

# The Sedona Conference WG11 Brainstorming Group Outline – Advisability of Adopting a Strict Liability Regime for Data Breaches Involving Personal Information (October 2021)

---



This confidential outline of The Sedona Conference Working Group 11 on Data Security and Privacy Liability is not for publication or distribution to anyone who is not a member of Working Group 11 without prior written permission. Comments and suggested edits to this document are welcome by email to [comments@sedonaconference.org](mailto:comments@sedonaconference.org) no later than November 29, 2021.

## **The Sedona Conference WG11 Brainstorming Group Outline – Advisability of Adopting a Strict Liability Regime for Data Breaches Involving Personal Information (October 2021)**

### **Brainstorming Group Members:**

Andrea D'Ambra (Brainstorming Group Leader)

Mark Bailey

Chris Cronin

Kelly Ruane Melchiondo

Tony O'Neill

Krysta Pachman

Carrie Parikh

David Schwartz

Harper Segui

David Sella-Villa

Hon. Tom Vanaskie (ret.)

Phil Yannella

Ryan Kriger (Steering Committee Liaison)

This confidential outline of The Sedona Conference Working Group 11 on Data Security and Privacy Liability is not for publication or distribution to anyone who is not a member of Working Group 11 without prior written permission. Comments and suggested edits to this document are welcome by email to [comments@sedonaconference.org](mailto:comments@sedonaconference.org) no later than November 29, 2021.

## **I. Background**

Generally, strict liability holds manufacturers of products liable in tort for putting defective products into the marketplace, which injure consumers. The policy underpinnings as described in the Restatement Third are instructive in considering whether strict liability should be applied data breach litigation:

Holding a manufacturer liable for product-related injuries without a showing of negligence can reasonably be justified on two grounds, both of which may be deemed socially valuable. First, since manufacturers are in the best position to control and eliminate the risks posed by defective products that might roll off the assembly line, it does not seem unreasonable or unfair to impose on them an economic incentive to develop the most effective quality control systems attainable. Any departure from best efforts in this area can justifiably be made extremely costly for the manufacturer. Second, even when an occasional defect does slip through, the burden of a resulting injury can be shouldered better by the manufacturer than by the consumer. While it would be irrational to say that society expects defect-free production runs, it is not unreasonable to require that the manufacturer foot the bill for injuries that result when an inadvertently defective product causes harm, notwithstanding his due care efforts. The manufacturer can spread the risk through insurance and price adjustments, whereas the injured individual might suffer a crushing financial blow underwriting the loss himself...

§ 12:2. Strict liability under the Restatement Third, Torts: Products Liability, 2 The Law of Prod. Warranties § 12:2. Additionally, and as alluded to above, another policy purpose is to relieve an injured plaintiff of the evidentiary burdens inherent in a negligence action.<sup>1</sup> Limitations of negligence theories generally is what prompted development and expansion of the doctrine.<sup>2</sup>

States vary in application, but generally the most instructive source is the Restatement. Some states, for the purpose of analyzing the elements and defenses of strict liability, have held there is no distinction between negligence and strict liability. Others have employed specific tests, discussed below.

Unless otherwise indicated, Restatement Third citations are utilized throughout.

## **II. APPLYING STRICT LIABILITY IN PRODUCT DEFECT CASES:**

### **(A) Three Types of Strict Product Liability:<sup>3</sup>**

1. Manufacturing Defects: Defects arising from flaws in the manufacturing process;

---

<sup>1</sup> *Greenman v. Yuba Power Products, Inc.*, 59 Cal. 2d 57, 63 (1963). [need parentheses here]

<sup>2</sup> *Cronin v. J.B.F. Olson Corp.*, 8 Cal. 3d 121 (1972). [need parentheses here]

<sup>3</sup> *Garrett v. Howmedica Osteonics Corp.*, 214 Cal. App. 4th 173 (2013). [need parentheses here]

This confidential outline of The Sedona Conference Working Group 11 on Data Security and Privacy Liability is not for publication or distribution to anyone who is not a member of Working Group 11 without prior written permission. Comments and suggested edits to this document are welcome by email to [comments@sedonaconference.org](mailto:comments@sedonaconference.org) no later than November 29, 2021.

2. Design Defects: Defects that exists when the product is built in accordance with its intended specifications, but the design itself is inherently defective;<sup>4</sup> and
3. Warning Defects: The product is dangerous due to adequate warnings or instructions.

**(B) Elements and Tests:**

1. Primary Elements Establishing Strict Liability in Product Liability Cases:<sup>5</sup>
  - (a) Plaintiff was injured by a defect in the product; and
  - (b) The product was defective when it left the hands of the retailer or manufacturer.
2. Tests- Defective Design:

*Consumer Expectation Test.* In determining whether a product design is defective, some courts under [Restatement (Second) of Torts] § 402A invoke a “consumer expectation” test. If the dangerous design would catch the average consumer by surprise, the product is defective. This test is consistent with the language of Comment g to § 402A. § 12:3. Warranty and strict tort compared—Defect requirement, 2 The Law of Prod. Warranties § 12:3

*Risk Utility Test.* The risk of harm is balanced against the utility of the product in the form it was produced. Under this standard, the court asks how useful the product is to the general public; how feasible it is for the manufacturer to spread his liability losses in the form of insurance or higher prices; how obvious the danger in the product is; how easily the user could avoid the danger by the exercise of due care; how difficult it is for the manufacturer to change the design; how available are substitute products that are designed more safely; and how likely is serious injury caused by the design? § 12:3. Warranty and strict tort compared—Defect requirement, 2 The Law of Prod. Warranties § 12:3.

Here, a plaintiff need only demonstrate that the design proximately caused injuries. Once demonstrated, burden shifts to defendant to establish the benefits of the challenged design, when balanced against such factors as the feasibility and cost of alternative designs, outweigh its inherent risk of harm.<sup>6</sup>

---

<sup>4</sup> *Barker v. Lull Engineering Co.*, 20 Cal. 3d 413 (1978).

<sup>5</sup> *See Daly v. Gen. Motors Corp.*, 20 Cal. 3d 725, 758 n.2 (1978) (citing *Jiminez v. Sears, Roebuck & Co.*, 4 Cal. 3d 379, 393 (1971)): “To prevail at trial on a theory of strict liability in products cases, plaintiff must prove that (1) he was injured by a defect in the product, and (2) the product was defective when it left the hands of the retailer or manufacturer.”

<sup>6</sup> *Chavez v. Glock, Inc.*, 207 Cal. App. 4<sup>th</sup> 1283, 1303, 144 Cal. Rptr. 3d 326, 343 (2012)

This confidential outline of The Sedona Conference Working Group 11 on Data Security and Privacy Liability is not for publication or distribution to anyone who is not a member of Working Group 11 without prior written permission. Comments and suggested edits to this document are welcome by email to [comments@sedonaconference.org](mailto:comments@sedonaconference.org) no later than November 29, 2021.

### 3. Failure to Warn:

Unlike a design defect, this strict product liability cause of action is intended to drive a manufacturer to inform consumers about a product's hazards and faults of which they are unaware, so that they can refrain from using the product altogether or evade the danger by careful use.

The manufacturer must have knowledge (actual or constructive) of the risk.<sup>7</sup> Defendant in a strict products liability action based on an alleged failure to warn of a risk of harm can present evidence of the state-of-the-art; that is, evidence that the particular risk was neither known nor knowable by the application of scientific knowledge available at the time of manufacture or distribution.

## III. TYPICAL DEFENSES:

(A) **Economic Loss Doctrine:** This doctrine shields a party from tort liability when damages are purely economic and without accompanying personal injury or property damage. The primary purpose of the ELD is to prevent a party from seeking greater recovery in tort than would otherwise be available under the agreed-upon remedies outlined in the parties' contract. Exceptions to the ELR exist in data breach litigation for negligence, and it would likely apply to strict liability if applied in such a context (e.g. "special duty").

(B) **Assumption of Risk (a.k.a. "Obvious Danger Rule")**<sup>8</sup>

- (a) Consumer voluntarily and unreasonably proceeds to encounter a known danger;
- (b) Consumer must become aware of the defect and danger and still proceed unreasonably to make use of the product.

2. **Sophisticated User Defense:**<sup>9</sup> Exempts manufacturer from obligation to provide users with warnings about product's potential hazards when the users are "sophisticated users."

(C) **Ordinary Contributory Negligence:** Contributory negligence takes into account the failure of the plaintiff to act prudently as a contributory factor in the injury suffered and may sometimes reduce the amount recovered from the defendant. This ordinary contributory negligence does not bar recovery in a strict liability action.

## IV. HOW ARE DATA BREACH CASES SIMILAR TO OR ARE DIFFERENT FROM PRODUCTS LIABILITY CASES

(A) Strict liability in products cases is premised on the fact that the manufacturer of a product has sole control over the manufacturing process. The harm is inflicted by the product. Conversely, in the vast majority of data breach cases, any harm caused

---

<sup>7</sup> *Anderson v. Owens-Corning Fiberglas Corp.*, 53 Cal. 3d 987, 995 (1991).

<sup>8</sup> *Barth v. B. F. Goodrich Tire Co.* 265 Cal. App. 2d 228, 243 (1968).

<sup>9</sup> *Johnson v. American Standard, Inc.*, 43 Cal. 4th 56 (2008).

This confidential outline of The Sedona Conference Working Group 11 on Data Security and Privacy Liability is not for publication or distribution to anyone who is not a member of Working Group 11 without prior written permission. Comments and suggested edits to this document are welcome by email to [comments@sedonaconference.org](mailto:comments@sedonaconference.org) no later than November 29, 2021.

to the data subject is caused by an outside actor committing a crime against the organization whose systems were breached and the data subjects themselves.

1. It's widely acknowledged in the data security community that there is no hack-proof system. So why would an organization be held strictly liable when they have taken reasonable security measures and still are breached?
  2. In cases where a misconfiguration of an organization's systems or accidental distribution publicly exposes data that is intended to be confidential, it might be argued that the organization had sole control over the process and protections in place, and might therefore be held strictly liable.
- (B) In data breach cases, evidence of how the organization protected information is readily available in audit logs and written security protocols.
- (C) Data breaches do not necessarily cause harm to data subjects. In fact, in many instances, the harm is borne solely by the organization suffering the breach. In products liability cases, the harm is borne solely by the consumer who uses and is injured by a defective product. Data breaches always cause harm to the organization as it is the primary victim of the attack. While some breaches may target data subject information such as credit card numbers, the most popular and prevalent data breaches presently –ransomware—shut down an organization's IT infrastructure and often take confidential information to use as leverage to get the organization to pay the ransom. Once the ransom is paid, the data serves little purpose other than to take up space on whatever cloud storage account the threat actor used. Moreover, in most cases, even if the threat actor wanted to use the PII of data subjects located in the data set, the amount of effort required to locate and compile that information is likely far greater than its worth on the dark web.

## V. HARMS

(A) Potential Harms/Damages from Data Breach:

1. **To Data Subjects:**
  - (a) Costs associated with actual identity theft and fraud.
  - (b) Time and/or money spent mitigating risk of harm → in some instances, courts view this through the lens of preventing future, not actual harm; or otherwise attempting to manufacture damages.
  - (c) Diminution of the value of PII.<sup>10</sup>

---

<sup>10</sup> *In re Marriott Int'l, Inc., Customer Data Sec. Breach Litig.*, 440 F. Supp. 3d 447, 462 (D. Md. 2020) (“Neither should the Court ignore what common sense compels it to acknowledge—the value that personal identifying information has in our increasingly digital economy. Many organizations, like Marriott, collect personal

This confidential outline of The Sedona Conference Working Group 11 on Data Security and Privacy Liability is not for publication or distribution to anyone who is not a member of Working Group 11 without prior written permission. Comments and suggested edits to this document are welcome by email to [comments@sedonaconference.org](mailto:comments@sedonaconference.org) no later than November 29, 2021.

- (d) Invasion of privacy as cybercriminals traffic information.
- (e) Increased risk of identity theft in the future□ typically held that this is not an actual injury
- (f) Injunctive relief□ defendant is in the best position to remedy the problem and prevent future breaches (in line with general strict liability policy factors, including the defendant shouldering the burden).
- (g) Emotional distress/anxiety.
  - i. “The privacy torts, recognized in the vast majority of states, allow plaintiffs to recover for the disclosure of private information or the improper intrusion into private matters resulting in emotional distress if the defendant’s conduct is ‘highly offensive to the reasonable person.’” Daniel J. Solove & Danielle Keats Citron, *Risk and Anxiety: A Theory of Data Breach Harms*, 96 Tex. L. Rev. at 746.
  - ii. Consider particularly embarrassing/reputational data exposed v. average PII.

**2. To Breached Organizations:**

- (a) Loss of business operations/revenue due to ransomware.
- (b) Ransom payments.
- (c) Information leaked to competitors
- (d) Confidential organization information exposed to other cybercriminals via the dark web.
- (e) Regulatory investigations and potential fines.
- (f) Reputational damage to the organization
- (g) Regulatory compliance and notification costs
- (h) Contractual liability to commercial customers

**VI. PROS AND CONS OF IMPOSITION OF STRICT LIABILITY IN DATA BREACH CASES:**

---

information. Consumers too recognize the value of their personal information and offer it in exchange for goods and services.”).

This confidential outline of The Sedona Conference Working Group 11 on Data Security and Privacy Liability is not for publication or distribution to anyone who is not a member of Working Group 11 without prior written permission. Comments and suggested edits to this document are welcome by email to [comments@sedonaconference.org](mailto:comments@sedonaconference.org) no later than November 29, 2021.

**(A) Policies Supporting Imposition of Strict Liability in Data Breach Cases**

1. Typically, SL has been favored in products liability context because defendant organizations are in a superior position to implement necessary safety controls, bear primary responsibility for such controls and because consumers are reliant upon organizations for safety feature;
2. This policy rationale may be applied to certain kinds of data breaches. For example, data breaches implicating consumer data involving a defendant's own network.
  - (a) Other kinds of data breaches may not align as well with these policy goals – e.g., actions against defendant organizations for breaches involving vendor network.
3. One benefit of SL in products liability context is that has led to the development of safety standards – e.g., warning labels – derived from judicial rulings. This dynamic may also result in baseline standards for data security controls (see below for additional details), which is currently lacking under current negligence-based approach.

**(B) Potential Benefits of Strict Liability in Data Breach Cases**

1. Plaintiffs
  - (a) Imposition of SL would enable injured plaintiffs to more readily recover available damages by eliminating burden of proving liability in certain matters;
  - (b) Potential imposition of SL would theoretically incentivize adoption of baseline security controls, protecting consumers.
2. Defendants
  - (a) Imposition of SL regime would provide defendants with benefit of judicial ruling on legal adequacy of controls
    - i. This contrasts with current negligence-focused litigation in which issue of reasonableness is deemed a jury issue and results in unwillingness of defendants to legally test adequacy of controls.

**(C) Policies Supporting Not Imposing Strict Liability in Data Breach Cases**

1. This is a matter for the legislature, not for the expansion of common law doctrine. See *In re Hannaford Bros. Co. Customer Data Sec. Breach Litig.*, 613 F. Supp. 2d 108 (D. Me. 2009), *aff'd in part, rev'd in irrelevant part sub nom. Anderson v. Hannaford Bros. Co.*, 659 F.3d 151 (1st Cir. 2011)



This confidential outline of The Sedona Conference Working Group 11 on Data Security and Privacy Liability is not for publication or distribution to anyone who is not a member of Working Group 11 without prior written permission. Comments and suggested edits to this document are welcome by email to [comments@sedonaconference.org](mailto:comments@sedonaconference.org) no later than November 29, 2021.

(refusing to expand strict liability doctrine to data breach context and noting “plaintiffs ask me to conclude that this new area of electronic data theft is rife with risk and damage, calling for a new common law remedy. Such an expansion of Maine law is for the Maine Law Court or Legislature, not for me as a federal judge. . . [T]he general common law does not support the expansion of strict liability that the plaintiffs have requested.”).

2. Legislation in the US has not been moving in this direction, and generally contemplates that organizations will be evaluated on whether they implemented reasonable cybersecurity standards to protect data. See, e.g., CCPA, Cal. Civil Code 1798.150(a)(1) (permitting consumers to bring suit if a data breach occurs that was “a result of” the business failing to “implement and maintain reasonable security procedures and practices”). Analogously, recent amendments to the HITECH Act would permit HHS to consider whether organizations meet industry cybersecurity standards, which is almost certainly intended to give HHS more latitude when evaluating organizations who have been breached in spite of taking reasonable steps to safeguard data. See H.R. 7898 (amending the HITECH Act to empower the head of the U.S. Department of Health and Human Services (HHS) to curtail or end audits of, and reduce or eliminate fines for, any healthcare organization deemed to have been complying with the latest cybersecurity standards for at least 12 months).
3. Strict liability doctrine is not intended to apply to activities that are in the common usage. See Restatement (Third) of Torts § 20 (2009). The rationale is that there is a risk warranting strict liability when an individual engaged in uncommon and dangerous activity that poses a risk on others that others do not benefit from (e.g. storage of hazardous chemicals, dynamite blasting). But there is no need for strict liability when many people impose a risk on each other, because all of them enjoy the benefits and share the risks of the activity. See Restatement (Third) of Torts § 20, cmt.(j) (2009) (“Whenever an activity [such as the use of an automobile] is engaged in by a large fraction of the community, the absence of strict liability can be explained by principles of reciprocity. Even though various actors may without negligence be creating appreciable risks, the risks in question are imposed by the many on each other.”). While the activity need not be rare, abnormally dangerous activities are not commonly carried out by a majority of people on a regular basis. Scholars have warned that new technical threats are not necessarily abnormal. Bryan H. Choi, *Crashworthy Code*, 94 WASH. L. REV. 39, 51 (2019) (noting “technological novelty should not be conflated with abnormality” when considering examples such as autonomous vehicles for strict liability protection).
4. The harm caused is economic, not physical. The intention of the strict liability doctrine is to ensure individuals are compensated regardless of negligence for “physical harm.” Restatement (Third) of Torts § 20 (2009)

This confidential outline of The Sedona Conference Working Group 11 on Data Security and Privacy Liability is not for publication or distribution to anyone who is not a member of Working Group 11 without prior written permission. Comments and suggested edits to this document are welcome by email to [comments@sedonaconference.org](mailto:comments@sedonaconference.org) no later than November 29, 2021.

(applying strict liability to abnormally dangerous activity (a) An actor who carries on an abnormally dangerous activity “for physical harm resulting from the activity.”)

5. Organizations should not be held strictly liable for or bear the cost of harms caused by external actors. A negligence standard fairly allocates the cost to those actors who negligently fail to protect data. Normally strict liability is applied to actors who are monetarily incentivized to continue to engage in dangerous activity despite the risks to others (dynamite blasting, use of poisons or explosive, groundwater contamination), but here, organizations are also a victim of the incident.
6. There are standards already established for reasonable data security, e.g. NIST Cybersecurity Framework, ISO 27001, Sedona’s Commentary on Reasonable Data Security.

**(D) Potential Negative Consequences of Strict Liability in Data Breach Cases**

1. Punishes business regardless of the degree of steps they have taken to protect data
2. Fails to account for rapid evolution of cyberattack methods that can target even the best prepared organizations.
3. Opens the door to litigation against nearly all businesses for everyday activities

**VII. Scope of Strict Liability**

Imposition of a strict liability regime will require a determination of the circumstances in which it should be applicable. The following questions would likely need to be answered in evaluating the scope of liability.

**(A) *For What Types of Incidents Should Strict Liability Apply?***

1. Breaches of Personal Data?
  - (a) A data breach at an organization that results in the unauthorized access or acquisition of an individual’s personal data.
  - (b) Most of the discussed justifications for imposition of strict liability are more directly (or even uniquely) applicable to circumstances where an entity is in possession of an individual’s personal data and that data is accessed or acquired by an unauthorized third party.
2. Other Data Incidents?
  - (a) Ransomware Incidents?

This confidential outline of The Sedona Conference Working Group 11 on Data Security and Privacy Liability is not for publication or distribution to anyone who is not a member of Working Group 11 without prior written permission. Comments and suggested edits to this document are welcome by email to [comments@sedonaconference.org](mailto:comments@sedonaconference.org) no later than November 29, 2021.

- i. Some of the highest profile data security incidents in recent years have involved ransomware. These incidents can involve the threat to release information or to deny (or continue to deny) access to information (through encryption) unless a ransom is paid.
- ii. To the extent a ransomware incident involves unauthorized access or exfiltration of personal data, it would likely be treated as a breach of personal data.
- iii. To the extent a ransomware incident involves only actual or threatened denial of access to information, the arguments for imposition of strict liability seem less applicable.

(b) Deletion of Data

- i. In some instances, an organization may suffer an attack that results in the deletion of data or may inadvertently delete data.
- ii. Like ransomware incidents involving denied access to information, the arguments for imposition of strict liability seem less applicable in these circumstances.

**(B)** *To What Degree Should Defendant's Conduct Dictate Imposition of Strict Liability?*

1. In all (or nearly all) data breaches, the organization holding the data is also a victim of an attack by a threat actor. Concerns were expressed within the brainstorming group about imposing strict liability on a victim of a data breach. Some members suggested that imposition of strict liability could be limited to situations where the defendant engaged in certain extreme and disfavored conduct.
2. The following conduct by a defendant that resulted in the breach could be utilized as a trigger for strict liability:
  - (a) Defendant failed to comply with certain baseline reasonable security measures (i.e. failing to require two factor authentication).
  - (b) Defendant made representations that it was compliant with certain standards or met/exceeded certain tests, but was not compliant therewith.
  - (c) Defendant failed to encrypt sensitive data.

**(C)** *Should Only Certain Types of Defendants Be Strictly Liable?*

1. The scope of strict liability could be narrowed by imposing it only on defendants engaged in certain industries or activities.

This confidential outline of The Sedona Conference Working Group 11 on Data Security and Privacy Liability is not for publication or distribution to anyone who is not a member of Working Group 11 without prior written permission. Comments and suggested edits to this document are welcome by email to [comments@sedonaconference.org](mailto:comments@sedonaconference.org) no later than November 29, 2021.

2. For example, strict liability could be imposed only if defendant's primary purpose is the collection, maintenance, and storage of consumers' data (versus incidental collection of data).

**(D)** *Should Only Certain Types of Plaintiffs Be Able To Bring Strict Liability Claims?*

1. The question of public versus private enforcement is addressed elsewhere, but if strict liability applies in actions brought by private litigants, it could be limited to only certain types of plaintiffs.
2. Individuals Whose Data Was The Subject of a Breach
  - (a) If a defendant could be strictly liable for a data breach in an action brought by a private litigant, then the natural plaintiff would seem to individual(s) whose data was the subject of the breach.
3. Third-Party Organizations Suffering Losses as a Result of Data Breaches
  - (a) Many of the arguments for strict liability are not applicable when the plaintiff is not an individual whose personal data is the subject of the breach.
  - (b) Currently the relationships between the organization who suffered the data breach and third-party organizations affected by the breach is governed by contract and the risks of a data breach are allocated between the parties pursuant to contract. For instance, a service provider that holds personal data for an organization may indemnify the organization for any losses suffered as a result of a data breach while the data was in the possession of the service provider.
  - (c) The greater bargaining power of these third-party organizations (versus individuals) would favor against strict liability when actions are brought by third-party organizations.

## **VIII. Data Minimization**

**(A) Definitions of Data Minimization in the Law**

1. Present the concept of data minimization defined in the GDPR.
2. Present how the concept appears in the California, Colorado, and Virginia privacy protection laws.
  - (a) Address how data minimization of PII affects both how much data is collected and how long an organization holds onto that data.
  - (b) The drafting team could suggest a definition of data minimization that considers any differences among these several definitions of

This confidential outline of The Sedona Conference Working Group 11 on Data Security and Privacy Liability is not for publication or distribution to anyone who is not a member of Working Group 11 without prior written permission. Comments and suggested edits to this document are welcome by email to [comments@sedonaconference.org](mailto:comments@sedonaconference.org) no later than November 29, 2021.

data minimization. The definition should consider the context of data breaches and the U.S. class action regime that would use it.

- (c) Absent a U.S. federal law requiring data minimization along the same lines as the GDPR, applying strict liability for failures to comply with data minimization laws would necessarily require a state by state application and the majority of states presently have no data minimization requirements.

**(B) Relationship between Data Minimization and Strict Liability**

1. If an organization violates a legislated data minimization requirement and it suffers a data breach of the PII in question, then the organization would be strictly liable for any damages resulting the breach of that PII.
2. Strict liability would attach immediately to PII that is held in violation of data minimization principle.
3. Strict liability would attach later if the PII is retained beyond its period of utility. Discussion of whether it would be necessary for organization to publish data retention schedules publicly.

**(C) Ending Data's Useful Life**

1. Data Sanitization. An organization can avoid strict liability if it destroys PII through a process of media sanitization.
  - (a) *Need of Data Mapping as a Prerequisite*. Media sanitization is possible once an organization has an effective data mapping and classification system in place. That way the specific media holding the no-longer-useful PII can be clearly identified for sanitization.
  - (b) *NIST Guidance*. NIST has provided guidance on the process of actually deleting data and/or destroying media that contain the PII in question. See NIST SP 800-88 Rev. 1, Guideline for Media Sanitization, and NIST SP 800-53 Rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations, April 2013. Other technical standards might also be considered.
  - (c) *Shifting Burdens for Strict Liability*. Following a prescribed process for media sanitization would create a presumption against strict liability for any resulting breach of the PII in question. Plaintiff could shift the liability standard back to strict liability if it can show that the organization failed to follow a prescribed media sanitization process.

This confidential outline of The Sedona Conference Working Group 11 on Data Security and Privacy Liability is not for publication or distribution to anyone who is not a member of Working Group 11 without prior written permission. Comments and suggested edits to this document are welcome by email to [comments@sedonaconference.org](mailto:comments@sedonaconference.org) no later than November 29, 2021.

2. Deidentification. An organization can avoid strict liability if it successfully de-identifies PII at the end of its useful life.
  - (a) *Different Methods of Deidentification*. Deidentification can include anonymization, redaction, or scrubbing of certain metadata retained from an initial data collection. Successful deidentification allows organizations to derive some use from the data, but with very little risk of the data subject being identified or identifiable. Accordingly, if the event of breach of deidentified data, the organization would not be subject to strict liability because the risk of privacy harms to the data subject would arguably be very small.
  - (b) *Distinguishing the Risk of Deidentification from the Risk of Sanitization*. As compared to data sanitization where the processes of destroying data or media are definitive, de-identification bears at least some risk of being undone.
  - (c) *Current Deidentification Standards in the Law*.
    - i. GDPR guidance on anonymization, as a method of deidentification, strongly suggests that the process must be irreversible. In the GDPR's accountability model, organizations would need to demonstrate compliance with this standard. If anonymization were used as means of avoiding strict liability, the burden would shift to a potential plaintiff to show that the breached data had not in fact been anonymized. The drafting team could discuss the merits of this approach in the context of data breach class actions.
    - ii. HIPAA guidance on deidentification calls for the removal of eighteen different data points from a data set. In conjunction with that, an independent statistician can evaluate the risk of personal identification from the remaining data. If this method of deidentification were used as a means of avoiding strict liability, the organization could avoid strict liability by having an independent statistical analysis done which demonstrates that the PII had been effectively deidentified. The drafting team could discuss the merits of this approach in the context of data breach class actions.
  - (d) *Limiting Deidentification Techniques*. The drafting team could suggest limits to the application of deidentification techniques for the purposes of avoiding strict liability. Methods worth discussing might include encryption that takes many years to break and redaction.

## IX. Enforcement

This confidential outline of The Sedona Conference Working Group 11 on Data Security and Privacy Liability is not for publication or distribution to anyone who is not a member of Working Group 11 without prior written permission. Comments and suggested edits to this document are welcome by email to [comments@sedonaconference.org](mailto:comments@sedonaconference.org) no later than November 29, 2021.

**(A)** The enforcement question contains at least two subparts.

1. First, should enforcement be delegated exclusively to government agencies – e.g., state attorneys general – or should there be private enforcement?
  - (a) Some data security laws contain a private right of action..
    - i. For example, the California Consumer Privacy Act (“CCPA”) permits private rights of action with statutory damages of between \$100 and \$750 “per consumer per incident or actual damages, whichever is greater.” Cal. Civ. Code § 1798.150(a)(1).
      - i. The private right of action applies to data breaches involving personal information that are the result of the organization’s negligence. *Id.*
      - ii. The 2020 California Privacy Rights Act (“CPRA”) expanded the CCPA’s private right of action to include email address in combination with a password or security question and answer that would permit access to the consumer’s account. See *id.*
    - (b) Similarly, under Illinois’ Biometric Information Privacy Act (“BIPA”), private plaintiffs 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 . . . .”
  2. Supporters of a private right of action applaud these statutes, arguing that a private right of action is necessary to ensure widespread compliance. [We recommend a literature review on this issue.]
  3. Opponents of a private right of action believe that the private right of action will create a flood of litigation and that enforcement is best left to law enforcement. [We recommend a literature review.]

**(B)** Second, how will the remedies be crafted in a strict liability enforcement regime?

- (a) Will all or some remedies be automatically triggered, or will plaintiffs be required to quantify and demonstrate the amount of harm?
  - i. BIPA does not require actual injury for private plaintiffs to recover. The Illinois Supreme Court has upheld this statutory

This confidential outline of The Sedona Conference Working Group 11 on Data Security and Privacy Liability is not for publication or distribution to anyone who is not a member of Working Group 11 without prior written permission. Comments and suggested edits to this document are welcome by email to [comments@sedonaconference.org](mailto:comments@sedonaconference.org) no later than November 29, 2021.

scheme. *Rosenbach v. Six Flags Ent. Corp.*, 2019 IL 123186, ¶ 1.

- ii. For a discussion on how to calculate the number of “incidents,” see The Sedona Conference Commentary on Quantifying Violations under U.S. Privacy Laws, July 2021.

- (b) Will the amount of monetary rewards/sanctions increase or decrease based on the culpability (i.e., negligence, recklessness, or intentional misconduct) of the organization that maintains the data?

- i. The CCPA (which is not a strict liability law) provides, “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.” Cal. Civ. Code § 1798.150(2).

## **X. STRICT LIABILITY COST BENEFIT ANALYSIS**

- (A) To find strict liability analogies in law the Brainstorming group looked to product liability. We noted two methods for evaluating liability; one being consumer expectations and the other being a risk-benefit test. Both methods allow for determinations of reasonableness, but the risk-benefit test was instructive for our effort.

- 1. In the case of the former, the Brainstorming group doubted that consumers’ expectations could be helpful.
  - (a) Data risks are often less obvious to consumers than traditional product risks.
    - i. Consumers who care little about their privacy are likely not aware of the ways that data aggregators, marketers, and hackers exploit data subjects’ information to their detriment.
  - (b) Data risks are often not controlled by information stewards, but by attackers who compromise data products and services.
    - i. Imagine the fundamental shift in product liability questions if children’s toys, house paint, and car tires were altered and weaponized by elite state actors to harm consumers.



This confidential outline of The Sedona Conference Working Group 11 on Data Security and Privacy Liability is not for publication or distribution to anyone who is not a member of Working Group 11 without prior written permission. Comments and suggested edits to this document are welcome by email to [comments@sedonaconference.org](mailto:comments@sedonaconference.org) no later than November 29, 2021.

2. The case of the latter, however, is resolvable using a recent Sedona Conference publication.
- (B) The Sedona Conference published a paper in February, 2021 titled, *Commentary on a Reasonable Security Test* that helps adjudicators determine the reasonableness of safeguards that reduce the risk of data breaches. The paper provides a test that includes three factors: harm to others, cost to an information steward, and the utility of the risk. If those factors are present, then a negligence regime may apply. If one of those factors is not present, then a strict liability regime may apply.
1. The test states, in brief, that a safeguard is reasonable if its added burden is not greater than its added benefit.
  2. The “harm to others” factor considers what the *ex-ante* foreseeable harm would have been at the time a safeguard was designed, implemented, and operated. This factor ensures that harm to the public or to plaintiffs is weighed as part of an organization’s due care analysis and planning.
  3. The “cost” factor considers burdens that safeguards impose on the information steward such as increased financial costs, reduced efficiency, lost opportunity, etc. This factor ensures that the increased burden of safeguards is weighed as part of an organization’s due care analysis and planning.
  4. The “utility” factor considers the reduced benefit of the risk if a safeguard were to be applied. This factor ensures that the reason for engaging in the risk in the first place – the benefit enjoyed by the public or plaintiff – is weighed as part of the organization’s due care analysis and planning.
- (C) The Brainstorming group considered that the utility factor provides a critical distinction between a negligence regime and a strict liability regime.
1. In the case where a harmed party enjoyed a benefit from a risk (the information steward used, stored, or transmitted their information to provide a benefit to the data subject), a negligence regime applies because the interests of both the information steward and the data owner (the data subject) are considered and are material to a balancing test. In this case the test implies that:
    - (a) A data subject may engage in risk when they understand the nature of the risk-benefit trade-off.
    - (b) An information steward may elect to forego safeguards (or seek alternative safeguards) whose risk-benefit trade-off is not worthwhile to potentially harmed parties.

This confidential outline of The Sedona Conference Working Group 11 on Data Security and Privacy Liability is not for publication or distribution to anyone who is not a member of Working Group 11 without prior written permission. Comments and suggested edits to this document are welcome by email to [comments@sedonaconference.org](mailto:comments@sedonaconference.org) no later than November 29, 2021.

2. However, in the case where a harmed party did not enjoy a benefit from the risk (the information steward used, stored, or transmitted their information without providing a benefit to the data subject), then only the interests of the information steward are considered. The utility would create no benefit to the harmed party, and applying the test would imply that:
  - (a) A data subject would gain no benefit from a risk, while ...
  - (b) An information steward benefitted from the data subject's risk.
3. In this second case, a strict liability regime could apply.
4. The *Commentary* addressed a critical and current public policy question: How would we know when safeguards that protect data subjects balance the interests of the data subjects and data stewards? A strict liability commentary that uses the utility factor to distinguish between reasonableness and strict liability regimes would assert that information stewards face increased scrutiny, responsibility, and risk when the public or consumers do not benefit from risks that the information steward exposes them to.

## **XI. CAN CONSENSUS BE REACHED ON A COMMENTARY ON THIS TOPIC?**

- (A) Given that this would require federal legislative action imposing a consistent standard across the U.S., the audience for any commentary would likely be legislators.
- (B) While regardless of the final recommendations, we would expect some members to be strongly opposed. That said, if this is part of a regime that standardizes data security and notice obligations nationwide and that includes input from all interested parties, it is possible that there is a potential path forward to reach consensus.