CYBERLAW CLINIC
HARVARD LAW SCHOOL | BERKMAN KLEIN CENTER FOR INTERNET & SOCIETY

MEMORANDUM

To: Representative Stephanie Jerome

From: Harvard Cyberlaw Clinic

Date: January 5, 2024

Re: Private Rights of Action for Data Privacy

1. OVERVIEW

The vast majority of states do not have any private right of action in their data privacy bills. There are two notable exceptions – Illinois's biometric privacy law and specific parts of California's comprehensive data privacy law. However, the lack of precedent should not deter the Vermont legislature from including a private right of action in its bill. There is robust reasoning to explain how a private right of action will not only increase enforcement of any privacy laws, but also provide a way for Vermonters to access justice.

This section compares provides background information about, justifications for, and recommendations regarding the inclusion of a private right of action in the Vermont comprehensive privacy bill.

2. PRIVATE RIGHTS OF ACTION IN PRIVACY STATUTES ACROSS STATES

2.1. California

The California Consumer Privacy Act (CCPA) provides for a private right of action, but only in the context of data breaches. The CCPA amended California data breach law to permit a private right of action for "unauthorized access and exfiltration, theft, or disclosure as a result of the business's violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information".[1] However, the legislature narrowed the definition of "personal information" for the purpose of data breach liability, limiting it to an individual's:

- Email address in combination with a password or security question and answer that would permit access to an online account; or[2]
- First name, or first initial, and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted or redacted:
    - SSN or other tax identification number;
    - driver's license number, California ID number, passport number, or military identification number;
    - any other unique identification number issued on a government document commonly used to verify the identity of a specific individual;

[1] Cal. Civ. Code § 1798.150(a)(1).
[2] Cal. Civ. Code § 1798.150 (a)(1).

- account number, credit or debit card number, in combination with the security code, password, or other information required to access the account;
- medical information (as defined in that section);
- health insurance information (as defined in that section);
- unique biometric data generated from measurements or technical analysis of human body characteristics used to authenticate a specific individual, such as a fingerprint, retina or iris image, or a physical or digital photograph, but only when used or stored for facial recognition purposes; or
- genetic data.[3]

In contrast to California's general data breach definition, the data breach right's definition does *not* cover the loss of a consumer's username plus password or other online account access information, unless the username is also the consumer's email address.[4]

The private right of action for data breaches under the CCPA allows a consumer to seek damages, injunctive or declaratory relief, or any other relief the court deems proper.[5] A consumer may seek either statutory damages between $100 to $750 per California resident and per incident, or actual damages, whichever is greater.[6]While the statutory damages may seem high, the CCPA does limit damages by giving businesses opportunity to respond or fix this issue before a consumer files a lawsuit. To qualify for statutory access damages, the consumer must identify specific violations and give the business 30 days to cure those violations. To cure, the business must provide the consumer with a written statement that it has cured the violation and no further violations will occur. If the business continues with its alleged violations, the consumer can file a lawsuit requesting statutory damages for the original violation as well as any new violation occurring after the notice, including breaching the written statement.

To avoid businesses from taking advantage of the right to cure, the CCPA expressly provides that implementing and maintaining reasonable security procedures and practices after a breach does not constitute a cure for that breach. Furthermore, the CCPA explicitly prohibits any agreement or contract

---

[3] Cal. Civ. Code § 1798.150 (a)(1) *referencing* Cal. Civ. Code § 1798.81.5 (d)(1)(A).
[4] *Understanding the California Consumer Privacy Act (CCPA) and the California Privacy Rights Act (CPRA)*, Westlaw Practical Law, https://us.practicallaw.thomsonreuters.com/w-017-4166.
[5] *Id.*
[6] *Id.*

provision that seeks to waive or limit a consumer's rights under the CCPA, including representative action waivers.[7]

2.2. Illinois

Illinois's Biometric Information Privacy Act (BIPA) differs from the previously discussed statutes and in content. It is one of three state privacy laws that focuses specifically on biometrics – the others being the Texas Capture or Use of Biometric Identifier Act (CUBI) and the Washington Biometric Law – but deserves focus here because it includes a private right of action. BIPA was passed unanimously in 2008, before the increased attention on data and biometric privacy that has permeated the past few years. Because of this, BIPA's inclusion of a private right of action was likely less noticed, and thus less opposed, by the business community than it would be today. BIPA came to prominence in political and legal culture in with a number of headline making cases that have occurred since 2019.[8]

In contrast to the limited private right of action provided for data breaches in California, BIPA specifically provides a private right of action as an enforcement mechanism for all violations. In pursuing a lawsuit related to one of these violations, the plaintiff may seek to recover "against a private entity that *negligently* violates a provision of this Act, liquidated damages of $1,000 or actual damages, whichever is greater; against a private entity that *intentionally or recklessly* violates a provision of this Act, liquidated damages of $5,000 or actual damages, whichever is greater; reasonable attorneys' fees and costs, including expert witness fees and other litigation expenses; and other relief, including an injunction, as the State or federal court may deem appropriate."[9] Similarly to the recommendation we provide, BIPA accounts for differences in intent in determining damages.The breadth of litigation that has resulted from BIPA, and the size of damages that can result, distinguishes BIPA from other laws that have passed in this space as well.[10]

---

[7] *Id.*

[8] *Is Biometric Information Protected by Privacy Laws?*, Bloomberg Law (May 3, 2023), https://pro.bloomberglaw.com/brief/biometric-data-privacy-laws/.

[9] 740 Ill. Comp. Stat. Ann. 14/20.

[10] From 2008-2016 only 15 BIPA lawsuits were filed in Illinois. *Biometric Privacy Class Actions By The Numbers: Analyzing Illinois' Hottest Class Action Trend*, Seyfarth Shaw LLP (June 28, 2019), https://www.workplaceclassaction.com/2019/06/biometric-privacy-class-actions-by-the-numbers-analyzing-illinois-hottest-class-action-trend/. However, since 2016 litigation numbers have increased exponentially with approximately 1500 BIPA suits being filed in the last five years. James Hickey & Colin Willmott, *The Rising Specter of BIPA Claims in Illinois*, Kennedys (Aug. 24, 2023), https://kennedyslaw.com/en/thought-leadership/article/2023/the-rising-specter-of-bipa-claims-in-illinois/.

2.3. States Without a Private Right of Action

As noted above, most states with comprehensive privacy laws do not have private rights of actions. A few notable states – Colorado, Virginia, and Connecticut – that have varying statutory schemes are highlighted below.

2.3.1. Colorado[11]

Under the Colorado Privacy Act (CPA) the Colorado Attorney General has enforcement and regulatory authority.[12] Similar to Vermont's previous draft legislation, the CPA specifically disclaims a private right of action.[13] Moreover, while the CPA provides that violations constitute an unfair trade practice under state consumer protection law, which generally allows for private enforcement,[14] the private right of action is not available for these types of violations.[15] The potential civil penalty maximum for unfair trade practice violations is $20,000 per violation, increased to $50,000 for violations committed against an elderly person.[16]

2.3.2. Virginia[17]

The Virginia Consumer Data Protection Act (VCDPA), similar to Vermont's previous draft legislation, specifically does not provide a basis for a private right of action.[18] The Virginia Attorney General has enforcement authority under the VCDPA.[19] VCDPA violations may result in potential civil penalties of up to $7,500 per violation and reasonable expenses, including attorneys' fees.[20]

2.3.3. Connecticut[21]

The Connecticut Personal Data Privacy and Online Monitoring Act (CTDPA), similar to Vermont's previous draft legislation, specifically does not provide a

---

[11] For more detail, see *Colorado Privacy Act (CPA) Quick Facts: Overview*, Westlaw Practical Law, https://us.practicallaw.thomsonreuters.com/w-036-4960.
[12] Colo. Rev. Stat. Ann. § 6-1-1311.
[13] Colo. Rev. Stat. Ann. §§ 6-1-1310(1) and 6-1-1311(1)(b).
[14] Colo. Rev. Stat. Ann. § 6-1-113.
[15] Colo. Rev. Stat. Ann. § 6-1-1311(1)(c)).
[16] Colo. Rev. Stat. Ann. §§ 6-1-112(1)(a), (c).
[17] For more detail, see *Virginia Consumer Data Protection Act (VCDPA) Quick Facts: Overview*, Westlaw Practical Law, https://us.practicallaw.thomsonreuters.com/w-038-3134.
[18] Va. Code Ann. § 59.1-584(E).
[19] Va. Code Ann. § 59.1-584(A).
[20] Va. Code Ann. § 59.1-584(C), (D).
[21] For more detail, see *Connecticut Personal Data Privacy and Online Monitoring Act (CTDPA) Quick Facts: Overview*, Westlaw Practical Law, https://us.practicallaw.thomsonreuters.com/w-038-3118.

basis for a private right of action.[22] Connecticut's law goes even further to say that any violations of this law also cannot utilize the Unfair Trade Practices Act's[23] private right of action.[24] Initial violations may result in an injunction, an order directing restitution, or both, along with reasonable attorneys' fees.[25] Aligning with our recommendation for Vermont that penalty increases by accounting for intent and the type of data, Connecticut provides that willful initial violations can also result in a civil penalty of up to $5,000 per violation.[26]

3. POLICY RATIONALE FOR A PRIVATE RIGHT OF ACTION

Most states do not include a private right of action in their data privacy laws. This can largely be attributed to hesitation and pushback from the business community,[27] even as organizations like the Chamber of Commerce and large companies have come to recognize that data privacy legislation is important.[28] However, the conversation has begun to shift with policy makers and business leaders previously opposed to a private right of action starting to see its' use.[29] At a Senate Commerce Committee hearing in 2021 Sen. Roger Wicker (R-MS), the main sponsor of the leading Republican bill, disclosed in his opening statement that he "'proposed incorporating a narrow private of action' in bipartisan negotiations that took place in 2019, and said, 'I remain open to the idea' . . . He used most of his question time to elicit witnesses' views on the legitimate scope of a private right of action, directly asking 'what would you

---

[22] Conn. Gen. Stat. Ann. § 42-525(d), (e).
[23] Conn. Gen. Stat. Ann. ¬ß 42-110g.
[24] Conn. Gen. Stat. Ann. § 42-525(d), (e).
[25] Conn. Gen. Stat. Ann. §§ 42-110d(d), (e) and 42-110m(a).
[26] Conn. Gen. Stat. Ann. § 42-110m(b).
[27] As the non-profit EPIC explained to the Maine legislature, "I want to flag for the Committee that you should be skeptical of industry lobbyists urging you to mimic current state privacy laws, particularly the Virginia model. Virginia's 'privacy' law was drafted by and passed with the support of Amazon, Microsoft, and industry trade groups, with little to no involvement of consumer and privacy advocates. Reuters found that '[i]n recent years, Amazon.com Inc has killed or undermined privacy protections in more than three dozen bills across 25 states, as the e-commerce giant amassed a lucrative trove of personal data on millions of American consumers.' They did this not only by opposing strong privacy bills, but by pushing weak ones." *EPIC Testimony to the Maine Legislature Judiciary Committee regarding An Act to Create the Data Privacy and Protection Act*, EPIC (Oct. 16, 2023), https://epic.org/documents/epic-testimony-to-the-maine-legislature-judiciary-committee-regarding-an-act-to-create-the-data-privacy-and-protection-act/.
[28] *U.S. Chamber Warns It Will Oppose Any Privacy Legislation That Creates a Blanket Private Right of Action*, U.S. Chamber of Commerce (May 31, 2022), https://www.uschamber.com/technology/data-privacy/u-s-chamber-warns-it-will-oppose-any-privacy-legislation-that-creates-a-blanket-private-right-of-action.
[29] Cameron F. Kerry, *Senate Hearing Opens the Door to Individual Lawsuits in Privacy Legislation*, Brookings (Oct. 8, 2012), https://www.brookings.edu/articles/senate-hearing-opens-the-door-to-individual-lawsuits-in-privacy-legislation/.

allow [or] not allow.'"[30] Beyond the changing opinions and recognition of the importance of a private right of action from some lawmakers, recent scholarship and advocacy from privacy experts has detailed the reasons that a private right of action is essential for a functioning and effective data privacy law:

3.1. A private right of action would prevent enforcement agencies from being overwhelmed.

Given the limited size and capacity of the Vermont Attorney General's office, providing a private right of action will lessen the burden of enforcement on the government. This will allow the office to focus on the most egregious violations of the law and still have the capacity to be able to fulfill the rest of their duties. As EPIC stated in their testimony to the Maine Legislature Judiciary Committee,

> The scope of data collection online is simply too vast for one entity to regulate. Individuals and groups of individuals who use these online services are in a good position to identify privacy issues and bring actions to vindicate their interests. These cases preserve the state's resources, and statutory damages ensure that companies will face real consequences if they violate the law.[31]

Additionally, law professor Lauren Scholz stated in her article "Private Rights of Action in Privacy Law",

> The modern American administrative state is not capable of addressing an issue of information privacy's magnitude without support from private enforcement. . . . Private enforcement deters potential wrongdoers by allowing for a resilient avenue of enforcement, available even when agency funding or political will is lacking. . . . Matters brought to light by private enforcers, even if they are unsuccessful in their efforts, can aid public enforcers in their regulatory choices.[32]

Further, including a private right of action as part of a hybrid enforcement scheme also helps shape the law to the benefit of enforcers as technology shifts rapidly.

---

[30] *Id*.
[31] EPIC, supra note 27.
[32] Lauren Scholz, *Private Rights of Action in Privacy Law,* 63 WM. & MARY L. REV. 1639, 1645-47 (2022).

> A handful of plaintiffs and cases, then, provide the essential public good of creating case law that helps us understand how the law applies to changing circumstances . . . . Private enforcement brings interactions in the private sphere to the surface for evaluation by public actors. Without private enforcement, there is simply too much that is beyond the access and capability of the state's grasp.[33]

3.2. A private right of action would increase the effectiveness of the law.

Other areas in which a combination of public and private enforcement has succeeded include employment, civil rights, and consumer protection. By including a private right of action in legislation, the state bolsters enforcement potential leading to increased compliance. Compliance is already an issue with data privacy laws as companies see the lack of enforcement being brought by agencies and determine that they'd rather risk enforcement action than pay the cost of compliance.[34] In EPIC's Maine testimony this year they discussed how,

> Addressing modern privacy problems requires productive redundancy—that is, providing legal avenues for both government and private parties to observe and challenge privacy-invasive practices.[35]

Without a private right of action, Vermont's privacy bill will fail to be sufficiently effective. Without proper enforcement, companies are not incentivized to comply with the law in place. In writing about BIPA and its use of a private right of action, Professor Woodrow Hartzog said,

---

[33] *Id.* at 1657-59.

[34] *See* Mona Naomi Lintvedt, *Putting a Price on Data Protection Infringement*, 12 INT'L DATA PRIV. L. 1 (2022), available at https://ssrn.com/abstract=4283877 (discussing how unequal enforcement by European countries in regards to GDPR fines "can diminish the preventive and deterrent effect of the fines. The enforcement mechanisms will be of less value if applied differently by the DPAs and may eventually distort competition and lead to forum shopping"). This mirrors the argument around the inclusion of a private right of action in showing that business compliance requires real threat of enforcement and a public view that any business not in compliance could be held accountable, not just those government see as flashy or big cases. The author also discusses how the compensation of those harmed by bad data practices – not just fines that go to the state – would assist in enforcement as the public would see real benefit from their privacy rights being enforced. See, e.g., *GDPR Compliance Rate Remains Low According to New Talend Research*, talend (Dec. 3, 2019), https://www.talend.com/about-us/press-releases/gdpr-compliance-rate-remains-low-according-to-new-talend-research/ (one year after implementation of GDPR, 58% of surveyed businesses worldwide failed to address requests for personal data within one-month time limit).

[35] EPIC, supra note 27.

> So far, only private causes of action seem capable of meaningfully deterring companies from engaging in practices with biometrics based on business models that inevitably lead to unacceptable abuses. Regulators are more predictable than plaintiffs and are vulnerable to political pressure. Facebook's share price actually rose 2 percent after the FTC announced its historic $5 billion fine for the social media company's privacy lapses in the Cambridge Analytica debacle. Meanwhile, Clearview AI specifically cited BIPA as the reason it is no longer pursuing non-government contracts. On top of that, Clearview AI is being sued by the ACLU for violating BIPA by creating faceprints of people without their consent. [...] In general, businesses have opposed private causes of action more than other proposed privacy rules, short of an outright ban.[36]

Discussing the Telephone Consumer Protection Act, the Fair Credit Reporting Act, and the Driver Privacy Protection Act, Lauren Scholz stated that, "hybrid enforcement regimes already exist in privacy law, and they have proven more effective than regimes that only use public enforcement."[37] As a matter of practicality "the reality is public enforcers cannot address every instance of wrongful" behavior and "thus, private actors provide the primary incentive for companies to comply and agencies to continue to enforce these laws in every interaction with every consumer."[38]

3.3. A private right of action gives opportunity for consumers to be made whole.

The individual tenacity and privacy values that are inherent for Vermonters in general align with the need for a private right of action. A private right of action gives consumers the opportunity to seek justice and to receive financial compensation. By empowering Vermonters to take certain levels of enforcement into their own hands, the Vermont Legislature will be furthering these values. The states with statutes that provide only for regulator enforcement and penalties can impose large fines, but that money does not end up back in the pockets of the consumers that were actually harmed by data breaches or improper data management.[39]

---

[36] Woodrow Hartzog, *BIPA: The Most Important Biometric Privacy Law in the US?*, in REGULATING BIOMETRICS: GLOBAL APPROACHES AND URGENT QUESTIONS 96 (Amba Kak ed., 2020), available at https://scholarship.law.bu.edu/faculty_scholarship/3086.
[37] Scholz, supra note 32, at 1655.
[38] *Id.* at 1657.
[39] Amy Kelley, *'Paper Tiger' State Privacy Laws Worse Than Having No Law at All, Bloomberg Law* (Oct. 12, 2023), https://news.bloomberglaw.com/privacy-and-data-security/paper-tiger-

As Scholz said in her article,

> Private rights of action have expressive value that cannot be achieved through public regulation in the area of privacy. The nature of the right implies that an individual opportunity to be heard should be available. Privacy is a personal, dignitary right, so there should be some avenue for an individual to personally contest privacy violations. The ability to bring a claim is itself a recognition of the dignity of the plaintiff.[40]

Overall, this discussion and argument surrounding a private right of action has been going on since the federal government began passing limited federal privacy laws such as the Fair Credit Reporting Act, Gramm-Leach-Bliley Act, and Health Insurance Portability and Accountability Act. As professor and scholar Elizabeth D. De Armond stated in 2008, assessing how federal privacy laws fail to offer real remedies, "[w]ithout private remedies, the federal acts lose all the benefits of the private attorney general, the deterrence and standard-defining effects that arise from litigation brought by those who are harmed by the violations. In the case of privacy, that means that we are losing an opportunity to help further define the types of behaviors that breach the norms Congress intended to govern."[41]

While some may be concerned that a private right of action may hurt Vermont businesses, this can be avoided through applying our overall framework – increasing penalties from the law in accordance with the severity of the harm and intent – to a private right of action as well. For more discussion on this see the following section.

4. RECOMMENDATIONS FOR VERMONT

The version of Vermont's data privacy legislation introduced in 2023 specifically called out that it did *not* provide for a private right of action. Version 4.1 draft of Vermont H.121, the version circulated on June 20, 2023, included the following language in § 2425:

> (d) This chapter shall not be construed as providing the basis for, or be subject to, a
> private right of action for violations of this chapter or any other law.

---

state-privacy-laws-worse-than-having-no-law-at-all ("And for statutes that only allow for penalties, none of that money ends up in consumers' pockets to help them deal with fraud or identity theft—which is quite shocking, considering that consumers reported losing $9 billion to fraud and identity theft scams in 2022.").

[40] Scholz, supra note 32, at 1654.

[41] Elizabeth D. De Armond, *A Dearth of Remedies*, 113 PENN ST. L. REV. 1, 34 (2008).

(e) A violation of the requirements of this chapter shall constitute an unfair and

deceptive act in commerce in violation of section 2453 and shall be enforced solely by

the Attorney General, provided that a consumer private right of action under subsection

2461(b) of this title shall not apply to the violation.

We recommend against this for a number of reasons further explained in following section. Given the Vermont Legislature's interest in protecting consumer privacy in an enforceable, comprehensive way that also protects small businesses that act in good faith, we recommend that the legislature include an express private right of action in the new bill. By creating a private right of action for privacy violations, Vermont has the opportunity to lead the country in an effective, enforceable privacy law.

In keeping with our recommendations for the bill as a whole, the availability and penalty associated with a private right of action should be closely coordinate with the severity of the harm. A private right of action is not an all-or-nothing proposition. As evidenced by the CCPA, a private right of action might apply to only some parts of a comprehensive privacy law. Moreover, within a private right of action there are several statutory design choices that need to be made, including "(1) who has standing to sue; (2) which parties bear the costs of litigation; (3) what relief is available to winning plaintiffs; and (4) what are the rules of liability and burden of proof to win."[42]

4.1. Availability of the Right

One threshold decision to be made is what elements of the law will allow for a private right of action. Establishing a private right of action for any violation of the privacy law would provide maximal enforcement, but would also create the highest burden on regulated business and the court system. If a limited private right of action seems more practical—or politically feasible—we recommend that the legislature focus on a private right of action for two scenarios: (1) violations that involve sensitive data, such as biometrics and children's information; and (2) violations that involve the sale of individuals' personal data. This would prioritize areas where non-enforcement is most harmful, while limiting the potential for burdensome, frivolous lawsuits. Moreover, under the tiered system proposed in Section 1, businesses operating

[42] Joseph Jerome, *Private Right of Action Shouldn't Be a Yes-No Proposition in Federal US Privacy Legislation*, IAPP (Oct. 3, 2019), https://iapp.org/news/a/private-right-of-action-shouldnt-be-a-yes-no-proposition-in-federal-privacy-legislation/.

in these areas should already be taking heightened precautions with consumer data and therefore should be on notice that their data practices are subject to scrutiny.

4.2. Court Interpretations

Looking at court interpretations of BIPA also can provide guidance here. To the extent that the legislature does not expressly decide these issues, interpretation will be left to the judicial system. The history of interpretation of Illinois' BIPA – the oldest state privacy law with a private right of action – provides guidance on the role of courts in shaping a private right of action.

Three US Circuits have addressed standing issues with BIPA – the Second, Seventh, and Ninth. Each of these has had a slightly different interpretation on whether a statutory violation alone under BIPA is sufficient for the plaintiffs to have standing. The Seventh Circuit, which has seen the most of these cases given Illinois' location in that circuit, has said:

1. a vendor's collection of biometric data without consent **was** a sufficient injury-in-fact under BIPA Section 15(b);[43]
2. A vendor's failure "to publicly disclose its biometric retention and destruction guidelines before collecting" biometric data **was not** a sufficient injury-in-fact under BIPA Section 15(a);[44]
3. An employer's failure to disclose retention and destruction guidelines surrounding data it collects from its employees **was** a sufficient injury-in-fact under BIPA Section 15(a);[45]
4. A company's failure to obtain consent before disclosing or disseminating biometric information in violation of BIPA Section 15(d) **was** sufficient injury-in-fact;[46]
5. And, a class of individuals who suffered no injury but whose data was sold in violation of BIPA Section 15(c) **did not** have Article III standing.[47]

The Ninth Circuit stated generally that individuals' concrete privacy interests are protected under BIPA and violations of BIPA procedures "actually harm or pose a material risk of harm to those privacy interests."[48] Finally, in 2017 the Second Circuit determined that even though technical violations of BIPA

---

[43] *Bryant v. Compass Grp. USA, Inc.*, 958 F.3d 617, 624 (7th Cir. 2020), *as amended on denial of reh'g and reh'g en banc* June 30, 2020.
[44] *Id.*
[45] *Fox v. Dakkota Integrated Sys., LLC*, 980 F.3d 1146 (7th Cir. 2020).
[46] *Cothron v. White Castle Sys., Inc.*, 20 F. 4th 1156, 1161 (7th Cir. 2021).
[47] *Thornley v. Clearview AI, Inc.*, 984 F.3d 1241, 1246 (7th Cir. 2021).
[48] *Patel v. Facebook, Inc.*, 932 F.3d 1264, 1275 (9th Cir. 2019).

existed, there was no demonstrated actual injury. However, this decision is nonprecedential as it was remanded to be dismissed for lack of jurisdiction.[49] Given this interpretation, however, the Vermont legislature should be cautious on relying too heavily on a private right of action to do the work when there is no financial or personal injury apparent outside of the statutory violation. The legislature should also be sure to include in legislation notes, or the text itself, information on how it views privacy violations as harms unto themselves to encourage the courts to view privacy harms as tangible harms.

Similar to the Article III standing interpretation was the statutory interpretation issue of the word "aggrieved". Under BIPA, any person "aggrieved" by a violation has "a right of action . . . against an offending party."[50] However, in contrast to the differing interpretations on standing, the Illinois Supreme Court has held that, under Illinois *state* law, BIPA does not require individuals to suffer an actual injury beyond a statutory violation to sustain a private action as an aggrieved person. Under principles of statutory construction" a person need not have sustained actual damage beyond violation of his or her rights under the Act in order to bring an action under it."[51]

4.3. Procedural Requirements

The legislature will also need to decide whether to require any specific action from consumers before a lawsuit may be filed. For example, under the CCPA, a consumer must provide a 30-day notice and right to cure prior to initiating any action against a business for statutory damages.[52] If the business confirms in writing that the violation is cured and no further violations will occur, the consumer may not obtain statutory damages. If the business fails to follow up or they continue to violate the law, statutory damages are available. Vermont may want to consider including a requirement of this sort, at least in situations where the harm can be effectively cured. This gives consumers the ability to protect their privacy while also giving businesses an opportunity to fix their practices without the cost of litigation.

4.4. Cross-Border Scope

Another area of interpretation of BIPA that is relevant to Vermont's drafting is that of extraterritorial jurisdiction. BIPA's language does not address the law's reach, but in a law governing technology that inherently spans locations, it is an important question. "Plaintiffs may assert BIPA claims for conduct

[49] *Santana v. Take-Two Interactive Software, Inc.*, 717 F. App'x 12 (2d Cir. 2017).
[50] 740 ILCS (14/20).
[51] *Rosenbach v. Six Flags Ent. Corp.*, 129 N.E.3d 1197, 1205 (Ill. 2019).
[52] Cal. Civ. Code § 1798.150.

occurring outside of Illinois if they sufficiently allege specific facts that the purported violations occurred primarily and substantially in Illinois by demonstrating, for example, whether the plaintiff resides in Illinois, the defendant took action directed at the plaintiff in Illinois, the defendant's conduct harmed the plaintiff in Illinois, and the plaintiff communicated with the defendant in Illinois.[53] "If a defendant's conduct occurs online or in a cloud-based system, a court can also consider whether the defendant, if a business, is incorporated in or registered to do business in Illinois [or] the defendant targets online or cloud-based services or products at Illinois."[54] Courts have taken these rules and restrictions to mean that they must assess whether a defendant's violation occurred "primarily and substantially" within Illinois before allowing litigation to proceed.[55]

4.5. Damages

Once the legislature decides when and how a private right of action is available, it must decide what damages can be obtained. One common way to approach this is with a damages multiplier for bad faith or unlawful intent. BIPA, as an example provides for $5,000 in damages for knowing or reckless violations or $1,000 in damages for negligent violation of the statute.[56] Similarly, the current Vermont Consumer Protection laws provide "exemplary" damages: if the action of the defendant is shown to be in bad faith the court can award up to three times the actual value in damages to deter future wrongdoing.[57]

Another factor the legislature can take into account is the severity of the harm. This, combined with an intent framework, would provide differentiation between levels of harm. For example, the legislature could impose a damages multiplier if non-statutory (such as financial or reputational) harm occurred. Alternatively, the legislature can allow increased damages for violations involving data brokers – whose whole business is personal data – or businesses working with biometric or other sensitive data.

There are other ways the legislature can expand or limit damages, and thus incentives to sue, for a private right of action. For example, the legislature will have to determine whether the damages are for each violation or whether they

---

[53] *BIPA Compliance and Litigation Overview*, Westlaw Practical Law, https://us.practicallaw.thomsonreuters.com/w-026-4764.
[54] *Id.*
[55] *See, e.g.*, *In re Clearview AI, Inc., Consumer Priv. Litig.*, 585 F. Supp. 3d 1111, 1121-22 (N.D. Ill. 2022), *clarified on denial of reconsideration*, No. 21-CV-0135, 2022 WL 2915627 (N.D. Ill. July 25, 2022).
[56] 740 Ill. Comp. Stat. Ann. 14/20.
[57] 9 V.S.A. § 2461.

are cumulative. It will also have to decide whether to impose a fee-shifting, a decision that could significantly affect the desirability of litigation for small harms.

4.6. Incorporation of Consumer Protection Standards

The final decision point is whether a private right of action should exist in standalone form within the data privacy legislation, or whether the legislature should imply a private right of action through referring to the general Vermont consumer protection laws. This idea has been brought up in a number of conversations during the fall of 2023.

As previously noted, the Vermont Consumer Protection laws provide for a private right of action for "any consumer who contracts for goods or services in reliance upon false or fraudulent representations or practices prohibited by section 2453."[58] Section 2453 states that "unfair methods of competition in commerce and unfair or deceptive acts or practices in commerce" are unlawful and directs the courts to interpret the law "guided by the construction of similar terms contained in Section 5(a)(1) of the Federal Trade Commission Act as from time to time amended by the Federal Trade Commission and the courts of the United States."[59] While the legislature does have the option to simply refer to a violation of the data privacy act as a violation of section 2453, there may be issues with court interpretation that result in a less than fully effective private right of action.

The courts have repeatedly shown that they do not view privacy violations as harms of their own. As scholars Danielle Citron and Daniel Solove have stated, "courts . . . have wrought havoc on legislative plans for statutory damages in privacy cases by adding onerous harm requirements."[60] Courts "sometimes resist recognition of an unfamiliar harm in the absence of a concrete test or an obvious perpetrator".[61] Without specific guidance, the legislature runs the risk that courts will view the "unfamiliar" harm and the addition of a private right of action as an unclear mandate from the legislature and not give it the weight it is due.

Beyond the above points demonstrating skepticism in the court system around privacy violations as a harm, there is value in the legislature itself

[58] 9 V.S.A. § 2461(b).
[59] 9 V.S.A. § 2453(a) and (b).
[60] Danielle Keats Citron & Daniel J. Solove, *Privacy Harms,* 102 B.U. L. Rev. 793, 798 (2022).
[61] Ryan Calo, *The Boundaries of Privacy Harm*, 86 INDIANA L. J. 1131, 1134 (2011).

determining spelling out the availability of a private right of action. As scholar Eugene Volokh says,

> The very fact that legislatures can draw arbitrary lines, based on their sense of public attitudes, rather than purporting to make decisions based on principle, makes them familiar and legitimate places for weighing incommensurables such as safety and privacy. That is indeed a big part of a legislator's job: drawing lines based on the felt moral and practical attitudes of the majority. . . . [While] decisions in favor of liability can be revised by legislatures, just as decisions against liability can be. . . [S]uch an approach, though, seems likely to be inapt when it comes to privacy.[62]

The legislature is far better situated to make this determination than courts. By not being as clear as possible in the provision of a private right of action, the legislature risks undermining their own decisions and leaving it to judicial discretion to interpret "legislative intent."

[62] Eugene Volokh, *Tort Law vs. Privacy,* 114 COLUM. L. REV. 879, 944-47 (2014).