id.* at *4.

Anything else, according to the district court, would be at odds with *Williams* "and would effectively immunize illegal conduct if a defendant's bad acts crossed a certain threshold."[83] Quoting the Seventh Circuit, the *Wakefield* court concluded: "Someone whose maximum penalty reaches the mesosphere only because the number of violations reaches the stratosphere can't complain about the consequences of its own extensive misconduct."[84]

83. *Id*.

84. *Id.* (quoting United States v. Dish Network, *LLC*, 954 F.3d 970, 979–80 (7th Cir. 2020)).

IV. ARTICULATING A STANDARD FOR THE MEANING OF PER VIOLATION

The statutory landscape and applicable case law suggest that there is no one-size-fits-all answer to how violations should be quantified. Rather, the calculation of violations depends on the language and purpose of the statute and the nature of the conduct. As a result, it is quite possible that the same exact language could be subject to different interpretations as used in different laws, jurisdictions, or fact patterns.

As an initial matter, courts faced with a statutory damages or penalties provision will apply familiar principles of statutory interpretation, which are not addressed extensively in this paper. These will generally include looking initially at the plain meaning of the statute, and if that does not provide the answer, applying additional tools such as legislative history, a comparison to other language in the statute, and legislative intent.[85] Notably, in the context of damages provisions, which, depending on the mathematical calculation, could quickly lead to results in the billions of dollars, courts will seek to avoid interpreting the statute in a way that leads to absurd results or in a way that is inconsistent with due process.[86] Courts will also look to determine the legislative intent, which in the case of privacy damages and penalties provisions may include both deterrence and compensation elements.[87]

---

85. *See* United States v. LKAV, 712 F.3d 436 (9th Cir. 2013).

86. *See* Sloan v. Soul Circus, Inc., No.: 15-01389 (RC), 2015 WL 9272838, at *8 n.8 (D.D.C. 2015) (noting in the context of a remand petition that "'[i]n statutory interpretation it is a given that statutes must be construed reasonably so as to avoid absurdities . . . .' The Court cannot adopt the Circus's damages theory when such absurd consequences might follow." (quoting *In re* Nofziger, 925 F.2d 428, 434 (D.C. Cir. 1991) (*per curiam*))).

87. *See, e.g.*, Cabell v. Markham, 148 F.2d 737, 739 (2d Cir. 1945), *aff'd*, 326

As noted above, some statutes provide courts with more specific direction on how to assess the number of violations and calculate a penalty or civil damage award.[88] However, for those statutes that simply authorize a penalty or damages award "per violation," the case law, taking California as an example, suggests that the determination of the number of violations may depend on the circumstances of the case.[89] In *People v. Witzerman*, for example, the court upheld the trial court's decision to assess penalties for false advertising "roughly on a per victim rather than per culpable statement made basis."[90] The court held that "[w]hat constitutes a single violation . . . depends on the type of violation involved, the number of victims and the repetition of the conduct constituting the violation—in brief, the circumstances of the case."[91]

In subsequent cases, the California Court of Appeals has continued in this vein, deferring to the trial court's application of the facts in determining the number of violations.[92]

While varying circumstances will lead to different results,

U.S. 404 (1945) ("[R]emember that statutes always have some purpose or object to accomplish, whose sympathetic and imaginative discovery is the surest guide to their meaning.").

88. *See* Section II.B, *supra*.

89. *See* People v. Witzerman, 29 Cal. App. 3d 169, 181 and n.8 (Cal. Ct. App. 1972).

90. *Id*. at 180.

91. *Id.* at 171.

92. *See* People v. Overstock.com, Inc., 219 Cal.Rptr.3d 65, 85, (Cal. Ct. App. 2017), as modified (June 23, 2017) (noting that the trial court considered determining the number of violations "by the number of Californians who saw the offending advertisements, by the number of sales made through the offending pages, and by the number of days Overstock violated the statutes," and affirming the trial court's decision to calculate penalties on a per-day basis).

the number of violations should be calculated with reference to the specific facts the plaintiff proves in connection with the alleged statutory violations. This rule is illustrated in *State v. Ralph Williams' North West Chrysler Plymouth, Inc.*,[93] in which the Washington Attorney General alleged that a car dealership violated the Washington Consumer Protection Act by making ten different categories of misrepresentations to prospective car buyers.[94] The court concluded that each misrepresentation could constitute a separate violation, so long as "[e]ach cause of action required [respondent] to prove divergent facts to establish a violation."[95]

Thus, in evaluating the meaning of "per violation" measure of damages where the statute provides no further guidance, the following test can be articulated:

> **In the absence of clear statutory language or legislative history to the contrary, each violation is considered a separate and distinct violation when divergent facts are required to establish such a violation.**

This analysis will be backstopped by the due process limitations discussed in detail in the previous section. In particular, in the first instance, courts will look to avoid interpretations of the statute that will lead to significant constitutional concerns "where the text fairly admits of a less problematic construction."[96] In determining an appropriate level of damages, courts may also look to common law principles that have evolved in particular in the area of consumer protection laws to provide

93. 553 P.2d 423 (1976).

94. *Id*. at 430–31, 436.

95. *Id.* at 436.

96. Pub. Citizen v. U.S. Dep't of Justice, 491 U.S. 440, 455 (1989).

additional factors that they (or jurors) may apply. These factors include the good or bad faith of the defendant, the injury to the public, the defendant's ability to pay, and the desire to eliminate the benefits derived from the legal violations.[97]

Below are three scenarios that illustrate how the number of violations can be determined by looking to the specific, divergent facts the plaintiff has proved.

A. Scenario One: California Consumer Privacy Act

The CCPA grants consumers the right to direct organizations not to sell their personal information.[98] "A business that has received direction from a consumer not to sell the 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."[99] As stated before, under California Civil Code Section 1798.155(b), "[a]ny business, service provider, or other person that violates this title shall be . . . 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."

Assume a company called The Data Guys collects and sells personal information of California consumers. The California Attorney General brings an action and proves the following facts: 500 consumers sent an opt-out notice to The Data Guys. After receiving these notices, The Data Guys sold personal information of 250 of the consumers to Company A. The Data

97. *See* State *ex rel.* Woodard v. May Dep't Stores Co., 849 P.2d 802, 810 (Colo. App. 1992).

98. *See* CAL. CIV. CODE § 1798.120(a) (West 2020).

99. *Id.* § 1798.120(d).

Guys then sold the personal information of all 500 consumers to Company B. Later, the Data Guys sold the personal information of 150 of the consumers to Company C.

The Data Guys may argue that there can only be three violations, one for each of its sales to Companies A, B, or C. Or The Data Guys could argue that there were only 500 violations—one per each consumer. However, the California Attorney General has arguably proved 900 violations (one violation per customer per illegal sale—250 plus 500 plus 150). This approach appears sensible. There is no constitutional concern with multiple punishments for the same conduct. And the number of violations is tied to specific acts that must be proved with individualized evidence, each of which causes a distinct harm to the privacy interest of the affected consumers.

What if The Data Guys sold multiple pieces of personal information relating to each consumer? The CCPA's definition of "personal information" is quite broad and includes, for example, "[i]nternet 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."[100] With a little creativity, the Attorney General might be able to identify and prove hundreds or even thousands of "divergent facts"—i.e., distinct pieces of personal information sold by The Data Guys—potentially adding an exponential multiplier to the number of violations. In this instance, the trial court would retain discretion to determine the number of violations in a manner that is reasonable given the circumstances.[101]

---

100. *Id*. § 1798.140(o).

101. *See* People v. Overstock.com, Inc., 219 Cal.Rptr.3d 65, 85-86 (Cal. Ct. App. 2017) (affirming the trial court's use of per-day methodology for determining the number of violations where other approaches "would result in

B. Scenario Two: Colorado Security Breach Notification Law

Colorado law requires organizations that maintain, own, or license personal information about Colorado residents to provide notice to the affected residents when a security breach results or could result in the misuse of their personal information.[102] Penalties may be applied for each violation of Colorado Revised Statutes Section 6-1-716.[103]

Assume a company called The Open Network is hacked by cybercriminals. After gaining access to The Open Network's computer system, the attackers obtain the credentials of an employee and begin emailing The Open Network's unencrypted files to the attacker's account. When all is said and done, the hackers have stolen the names and social security numbers of 10,000 Colorado residents. The Open Network does not provide notice until a whistleblower threatens to inform the Colorado Attorney General. At this point, The Open Network provides notice, but 180 days have passed since the time that The Open Network should have provided notice under C.R.S. § 6-1-716. The Attorney General subsequently brings suit for failure to provide timely notice.

The Attorney General proves the following facts: Ten thousand Colorado residents had their information stolen, and The Open Network didn't provide notice to any of them. The Open Network's failure to provide timely notice lasted 180 days.

---

excessive penalties of at least hundreds of millions of dollars"); People v. Witzerman, 29 Cal. App. 3d 169, 180 (Cal. Ct. App. 1972) (finding no fault in the trial court's failure to "exhibit[] mathematical exactitude" and affirming the court's decision to apply a penalty for only a subset of the violations the court found).

102. COLO. REV. STAT. ANN. § 6-1-716 (West 2018).

103. *See* COLO. REV. STAT. ANN. § 6-1-112 (West 2019).

The Open Network might argue that the security breach was an isolated incident and that its failure to provide timely notice was therefore just a single violation. However, because the statute requires notice to all affected consumers, C.R.S. § 6-1-716(2), and the Attorney General proved a failure to provide notice to each one of them of them, the court could find 10,000 violations—one for each Colorado resident who did not receive the required notice.

The Attorney General might argue that there was a violation for each day that each consumer did not receive the required notice. According to the Attorney General, the number of violations would be 1,800,000 (10,000 times 180). However, the facts the Attorney General has proved are that notice was given 180 days late to 10,000 residents of State X. There are no "divergent facts" that establish a separate violation for each of the 10,000 residents for each day. Moreover, courts may be reluctant to read a "per day" component into the provision when it is entirely absent from the language of the statute, whereas other statutes explicitly incorporate a "per day" element.[104] The better result is a finding of 10,000 violations, one for each consumer the Attorney General proved was entitled to notice and did not receive it.

C. Scenario Three: Illinois Biometric Information Privacy Act

The Illinois Biometric Information Privacy Act (BIPA) imposes requirements on businesses that collect or possess biometric information (for example, retina or iris scans, fingerprints, or scans of hand or face geometry).[105] One requirement is

104. *See, e.g.*, FLA. STAT. ANN. § 501.171(9) (West 2019) (authorizing civil penalties of $1,000 per day for the first 30 days and $50,000 per day for days 31 to 180).

105. 740 ILL. COMP. STAT. ANN. § 14/1, *et seq.* (West 2008).

that a covered business may not "collect, capture, . . . or otherwise obtain a person's or a customer's biometric identifier or biometric information" without first obtaining informed consent from the person.[106] As noted above, among other remedies, BIPA provides for liquidated damages of $1,000 "for each violation" or $5,000 for "intentional violations."[107]

Assume that a hotel chain decides to replace keys with iris scans for controlling entry to its hotel rooms. At check-in, guests are asked to provide an iris scan after showing their ID. Under this new system, the guest's room door opens automatically when the guest approaches the door. Each time a guest enters her room, the hotel collects and retains the scan to improve its scanning technology. While guests are informed of the new procedure at check-in, the hotel fails to obtain the guests' informed, written consent as required by BIPA. Applying the statutory language of BIPA to this conduct, the court would be justified in finding a violation for each time that a guest had his or her iris scanned.

In the end, external consensus around how to calculate "per violation" damages is challenging, as the answer can lead to outsized results one way or the other. Ideally, legislatures would do a better job of answering this question explicitly in the first instance. If the intent is to punish conduct on a "per incident" basis, on a daily basis, or on a per consumer basis, this would be easy enough to incorporate into the language of the statute itself, and there are multiple examples of where legislatures have done the hard work to incorporate more concrete and explicit language along these lines in any number of different contexts. In the absence of such concrete language, courts will

106. *Id*. § 14/15(b).

107. *Id*. § 14/20.

be left to interpret the language that is there, and as discussed above, will do so using the tools that they always use. The law suggests that courts have a certain degree of flexibility in undertaking this analysis, and rigid calculations, especially those that lead to absurd or even unconstitutional results, will not prevail. Rather, courts will likely consider the legislative and remedial intent and look to avoid extreme outcomes on either side of the range of potential answers to the question.

V. CONCLUSION

Although the country's statutory framework for privacy litigation provides some uncertainty concerning how violations of certain statutes should be quantified, existing case law provides guidance when the statutes are ambiguous. Although greater certainty in the construction of privacy statutes can better alleviate uncertainty, application of the above flexible analysis can provide clarity for violators, certainty for regulators, and protection for consumers.