THOMAS J. DONOVAN, JR.
ATTORNEY GENERAL

JOSHUA R. DIAMOND
DEPUTY ATTORNEY GENERAL

SARAH E.B. LONDON
CHIEF ASST. ATTORNEY GENERAL

TEL: (802) 828-3171

http://www.ago.vermont.gov

STATE OF VERMONT
OFFICE OF THE ATTORNEY GENERAL
109 STATE STREET
MONTPELIER, VT
05609-1001

TO: **Sen. Michael Sirotkin, Chair**
Senate Committee on Economic Development, Housing, and General Affairs

Rep. Michael Marcotte, Chair
House Committee on Commerce and Economic Development

FROM: **Charity R. Clark, Chief of Staff**
Office of the Attorney General

Ryan Kriger, Assistant Attorney General
Office of the Attorney General

DATE: **January 4, 2022**

RE: **Recommendations for privacy legislation, 2022 legislative session**

INTRODUCTION

In February 2020, Chair Marcotte requested that the Attorney General's Office (AGO) convene a meeting of stakeholders to discuss the AGO's proposal that Vermont codify a Biometric Information Privacy Act (BIPA). In March 2020, after hosting this meeting, the AGO proposed that it convene a series of privacy forums to receive input from stakeholders and foster discussion of issues surrounding privacy in Vermont. Specific issues articulated included:

1. Appropriate protections on biometric data, including facial recognition;
2. Whether Vermont should adopt all or parts of the California Consumer Privacy Act (CCPA); and
3. Consumer protections that better address the privacy concerns of Vermonters.

Delayed due to the pandemic, these forums were held this fall on October 5, 2021 (Burlington and remote via Microsoft Teams), October 26, 2021 (Montpelier and remote via Microsoft Teams), and November 18, 2021 (White River Junction and remote via Microsoft Teams). These hearings were well attended, largely by consumer and industry advocates, who shared their thoughts on potential privacy legislation. Written comments by stakeholders are attached to this report, and videos of the three forums can be found at the AGO's You Tube channel.

The AGO proposes a set of privacy protections each of which seeks to protect Vermonters while respecting the need for businesses to innovate and prosper, and which work together to provide a comprehensive privacy regime. These recommendations look to protections that have been proposed or enacted around the country and apply what we have learned through our deep experience in this field.

GENERAL PRINCIPLES

Our recommendations are grounded in a few basic principles.

The first principle is **data minimization**. That is, businesses should collect only the data they require to carry out business transactions with customers, and no more. Data minimization could reduce the need for complex regulations about opting out of the sale or sharing of consumer data. Data minimization can also help businesses avoid disastrous data breaches by limiting the data they stand to lose in such a breach.

The second principle is **limits on secondary uses of data**. Once a business collects data, it might share that data with others. Currently there is no legal requirement that a business that acquires data use it for the purpose for which it was acquired. This would be a critical and much needed guardrail for the data ecosystem.

These two protections would provide much-needed correctives to much of the data ecosystem, but they don't cover one critical set of actors – **data brokers**. Data brokers do not collect data directly from consumers, so data minimization policies won't reach them. They gather and aggregate data from a number of sources, including public sources, so limits on secondary uses of data may not affect them. Fortunately, Vermont is on the forefront of data broker regulation, and there are simple, commonsense adjustments to our Data Broker Law that can address gaps in these protections.

Finally, there are certain categories of information which, even under requirements of data minimization and restrictions on secondary uses, still require additional protections. The most prominent of these is **biometric information**, as we address below.

Separate from the question of what protections should be implemented is the question of how those protections should be enforced. A strong law with weak enforcement mechanisms will not protect Vermonters.

PROPOSED LEGISLATION

Comprehensive Privacy Protections

Our proposal is informed by the following observations concerning the state of privacy today:

- many businesses collect more data than they need to complete a given transaction;
- businesses often retain their data after it has outlived its use;
- many businesses underinvest in data security;
- consumers often have little choice as to how much data they must give up because they either don't know their data is being collected, the privacy policies are so voluminous and incomprehensible that even a close reading does not provide clear answers, or there is no real choice for consumers among competing products that have similar privacy policies;
- consumers are used to comparing products and services based on price, but often the price they pay is both in money *and* data; the consumer may be unaware of the value of their data, whether they are providing data or what types of data they are providing; thus, consumers are unable to make informed decisions and compare products and services;
- absent regulation, businesses that collect and monetize data without the consumer knowing about it and that also underinvest in data security will enjoy financial savings and competitive advantage over businesses that offer the same product, but do provide privacy protections and do invest in data security;
- data can be shared with third parties that do not respect the purposes for which the data was initially collected, and may then be further shared or collected by data brokers; in other words, there are no protections for data once it has entered the "data marketplace;"
- businesses that share data may promise and intend to aggregate, de-identify, or anonymize the data, but fail to do so effectively or try to do so but underestimate how easily a sophisticated entity can re-identify data, thus failing to provide a critical privacy protection without consequences;
- data that is collected from consumer purchases, online behavior, service applications, phone and internet service providers, and numerous other sources can be combined with so-called "public information," including government records which were never intended to be compiled into massive dossiers, or online activities like public social media postings, which consumers are unaware

is being collected for secondary uses that may be contrary to their wishes or best interests;[1]

- against the background of all this data collection and sale, the onus is usually placed on the consumer to take extensive measures to opt out of the collection and sale of their data, rather than on the businesses that are profiting from the collection; and
- as a result of this state of affairs, privacy-minded consumers may choose to forego the benefits of beneficial technologies, such as contact-tracing apps or health monitoring apps, because they are distrustful that their privacy will be respected and may believe that there are unlikely to be legal consequences if their privacy is violated.

Many of the "comprehensive" privacy laws being proposed in other states provide additional rights to consumers, such as to know how their data is collected, to opt out of the sale of data, or to request that their data be deleted; but these laws often do not require the businesses themselves to proactively respect consumers' privacy.

We recommend a set of data controls that place the onus of privacy protection upon entities that collect, distribute, and profit from consumer data. These controls should apply to each part of the data ecosystem: the entities that collect consumers' data, the third parties that may acquire that data from the data collectors, and the data brokers that trade in data that may not have an easily discernable connection to a consent or notice.

Such controls should include the following:

1. Data minimization. Prohibit businesses from collecting more information than necessary to fulfill a given transaction, or from retaining information longer than necessary. The California Consumer Privacy Act (CCPA) has already introduced one such version of such controls.
2. Limits on secondary uses of data. Require third parties that acquire data to comply with the original consent and notice for which the data was collected. This should be an independent legal duty applied to third parties, not one that derives from their duties to the data collectors.
3. "Do Not Track" designation. Enable consumers to opt out of online tracking and Data Broker sharing of data through a centralized mechanism and by requiring businesses to respect Do Not Track signals.

[1] Many privacy laws contain exemptions for "public information," which, depending on the interpretation of this phrase, can significantly weaken their intent. This complex issue requires further study before any recommendation can be made.

4. Expand the Data Broker Law. Establish additional protections for consumers regarding data held by Data Brokers (covered in more detail below); and
5. Guardian consent, right to control sale of data, right to be forgotten, and additional disclosures. The California Consumer Privacy Act (CCPA) includes several worthwhile improvements to policies around data, such as:
    1. Businesses must obtain parental or guardian consent for minors for data sharing purposes.
    2. "Do Not Sell My Personal Information" link on the home page of the website of the business, that will direct users to a web page enabling them, or someone they authorize, to opt out of the sale of the consumer's personal information.
    3. Consumers have a limited right to require businesses to delete their personal information.
    4. Business must designate methods for submitting data-access requests.
    5. Consumers have a right to request the personal information collected and third parties with which it is shared.
    6. Businesses must disclose:
        a. The personal information categories collected;
        b. The intended use/purposes for each category;
        c. Further notice is required to:
            i. Collect additional personal information categories;
            ii. Use collected personal information for unrelated purposes.

Biometric Privacy Protections

Biometric identifiers are data derived from our physical characteristics in order to uniquely identify us. These identifiers are derived from our faces, fingerprints, voices, retinas, or even our walking gait or the way we type.

Biometric identifiers raise a number of privacy issues. We know that many people object to being tracked online – biometric identifiers allow us to be easily tracked and surveilled in the real world. They have the potential to eliminate the anonymity that we take for granted as we move through our daily routine. Furthermore, information about our health or other physical characteristics can potentially be derived from biometric identifiers. Once our biometrics have been captured, we have little recourse – it is a major undertaking, or impossible, to alter our physical beings. Nor should we have to.

These issues have recently come to the fore in the Attorney General's lawsuit against Clearview AI, a business that has collected billions of online photographs in order to market a facial recognition app which allows us to be easily identified by strangers wherever we go.

The first Biometric Information Protection Act (BIPA) was introduced in Illinois in 2008. This law has drawn criticism from industry stakeholders due to its failure to address situations involving security and fraud prevention, and because of its private right of action, which contains statutory penalties of $1,000 for negligent violations and $5,000

for intentional or reckless violations. Numerous stakeholders suggested we look to the Washington State BIPA instead. We recommend looking to the best parts of the Washington and Illinois BIPA laws, both of which have acknowledged shortcomings.

Importantly, we must recognize that biometrics are primarily used for two distinct purposes: authentication and identification. Authentication requires a 1-to-1 comparison of two biometric identifiers to confirm that an individual is who they claim to be, and is necessary for fraud prevention, user credentialing, and security.

Identification requires a 1-to-many comparison wherein a biometric identifier is searched against a set of other identifiers, and is used for surveillance, marketing, and other purposes. A major concern regarding collection of biometrics is that an individual may be included in one of these data sets without their consent. Government-controlled data sets such as mugshots or DMV photos can be overseen by policymakers, while private data sets are often opaque to the public and regulators and subject to limited or zero oversight. Furthermore, as Fourth Amendment and legislative protections that may limit governmental collection of certain datasets do not apply to commercial actors, governmental entities can skirt these protections by acquiring data sets compiled by commercial actors. We are already seeing this in play with Clearview AI.

As a general matter, identification seems to be a far more controversial use of facial recognition than authentication. That is why a law should not lump these two uses together or address them in the same way.

We propose a BIPA that would:

1. Not apply to Biometric Identifiers collected solely for the purpose of authenticating consumers relating to the security of goods and services being provided;
2. Require businesses that collect, use, or retain Biometric Identifiers for any other purpose to first provide notice, obtain consent, and have a mechanism by which consumers can withdraw consent;
3. Permit businesses to disclose Biometric Identifiers to third parties only in specific circumstances, unless they have consent for the disclosure;
4. Require businesses to only retain Biometric Identifiers as long as necessary and to protect the Biometric Identifiers with strong data security;
5. Address the scenario where biometrics are collected in a circumstance where acquiring consent would be unduly burdensome or impossible, such as surveillance cameras;
6. Require third parties that obtain Biometric Identifiers to use them pursuant to the terms under which they were collected; and
7. Describe what is meant by notice and consent so that businesses will not be uncertain of their compliance obligations.

Expansion of the Data Broker Law

The Data Broker Law was a first-in-the-nation law passed nearly four years ago. Since its passage, a number of obvious changes have come to light that could be made to better protect Vermonters:

1. Data Brokers currently must disclose whether they permit consumers to opt-out of the Data Broker selling the consumer's data. We propose that Data Brokers are required to provide an opt-out.
2. In addition to opting out of sales of their data, consumers should have the right to demand that Data Brokers delete their data, a "right to be forgotten."
3. Consumers should not have to individually contact each Data Broker in Vermont's Data Broker registry in order to opt out. They should be permitted to sign up for a service similar to the national Do Not Call registry, which all registered data brokers would be required to periodically check and opt out all consumers registered with the service. To the extent the mechanics of such a "Do Not Track" registry are overly complicated to resolve during this legislative session, we recommend a working group be assembled at the close of the session.
4. Data Brokers currently must disclose whether they credential data purchasers, which stakeholders have described as a best practice for data brokers. They could be required to credential purchasers in a similar manner to what is required in the Fair Credit Reporting Act (FCRA).
5. Data Brokers must now track and annually disclose a special category of data breach called a Data Broker Security Breach. However, at present, if a data broker experiences such a breach, they have no obligation to notify consumers or our office when it happens. Data Broker Security Breaches should be brought in line with our normal Breach Notice Act, with appropriate adjustments due to the nature of the industry.
6. Remedies for providing false information should be added.
7. The enforcement mechanism should be strengthened.

ENFORCEMENT

Strong consumer protections mean nothing if they are not enforced. It is often difficult to learn that a violation has taken place, and enforcement can require extensive expertise and resources. If a strong protection law is created but insufficiently enforced, it can in some ways be worse than doing nothing, as it could harm citizens' faith in their government to protect them.

Therefore, if a law is passed, we recommend that it come with strong enforcement mechanisms. The mechanisms built into the Vermont Consumer Protection Act are already fairly strong, but there is still the resource issue to contend with. We recommend that enforcement of a privacy law not restrict enforcement to the Attorney General. The Vermont Consumer Protection Act has a private right of action, but it is focused on damages, which are often difficult to prove. However, 9 V.S.A. § 2461(b) permits consumers to sue for "exemplary damages not exceeding three times the value of the consideration given by the consumer."

"Exemplary damages" are the same as punitive damages, but the limitation is that consideration (the thing exchanged in a transaction, usually money) might be difficult to determine where data is involved, and in the case of data brokers and other third parties, the consumer may have given no consideration at all. We recommend that clear and specific statutory damages be included in the law. As an example, this is already the case in Vermont's Fair Credit Reporting Act, 9 V.S.A. § 2480f(b), which states:

> A consumer aggrieved by a violation of this subchapter or rules adopted under this subchapter may bring an action in Superior Court for the consumer's damages, injunctive relief, punitive damages in the case of a willful violation, and reasonable costs and attorney's fees. In the case of a violation by a credit reporting agency, or in the case of a willful violation by any person, the court, in addition, may issue an award for the consumer's actual damages or $100.00, whichever is greater.

Statutory damages and a private right of action should be structured in such a way that small- to mid-sized and less sophisticated businesses do not face the risk of ruinous litigation over minor infractions, while all businesses including larger and more sophisticated businesses face meaningful consequences for egregious violations.

CONCLUSION

Vermont has an opportunity to enact common-sense legislation that will have a huge impact on the safety of Vermonters. We should take this opportunity, be creative, and enact real, effective, enforceable protections. In summary:

1. A Biometric Information Privacy Act that includes a private right of action and clear and specific damages;
2. Data minimization provisions like those in the California Consumer Privacy Act;
3. Limit secondary uses of data by requiring third parties that acquire data to comply with the original consent and notice for which data was collected;
4. Explore enabling consumers to opt out of online tracking and Data Broker sharing of data through a "Do Not Track" system;
5. Expand the Data Broker Law; and
6. Adopt certain provisions of the California Consumer Privacy Act.

Attachments:

Letter from State Privacy & Security Coalition
VPIRG Written Comments on Data Privacy Recommendation Hearings
Letter from Consumer Reports
Letter from Thomas Weiss
Letter on behalf of a coalition of companies (Spokeo, PeopleFinders, MyLife, Truthfinder, BeenVerified, and PeopleConnect)
Letter from TechNet – regarding BIPA
Letter from TechNet – regarding comprehensive data privacy legislation
Letter from The Coalition for Genetic Data Protection

STATE PRIVACY & SECURITY COALITION

December 20, 2021

Ms. Charity Clark
Chief of Staff, Attorney General TJ Donovan
109 State Street
Montpelier, VT 05609

Re: Vermont Biometric Privacy Bill

Ms. Clark,

The State Privacy and Security Coalition, a coalition of 30 leading communications, media, technology, retail, payment and automotive companies and 7 major trade associations, writes in response to your request for stakeholder feedback on adopting a model for a Vermont biometric privacy bill.

Our members recognize the importance of consumer privacy and the sensitivity of biometric data that can identify individuals. However, we caution against replicating several of the serious problems in the Illinois Biometric Information Privacy Act (BIPA), which has produced significant unintended consequences for both businesses and consumers in that state – so much so that there is bipartisan support to amend the law 14 years later. These include BIPA's 1) private right of action (PRA), 2) overbroad definitions that cover even collection of information that does not identify an individual, which exacerbates the negative effects of its other problems, and 3) failure to exempt uses and provision of biometric data for fraud and security purposes.

The Private Right of Action Will Make Consumers Less Safe

First, including a private right of action for statutory damages would create massive class action litigation exposure for any *alleged* violations of the law by commercial entities, significantly deterring uses of biometric data including for anti-fraud, authentication and other security purposes that benefit consumers. As in Illinois, the result would be to enrich trial lawyers without striking a balance that allows the use of biometric data for purposes that benefit Vermont residents. Put simply, a private right of action means businesses will be much less likely to offer services that keep Vermonters' identities safe.

The litigation numbers bear this out: in the last five years, trial lawyers have filed *more than 1000 class action lawsuits based on BIPA.* 14 years of experience with Illinois' law have shown that this approach leads businesses to decline to offer their full suite of services to state residents, or avoid offering their services in the state at all, due to the overzealous litigation this legislation catalyzed. For this reason, Illinois is considering amending the law in order to address this significant unintended consequence and bring beneficial services back to Illinois consumers.

Furthermore, although we appreciate ideas to restrict the PRA, such as by specifying damages "up to" the statutory minimum, this is unlikely to solve the problem of frivolous lawsuits. This is because plaintiff trial lawyers' legal strategy to extract settlements does not rest even on the outcome of the case, but instead on the opportunity to inflict asymmetrical eDiscovery costs on businesses – with a cost to defend these non-meritorious actions averaging $500,000. These heavy costs to defend cases through summary judgment gives trial lawyers, who bear no or minimal eDiscovery costs, huge negotiating leverage for nuisance settlements, even if the defendant is compliant.

Furthermore, studies have revealed that private rights of action fail to compensate consumers *even when a violation has been shown*, and instead primarily benefit the plaintiff's bar by creating a "sue and settle" environment.[1] This is not to say that Vermont lacks effective enforcement options outside the trial bar. In Texas, for example, the attorney general recently launched a comprehensive investigation of biometrics violations by large digital platforms. On the other hand, the PRA in Illinois has not only failed to meaningfully protect consumers, but actually made them less safe, as anti-fraud, convenient authentication, and other beneficial services leave the state because of abusive litigation risk.

BIPA's Definitions Are Outdated and Do Not Reflect the Modern Online Ecosystem

Second, BIPA is written in such an overbroad manner that it covers information that *does not identify an individual*. Because the statute was drafted less than a year after the smartphone was invented, it does not reflect the modern understanding of biometric information as information that is used to identify individuals. This means that common and harmless features consumers use everyday, such as entertainment filters that measure face geometry but do not seek to identify an individual, are subject to BIPA litigation.

The definitions are further out of date because they cover any and all entities "in possession of" a biometric identifier, which includes incidental collection of biometric data that would not be stored and therefore poses minimal privacy risk to consumers. Again, the statute shows its age by wrapping in entities such as cloud storage providers, who have no way of obtaining consent from the consumer and no way of determining whose information they are storing. *This anonymity enhances consumer privacy*. BIPA's language exacerbates the problems described above by wrapping in a broad swath of businesses under its mandates, including those who do not ever store, disclose, or sell consumer biometric data.

BIPA Does Not Include a Cybersecurity Exception and Therefore Weeds Out Fraudsters Instead of Identifying Them

Finally, many biometric services proactively keep users, subscribers, and customers safe. Replicating BIPA would put Vermont citizens at much greater risk of fraud because biometrics

[1] Mark Brennan et al., Ill-Suited: Private Rights of Action and Privacy Claims, U.S. Chamber Institute for Legal Reform (July 2019).

are a leading means of fraud prevention. For example, biometric data is used to secure access to highly sensitive buildings, to detect fraudulent callers, and to prevent fraudulent takeovers of financial accounts.

Because BIPA does not allow for the use of biometric data for security or fraud prevention without written opt-in consent—and does not even have a clear security exception—it would put Vermont residents at great risk of security and fraud threats. Fraudsters, terrorists and other criminals simply will not consent to use of their biometric data for fraud prevention or security, so they would not be able to be screened by private businesses. This is not hyperbole – businesses in Illinois are already avoiding using biometric data for fraud or security purposes because of the huge class action risk.

This issue is even more acute in the post-COVID-19 era. Cybersecurity has never been more important, and the pandemic has resulted in an exponential increase in cybercrime activity against both private and public sector entities, including a 600 percent spike overall.[2] It is critical for the safety of both sectors that Vermont not remove an important tool to leverage in combatting cyber threats and preserving secure systems and identities.

For all these reasons, our coalition opposes using BIPA as a model. Instead, we strongly encourage Vermont to look to the Washington state biometrics law, as well as the protections for consumers included in the Virginia and Colorado omnibus privacy laws – protections that are, in fact, stronger than those that exist in the California privacy regime (CCPA & CPRA). These laws still require opt-in consent from the consumer, but reflect a more modern and widely-accepted approach to definitions and cybercrime.

Although Vermont may certainly decide to revise the Washington model rather than importing it wholecloth, this law is a product of lessons learned in the wake of BIPA. Its language solves many of the worst problems created in Illinois. In addition to providing for a security and fraud exemption, for example, the Washington law specifies a scope that covers "enroll[ing] a biometric identifier in a database." This is substantially clearer and more appropriate than the overbroad language in the BIPA law covering any and all collection.

Of course, the Washington law could still be updated in places. For example, the "enroll" language could be further clarified by adjusting that law's "commercial purpose" language to generally align with the Virginia and Colorado omnibus privacy language addressing profiling that results in "consequential decisions" affecting the consumer. This would focus the law's application on impact to the consumer, rather than the Washington law's emphasis on whether biometric information is being used for a marketing purpose. With these and perhaps additional refinements, we believe that the Washington law is a sound starting point for a version that is tailored to the concerns of Vermont consumers while avoiding the problems caused by BIPA.

[2] https://purplesec.us/cyber-security-trends-2021/.

STATE PRIVACY & SECURITY COALITION

We thank you in advance for your continued work and consideration, which we hope will succeed in making Vermont a true leader in sound biometrics privacy protection. Of course, we would be happy to discuss any of these issues further with you, if helpful.

Respectfully submitted,

Anton van Seventer
Associate

T +1 202 799 4642
F +1 202 799 5642
M +1 503 789 4852
anton.vanseventer@us.dlapiper.com

DLA Piper LLP (US)
500 Eighth Street, NW
Washington, DC 20004

DLA PIPER

dlapiper.com

VPIRG Written Comments on Data Privacy Recommendation Hearings

Thank you to the Attorney General's office for convening the stakeholder meetings around consumer data privacy this past fall and for the opportunity to submit these written comments. These comments will largely reinforce the recommendations VPIRG made during the hearings, but we include them here for your consideration.

While there are some specific areas of focus that we hope the Attorney General's office will include in its final report, our overarching position is that Vermont should move forward to enact privacy policies that treat consumer data privacy as a default and, as much as possible, remove the onus from Vermonters themselves to exercise their privacy rights and places the responsibility on would-be data collectors to respect Vermonters data privacy. To that end we would urge the Attorney General to support:

A strong data minimization standard

This is perhaps the single most effective policy Vermont could enact to change the conversation with regard to consumer privacy from a right that must be exercised to one that is the default. We support the data minimization standard language outlined in Consumer Reports Model State Privacy Legislation which states, "A business that collects a consumer's personal information shall limit its collection and sharing of that information with third parties to what is reasonably necessary to provide a service or conduct an activity that a consumer has requested or is reasonably necessary for security or fraud prevention."

Such a standard frees the consumer from potentially confusing opt-ins and opt-outs and disincentivizes businesses from using coercive techniques to receive user opt-in. As was mentioned in the hearings, data minimization is also a boon for data security insofar it limits the data collected, stored, and transmitted by companies, thus limiting the exposure of consumers to potentially harmful security breaches.

Finally, as to the ever present question of "can law keep pace with technology?" as it applies to data privacy—data minimization is one of the most future-proof policies Vermont could pursue. The concept of limiting the data an entity collects to only that which it needs to provide a service or activity requested by the consumer is applicable no matter what new data collection and retention methods one can envision.

Biometric privacy protections with a strong private right of action

While there was some discussion in the hearings about whether Illinois' Biometric Information Privacy Act is the right starting point for Vermont's consideration of biometric privacy protections, we believe it is insofar as it is the strongest state biometric privacy law in existence in terms of protecting consumers.

That is not to say that BIPA should not be reviewed and cannot be improved (it can and should—particularly with regard to definitions in the bill). But the Illinois law is the only one that contains a private right of action for violations of the law. Despite the claims of those in the industry, it is our

position that private rights of action are essential for strong enforcement of (and therefore strong compliance with) data privacy laws.

This ensures that individual consumers that have been wronged have the ability to bring a lawsuit against companies that have violated their privacy rights. It also helps the enforcement of such laws when the government entities tasked with enforcement may be under resourced.

Establishment of a brokered data breach notification requirement

VPIRG supported such a requirement during the drafting and debate process of Vermont's current data broker law. Ultimately, while a brokered data breach definition was included in the law, the law did not go so far as to require notifications of such breaches in line with Vermont's current data breach notification laws. Rather, the law simply requires data brokers to enumerate such breaches at the time of their registration.

There were no objections raised during the hearings to the establishment of a brokered data breach notification requirement, and we'd strongly support the consideration of one going forward.

Conclusion

These comments are not comprehensive—there were many good ideas surfaced during the hearings that we believe are worth exploring and hope are captured in the final recommendations. Nevertheless, we feel we that we have an opportunity to enact some commonsense protections to better safeguard Vermonter's personal information, and urge policy makers to give these serious consideration.

Zach Tomanelli
Communications & Technology Director
Vermont Public Interest Research Group

December 15, 2021

The Honorable T.J. Donovan, Attorney General
State of Vermont
109 State Street
Montpelier, VT 05609

Re: Prospective 2022 privacy legislation

Dear Attorney General Donovan,

Consumer Reports[1] sincerely thanks you for soliciting input into potential privacy legislation in the 2022 legislative session. Increased privacy protections are long overdue: consumers are constantly tracked, and information about their online and offline activities are combined to provide detailed insights into a consumers' most personal characteristics, including health conditions, political affiliations, and sexual preferences. This information is sold as a matter of course, is used to deliver targeted advertising, facilitates differential pricing, and enables opaque algorithmic scoring—all of which can lead to disparate outcomes along racial and ethnic lines.

Consumer Reports has developed model state privacy legislation that we urge you to consider when pursuing a privacy bill.[2] This model law uses the California Consumer Privacy Act (CCPA) as a baseline,[3] and provides additional protections to ensure that consumers' privacy rights are respected by default. It reflects our position that privacy laws should set strong limits on the data that companies can collect and share so that consumers can use online services or apps safely without having to take any action, such as opting in or opting out.

Above all, we recommend including in any privacy legislation a strong data minimization requirement that limits data collection, use and sharing to what is reasonably necessary to

[1] Founded in 1936, Consumer Reports (CR) is an independent, nonprofit and nonpartisan organization that works with consumers to create a fair and just marketplace. Known for its rigorous testing and ratings of products, CR advocates for laws and company practices that put consumers first. CR is dedicated to amplifying the voices of consumers to promote safety, digital rights, financial fairness, and sustainability. The organization surveys millions of Americans every year, reports extensively on the challenges and opportunities for today's consumers, and provides ad-free content and tools to 6 million members across the U.S.
[2] *Model State Privacy Act*, CONSUMER REPORTS (Feb. 23, 2021), https://advocacy.consumerreports.org/research/consumer-reports-model-state-data-privacy-act/.
[3] Cal. Civ. Code § 1798.100 et seq.

provide the service requested by the consumer, as outlined in our model bill. A strong default prohibition on data sharing is preferable to an opt-out based regime which relies on users to hunt down and navigate divergent opt-out processes for potentially thousands of different companies,[4] or an opt-in regime, in which companies could use coercive consent dialogs to push consumers to consent to inappropriate uses of their information. Consumer Reports has documented that some California Consumer Privacy Act (CCPA) opt-out processes are so onerous that they have the effect of preventing consumers from stopping the sale of their information.[5] We recommend using the following language from our model bill to shape a data minimization requirement:

> (a) A business that collects a consumer's personal information shall limit its collection and sharing of that information with third parties to what is reasonably necessary to provide a service or conduct an activity that a consumer has requested or is reasonably necessary for security or fraud prevention. Monetization of personal information shall not be considered reasonably necessary to provide a service or conduct an activity that a consumer has requested or reasonably necessary for security or fraud prevention.
> (b) A business that collects a consumer's personal information shall limit its use and retention of that information to what is reasonably necessary to provide a service or conduct an activity that a consumer has requested or a related operational purpose, provided that data collected or retained solely for security or fraud prevention may not be used for operational purposes.

However, should you choose to pursue opt-out legislation, for example, in the context of strengthening restrictions on data brokers or giving consumers the ability to opt out of the sharing or sale of their information at all companies, we recommend including the following provisions:

- *Global Opt Out.* In the absence of strong data minimization requirements, at the very least, consumers need tools to ensure that they can better exercise their opt-out rights, such as a global opt out (with a strong data minimization requirement, however, an opt out of sharing or sale to third parties is not necessary). CCPA regulations *require* companies to honor browser privacy signals as a "Do Not Sell" signal; Proposition 24 added the global opt-out requirement to the statute. The new Colorado law requires it as well.[6] Privacy researchers, advocates, and publishers have already created a "Do Not

[4] In contrast, California's Proposition 24 limits data processing to that which is necessary to carry out the purposes for which it was collected—which could incentivize companies to collect data for additional, unnecessary purposes. See Cal. Civ. Code § 1798.100(c), https://thecpra.org/#1798.100.
[5] *Consumer Reports Study Finds Significant Obstacles to Exercising California Privacy Right*s, CONSUMER REPORTS (Oct. 1, 2020), https://advocacy.consumerreports.org/press_release/consumer-reports-study-finds-significant-obstacles-to-exercising-california-privacy-rights/.
[6] Cal. Code Regs tit. 11 § 999.315(c); CPRA adds this existing regulatory requirement to the statute, going into effect on January 1, 2023, at Cal. Civ. Code § 1798.135(e) https://thecpra.org/#1798.135. For the Colorado law, see SB 21-190, 6-1-1306(1)(a)(IV)(B), https://leg.colorado.gov/sites/default/files/documents/2021A/bills/2021a_190_rer.pdf.

Sell" specification, the Global Privacy Control (GPC),[7] which could help make the opt-out model more workable for consumers.[8]

- *Authorized agent opt outs.* Similarly, allowing consumers to delegate to third parties the ability to submit opt-out requests on their behalf can help provide a practical option for consumers to exercise their privacy rights in an opt-out framework. Consumer Reports has already begun to experiment with submitting opt-out requests on consumers' behalf, with their permission, through the CCPA's authorized agent provisions. We found that consumers are enthusiastic about this option.[9]

  Authorized agent services can be an important supplement to platform-level global opt outs, by allowing for opt outs of offline data, and to help ensure that consumers can opt out of the sale of information by data brokers, with which consumers' browsers may not necessarily interact. As in California, authorized agents should also be permitted to perform access and deletion requests on behalf of consumers, for which there is not an analogous tool similar to the GPC.

  We recommend using the following language to establish a browser privacy signal and authorized agent opt outs (within an opt-out framework):

  > Consumers or a consumer's authorized agent may exercise the rights set forth in [section numbers addressing access, deletion, and opt out rights] of this act by submitting a request, at any time, to a business specifying which rights the individual wishes to exercise. Consumers may exercise their rights under [section number addressing opt out rights] via user-enabled global privacy controls, such as a browser plug-in or privacy setting, device setting, or other mechanism, that communicate or signal the consumer's choice to opt out.

- *Controls over targeted advertising.* We recommend strong definitions of sharing or sale, personal information, and deidentification, as laid out in our model bill, to ensure that pseudonymous information is covered by the opt out—providing key consumer controls over ad tracking. In California, many companies have sought to avoid the CCPA's opt-

[7] Global Privacy Control, https://globalprivacycontrol.org.
[8] Another model to consider is Senator Wyden's Mind Your Own Business Act, which outlines a system to facilitate global opt-outs through registries as well as persistent opt-out signals for both unauthenticated and authenticated data. S. 1444, § 6 (2021), https://www.congress.gov/bill/117th-congress/senate-bill/1444/text.
[9] Ginny Fahs, *Putting the CCPA into Practice: Piloting a CR Authorized Agent*, CONSUMER REPORTS (Oct. 19, 2020), https://medium.com/cr-digital-lab/putting-the-ccpa-into-practice-piloting-a-cr-authorized-agent-7301a72ca9f8; Maureen Mahoney et al., *The State of Authorized Agent Opt Outs Under the California Consumer Privacy Act*, CONSUMER REPORTS (Feb. 2021), https://advocacy.consumerreports.org/wp-content/uploads/2021/02/CR_AuthorizedAgentCCPA_022021_VF_.pdf.

out by claiming that much online data sharing is not technically a "sale"[10] (appropriately, Prop. 24 expands the scope of California's opt-out to include all data sharing and clarifies that targeted ads are clearly covered by this opt out).[11] For example, we recommend the following definition of sharing or sale, which is included in our model bill:

> "Share" [or sell] means renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's personal information by the business to a third party for monetary or other valuable consideration, or otherwise for a commercial purpose.

Further, to be comprehensive, the definition of personal information should include information "that identifies or could reasonably be linked, directly or indirectly, with a particular consumer, household, or consumer device."

- *No verification requirement for opting out*. Similarly, it's important to not require identity verification for opt-out requests. With a verification requirement, companies could require that consumers set up accounts in order to exercise their rights under the law—and hand over even more personal information. Consumers shouldn't have to verify their identity, for example by providing a driver's license, in order to opt-out of targeted advertising. Further, much of that data collected online (including for targeted advertising) is tied to a device and not an individual identity; in such cases, verification may be impossible, rendering opt-out rights illusory. In contrast, the CCPA pointedly does not tether opt out rights to identity verification.[12]

- *Strong enforcement*. So-called "right to cure" provisions in administrative enforcement, which was included in Virginia's Consumer Data Protection Act, have no place in privacy legislation. This "get-out-of-jail-free" card ties the AG's hands and signals that a company won't be punished for breaking the law. Further, given the AG's limited resources, a private right of action is key to incentivizing companies to comply. In addition, it's appropriate that consumers are able to hold companies accountable in some way for violating their rights. We would prefer a private right that would also afford consumers monetary relief, but empowering consumers to obtain injunctive relief and costs is a significant step forward.

---

[10] Maureen Mahoney, *Many Companies Are Not Taking the California Consumer Privacy Act Seriously—The Attorney General Needs To Act*, CONSUMER REPORTS (Jan. 9, 2020), https://medium.com/cr-digital-lab/companies-are-not-taking-the-california-consumer-privacy-act-seriously-dcb1d06128bb; *The State of Authorized Agent Opt Outs*, *supra* note 9, at 16.

[11] Maureen Mahoney, *Consumer Reports Urges Californians to Vote Yes on Proposition 24*, CONSUMER REPORTS (Oct. 23, 2020), https://medium.com/cr-digital-lab/consumer-reports-urges-californians-to-vote-yes-on-proposition-24-693c26c8b4bd.

[12] Cal. Civ. Code § 1798.130(a)(2).

Below, we suggest several private right of action options to consider. Consumer Reports' model bill includes a private right of action based on the CCPA's private right of action for a negligent data breach. Key aspects of this language are that a violation is an injury in fact, and that there is a limited right to cure for certain violations where cure might be possible (notably, there is no right to cure with respect to the core substantive privacy protections).

> (a) A consumer who has suffered a violation of this Act may bring a lawsuit against the business that violated this Act. A violation of this Act shall be deemed to constitute an injury in fact to the consumer who has suffered the violation, and the consumer need not suffer a loss of money or property as a result of the violation in order to bring an action for a violation of this Act.
> (b) A consumer who prevails in such a lawsuit shall obtain the following remedies:
> (1) Damages in an amount not greater than seven hundred and fifty ($750) per consumer per incident or actual damages, whichever is greater.
> (2) Injunctive or declaratory relief, as the court deems proper.
> (3) Reasonable attorney fees and costs.
> (4) Any other relief the court deems proper.
> (c) 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.
> (d) Actions pursuant to this section may be brought by a consumer if, prior to initiating any action against a business for statutory damages on an individual or class-wide basis, a consumer provides a business 30 days' written notice identifying the specific provisions of this title the consumer alleges have been or are being violated. In the event a cure is possible and the behavior underlying the violations was unintentional, if within the 30 days the business actually cures the noticed violation and provides the consumer an express written statement that the violations have been cured and that no further violations shall occur, no action for individual statutory damages or class-wide statutory damages may be initiated against the business. A cure shall not be possible for violations of sections 103, 104, 105, 110, 115, 120, 125, 126, 127, and 128. No notice shall be required prior to an individual consumer initiating an action solely for actual pecuniary damages suffered as a result of the alleged violations of this title. If a business continues to violate this title in breach of the express written statement provided to the consumer under this section, the consumer may initiate an action against the business to enforce the written statement and may pursue statutory damages for each breach of the express written statement, as well as any other violation of the title that postdates the written statement.
> (e) A consumer bringing an action shall notify the Attorney General within 30 days that the action has been filed.

The New York Privacy Act, which Consumer Reports supports, includes a private right of action. However, it is less protective than that in CR's model bill, since it applies only to those who can show injury — potentially a high bar for privacy violations.[13]

> Any consumer who has been injured by a violation of section eleven hundred two of this article may bring an action in his or her own name to enjoin such unlawful act or practice and to recover his or her actual damages or one thousand dollars, whichever is greater. The court may also award reasonable attorneys' fees to a prevailing plaintiff. Actions pursuant to this section may be brought on a class-wide basis.

The Civil Rights & Judiciary Committee Striker of the 2021 Washington Privacy Act, language which Consumer Reports supports, has a modest private right of action, with injunctive relief only.[14] We would prefer a private right that would also afford consumers monetary relief, but empowering consumers to obtain injunctive relief and costs would be a significant step forward and would help incentivize compliance.

> A consumer alleging a violation of section 103 or 107 (6), 4 (8), or (9) of this act may bring a civil action in any court of competent jurisdiction. Remedies shall be limited to appropriate injunctive relief. The court shall also award reasonable attorneys' fees and costs to any prevailing plaintiff.

- *Non-discrimination.* Consumers have a fundamental right to privacy, and should not be charged for exercising their privacy rights. As outlined in our model bill, privacy legislation should strictly prohibit companies from offering a different price based on whether or not a consumer has opted out of the sale of their information. However, we have also supported compromise legislation in the Washington Privacy Act, which not only clarifies that consumers cannot be charged for exercising their rights under the law, but it makes it clear that legitimate loyalty programs, that reward consumers for repeated patronage, are supported by the law:

> A [business] may not discriminate against a consumer for exercising any of the rights contained in this chapter, including denying goods or services to the consumer, charging different prices or rates for goods or services, and providing a different level of quality of goods and services to the consumer. This subsection does not prohibit a [business] from offering a different price, rate, level, quality,

[13] The New York Privacy Act (2021), https://www.nysenate.gov/legislation/bills/2021/s6701.
[14] Civil Rights and Judiciary Committee (SB 5062), https://lawfilesext.leg.wa.gov/biennium/2021-22/Pdf/Amendments/House/5062-S2%20AMH%20CRJ%20H1373.1.pdf.

or selection of goods or services to a consumer, including offering goods or services for no fee, if the offering is in connection with a consumer's voluntary participation in a bona fide loyalty, rewards, premium features, discounts, or club card program. If a consumer exercises their rights pursuant to [section number] of this act, a [business] may not sell personal data to a third-party [business] as part of such a program unless: (a) The sale is reasonably necessary to enable the third party to provide a benefit to which the consumer is entitled; (b) the sale of personal data to third parties is clearly disclosed in the terms of the program; and (c) the third party uses the personal data only for purposes of facilitating such a benefit to which the consumer is entitled and does not retain or otherwise use or disclose the personal data for any other purpose.[15]

- *Definition of consent and prohibition on dark patterns.* In the context of an opt in or opt out bill, a strong definition of consent can help ensure that privacy laws that are based on consent can be useful for consumers. Too often, companies often use dubious dark patterns to nudge users to click "OK," providing the veneer, but not the reality of, knowing consent.[16] We suggest the following language to consider, should you pursue consent-based legislation.

  (a) CONSENT.—
  (1) It shall be unlawful for a covered organization to collect, use, or disclose personal information unless
  (A) the individual to whom the data pertains has given affirmative express consent to such collection, use, or disclosure
  i) The general nature of the data processing shall be conveyed in clear and prominent terms in such a manner that an ordinary consumer would notice and understand them.
  ii) An individual may consent to data processing on behalf of his or her dependent minors
  (B) such collection, use, or disclosure is necessary and for the sole purpose of:
  a) protecting against malicious, deceptive, fraudulent, or illegal activity; or
  b) detecting, responding to, or preventing security incidents or threats; or
  (C) the covered organization is compelled to do so by a legal obligation.
  (2) REVOCATION.—
  (A) In General.— A covered organization shall provide an effective mechanism for an individual to revoke their consent after it is given.

[15] *Id.*
[16] *Most Cookie Banners are Annoying and Deceptive. This Is Not Consent,* PRIVACY INTERNATIONAL (last visited Aug. 28, 2020), https://privacyinternational.org/explainer/2975/most-cookie-banners-are-annoying-and-deceptive-not-consent.

(B) Effect.— After an individual revokes their consent, the covered organization shall cease collecting, using, or disclosing the individual's personal information as soon as practicable, but in no case later than 15 days after the individual revokes consent.

Further, a prohibition on dark patterns—deceptive interfaces that push consumers to take actions that they did not intend—can help ensure that consumers are able to exercise their preferences in a consent-based privacy law. Current CCPA regulations prohibit the use of dark patterns in CCPA opt outs;[17] and Proposition 24, which amends the CCPA and will go into effect in 2023, includes a prohibition of the use of dark patterns in obtaining consent, for example, consent to opt back into the sharing or sale of personal information.[18] Colorado's newly passed privacy law includes a nearly identical prohibition on dark patterns in obtaining consent.[19]

- *Data security requirements.* A comprehensive privacy bill would expand the definition of personal information to any information that could reasonably be linked, directly or indirectly, to a particular consumer, household, or device. As such, a privacy bill should ensure that the existing data security requirement in Vermont law covers this expanded definition of personal information, so that companies are required to use reasonable security protocols to safeguard the confidentiality and integrity of covered information. Information in online accounts and browsing activity can be very sensitive and should be protected from hackers.

Thank you again for your consideration, and for your work on this legislation. We look forward to working with you to ensure that Vermont consumers have the strongest possible privacy protections.

Sincerely,

Maureen Mahoney
Senior Policy Analyst

Justin Brookman
Director, Technology Policy

[17] Cal. Code Regs tit. 11 § 999.315(h).
[18] Cal. Civ. Code §1798.140(h).
[19] Colorado Privacy Act, SB 21-190 (2021), https://www.google.com/url?q=https://leg.colorado.gov/bills/sb21-190&sa=D&source=editors&ust=1639343861044000&usg=AOvVaw3MQRCsi1rHmLyp9ppkB2Pl.

P. O. Box 512
Montpelier, Vermont 05601
December 15, 2021

Office of the Attorney General
109 State Street
Montpelier, Vermont 05609-1001

Subject: Privacy forums on biometric information

Dear Ms. Clark and Mr. Kriger:

Thank you for the opportunity to participate in these privacy forums on biometric information.

My carefully considered comments and recommendations are contained in the attached document.

I hope you find them worthy of incorporation into a bill to regulate biometric information and to strengthen our protection of individuals and of the various categories of information.

Sincerely,

Thomas Weiss

Privacy forums on biometric information

Comments by Thomas Weiss
December 15, 2021

Introduction

Biometric information is unique, highly sensitive, and requires stronger protections, stricter regulations, and tighter enforcement than all other forms of personalized information. Recovery from a data breach involving other information is difficult. Recovery from a data breach involving biometric information is basically impossible. Any regulation of biometric information needs to strictly limit its collection and its use.

If we cannot guarantee protection of individuals' right to privacy and of protection from injury through use or misuse of biometric information, then we need to prohibit its collection.

These comments address the six topics we were asked to consider. My concerns are identified in the first four topics.
- what is the problem we are trying to solve?
- should Vermont adopt all or parts of the California Consumer Privacy Act
- using Illinois' Biometric Information Privacy Act
- review of Washington's statutes on Biometric Identifiers and on facial recognition

Features to reduce my concerns are in the fifth and sixth topics.
- protecting individuals through prohibitions and protections of biometric Information, including facial recognition
- protections that better address the privacy concerns of Vermonters (not already in the section on biometric information)

Presenting the Concerns

What is the Problem we are Trying to Solve?

1. The problem is that individuals are unable to protect themselves from the dangers of collection, use, and misuse of biometric information.

2. Biometric information is unique to each individual and cannot be changed when it is compromised.

3. There is no fair compensation to individuals for an unauthorized acquisition.

4. Any use of facial recognition, not authorized by the individual, is a violation of privacy and a loss of individual privacy protections. Facial recognition leads to dossiers on everyone, which may or may not be governmental. Social media companies maintain dossiers on all their customers and on everyone their customers interact with or identify. Because software designers, corporations, and social media companies can so easily coerce people into "authorizing" this violation of privacy using mandatory software agreements, Vermont's Data Privacy laws must protect individual's rights to privacy.

5. Our system of collection, storage, and protection of the various elements of information is inadequate to protect individuals and their biometric information. Secure protection of biometric data — if it is possible — will require amending a number of our existing statutes. It remains unclear as to whether we can protect individuals by protecting personal information derived from biometric data collection.

Navigating the existing categories is difficult.
Vermont defines six categories of information by the data elements that each contains.[1] Each category has different provisions regarding use or protection of data elements. When a data element is included in more than one category, the provisions on that element can conflict.

Exhibit 1 shows which data elements are included in each of the six categories of information. It also shows the form the data need to have in order to be protected and which entity is involved with each category.

Biometric information of some form or other is found in four of the categories.

Personally identifiable information (PII) has elements of "unique biometric data"[2] and "genetic information" that is in unencrypted, unredacted, or otherwise unprotected digital format. That is insufficient. Modern technology makes it easy to convert non-digital formats to digital formats. PPI is used by data collectors, who may disseminate the information to anyone.

Login credentials has some provisions in common with PII and other provisions that apply only to login credentials. The definition of login credentials excludes biometric information. However, biometric information (e.g., voice prints and fingerprints) are sometimes used as a login credential.

Brokered personal information (BPI) has the same element of "unique biometric data", but only when it is in digital format categorized or organized for dissemination to third parties. (BPI does not include the element of "genetic information".) BPI is the only form of information whose acquisition is restricted under §2431, prohibiting acquisition of information under certain conditions. BPI is used by data brokers.

What is the difference between "digital" in PPI and "computerized" in BPI? The statute uses two terms, so there must be a difference.

How do the provisions applying to data brokers interact with those applying to data collectors? Data brokers are both.

Covered information (CI) relates to students. It has data elements of "biometric information" and "voice recordings" that may be in any media or format. Covered information is used by operators.

How do the provisions applying to operators interact with those applying to data brokers and to data collectors? An operator meets the definitions of all three.

Social security numbers have a subchapter of their own. The numbers are also included in data elements of PII, BPI, CI, and PI. How do these five sets of provisions interact?

Personal information (PI) applies only within the Document Safe Destruction Act (§2445, within Chapter 62). PI has an element of "physical characteristics or description" which is a form of biometric information. "Business" is defined more narrowly by §2445 than "business" is defined by §2430 for all of Chapter 62. Section 2445 businesses need to "take all reasonable steps to destroy or arrange for the destruction of" a customer's records containing PI. Entities that dispose of personal information of residents "must take all reasonable measures to dispose of records".

---

1 The six categories are: personally identifiable information (PII); login credentials (LC); brokered personal information (BPI); covered information (CI); social security numbers (SSN); and personal information (PI).

2 unique biometric data generated from measurements or technical analysis of human body characteristics used by the owner or licensee of the data to identify or authenticate the consumer, such as a fingerprint, retina or iris image, or other unique physical representation or digital representation of biometric data

"Reasonable" is a vague term, subject to wide interpretation.

Governmental units are not subject to Section 2445. I acknowledge that records management for them is covered under records retention policies in other statutes. Destruction of governmental records needs to be covered by the provisions in section 2445 unless provisions elsewhere are more stringent.

Data brokers are not covered by §2445. A data broker has no customer as defined by the act.

What provisions apply to intermediaries in the record destruction process? Some businesses and solid waste management districts take documents from individuals for a fee. The documents are stored on site. The intermediary then transfers the documents to an entity which actually shreds them. It is not clear that these intermediaries are subject to section 2445. It is not clear whether intermediaries may act as data collectors when the documents are in their custody.

Too many unauthorized acquisitions are not security breaches

Not all unauthorized acquisitions are security breaches. Security breaches can only occur with PPI. Data broker security breaches can only occur with BPI. Loss of control of data elements that are not in either category are not considered security breaches. Loss of control of data elements of PPI or BPI not in the specified formats are not breaches. Exhibit 1 shows which elements are in each category, and by extension, which are subject to the breach provisions and which are not.

The treatment of data elements should be consistent, regardless of the type of data handler. Provisions can be circumvented when a specific entity falls into more than one category of data handler. Data in all categories must be secure regardless of definitions of entities and how many categories they may fall into.

Transfers are neither secure nor verifiable

Biometric information is different than other forms of personalized information. Illinois finds:

> "(c) Biometrics are unlike other unique identifiers that are used to access finances or other sensitive information. For example, social security numbers, when compromised, can be changed. Biometrics, however, are biologically unique to the individual; therefore, once compromised, the individual has no recourse, is at heightened risk for identity theft, and is likely to withdraw from biometric-facilitated transactions."
>
> "(f) The full ramifications of biometric technology are not fully known."

There are no mechanisms to assure that data being transferred are accurate and actually belong to the individual. None of the statutes I have reviewed (Vermont, Illinois, California, Washington, Texas) has such a mechanism. There is no way for the recipient to know that the information actually belongs to the individual that the provider claims. The consequences of mis-identification, severe in all cases, are much more severe with biometric information.

The burden of recovery is placed on the individual

Individuals have the burden of recovery from incorrect information and from unauthorized acquisitions of data (which include security breaches). The entity losing control of the information has no liability to the individual for the anguish of the unauthorized acquisition or for the time, effort, and expense of repairing the damage: closing accounts; opening new accounts; getting new identification; altering information on the secretary of state's system to protect individual's locations.

Individuals have no right to know what information is held, what entity holds it, and whether it is accurate. Individuals have no right to have the information corrected. (There is a limited exception in chapter 63 with regard to credit reporting agencies.)

Learning of unauthorized acquisitions is difficult. The notice procedures prevent direct notice to affected individuals in too many cases. Exhibit 2 shows the ten possible outcomes and how many of them prevent direct notice to the affected individuals.

It is much more difficult, perhaps impossible, to recover from an unauthorized acquisition of biometric information than to recover from unauthorized acquisitions of other data elements.

Inability of an individual to control the dissemination of information
An individual has no say in how information is disseminated. An individual has no knowledge of where the information goes. An individual is not compensated for the use of the information. Data elements that are too sensitive to be disseminated or to be allowed to be disseminated. Individuals lose control of their information when it is acquired by a data handler.

The definition of "unique biometric data" implies that the individual is not the owner of the data.

Lack of trust
Mr. Kriger stated on October 26 that we need a system that people can trust. I do not trust data collectors or brokers to protect me or my data. Data collectors have a record of inability to protect data. We have little idea of how well or poorly data brokers protect data because they are not required to report individual data breaches.

Disadvantages to individuals far outweigh advantages
Weighing advantages *vs.* disadvantages is part of decision making. I find that the disadvantages to individuals of collecting and using biometric information are far greater than the advantages to individuals.

Summary
The ramifications of the problem as it relates to biometric information include:
- loss of privacy
- being tracked
- the inability or unwillingness of some holders of information to protect the information they hold
- privacy policies that do not identify by name the entities with whom the information is shared
- privacy policies that allow sharing where not prohibited, instead of limiting sharing to when required, by law.
- the inability of individuals to protect themselves against identity theft
- the inability of individuals to control their own information
- the use of opt-out instead of opt-in (and opt-out is available only in limited cases)
- failure to recognize that the information belongs to the individual
- misuse or unauthorized use of information
- re-purposing the use of information without notification to the individual
- the "take-it-or-leave-it" aspects of not refusing collection
- the poor negotiating position of individuals when it comes to use of their data
- the inability to prevent those with legitimate access to the data from using the data in illegitimate ways
- governmental units are exempt from many of the provisions of chapter 62
- protection depends on the format or media and is not available across all formats and media.

Should Vermont Adopt All or Parts of the California Consumer Privacy Act?

Vermont should adopt the following concepts of the California Consumer Privacy Act. They are essential concepts for protection of individuals and their biometric information.
- a right to delete information
- a right to correct inaccurate information
- a right to know what information is being collected

- a right to access information
- a right to know what information is being sold and shared and to whom
- a right to opt out of sale or sharing of information (better yet is to make this an opt in requirement)
- a right to limit use and disclosure of sensitive information
- a right of no retaliation following opt out or exercise of other rights (better yet, add failure to opt in to the list)

Some of these rights are included in the provisions of chapter 63 relating to credit information and credit reporting. The rights do not apply to other forms of information or other holders of information.

There might be other concepts worth bringing into Vermont. (I have not looked at the California act in detail.) The concepts that we bring into Vermont likely will need adjustment to fit into our existing statutes.

Using Illinois' Biometric Information Privacy Act

The Illinois Act should not become a separate subchapter. Its organization and details have multiple conflicts with chapter 62. A better solution is to weave worthy concepts from that act into chapter 62.

Illinois requires only private entities to comply with the provisions on protection of biometric information. Vermont needs to require all data collectors (which include governmental agencies) to comply.

Sec. 15, handling of the data
We should require a written release by the subject in order to obtain biometric information, as in 15(b). We also need to prohibit receiving biometric information from anyone other than the individual.

The provisions of 15(c) (prohibiting certain transfers) and of 15(d) (allowing other transfers) conflict. Transfer by sale, lease, trade, or otherwise profit is prohibited by (15(c)). The disclosure, re-disclosure, or other dissemination is allowed with the consent of the individual (15(d)). The two provisions conflict, because a sale is a form of dissemination. So a sale is prohibited by (c) and dissemination by sale is allowed by (d).

Vermont should prohibit all transfers of biometric information by any means for any reason.

Illinois requires biometric information to be destroyed within three years of the individual's last interaction; or earlier if the initial purpose has been satisfied. Three years is too long. For example, if a data handler uses biometric identification of customers, then the waiting period for destroying the information needs to be much shorter than three years.

Illinois requires a handler of biometric data to have a retention schedule and guidelines for permanently destroying biometric data. The concept might be useful. The details will need to be modified. The Illinois requirement is written with businesses in mind, not individuals. Illinois' policy guidance allows too much flexibility and not enough details on how the policy should work and how data elements should be covered. This vague policy guidance will only compound the problems with our data broker registry. My limited review of the data broker registry is there is too much variability in their approaches and that formats are non-standard. The vagueness of the policy requirements in the Illinois act would lead to those same problems. Thus, Vermont should provide rigorous and developed conditions for the policy. The policy needs to be prepared before collection of biometric information is begun.

I do not trust the "reasonable standard of care within the entity's industry" (Sec. 15(e)(1)) as being protective. It seems each industry would have a different standard. I think our statutes need to provide specific, high standards for the protection of the data.

Using the "reasonable standard of care", one bringing a civil complaint would have to figure out the standard of care for that particular industry. And if the data passed through several entities before being breached, what a nightmare for the individual trying to bring a suit.

Sec. 20, right of action
Illinois' right of action is biased against individuals. It is ludicrous to think that this right of action will be a deterrent.

The expected gain of filing suit is minuscule compared to the expected loss if the business prevails. Having to sue, figure out the standard of care of the industry for a measly gain to the individual of $1,000 or $5,000 *vs.* the potential loss of paying attorney's fees to the business if the business prevails is totally inadequate as compensation for the damage done by the business. I am not sure what suitable compensation is or what is a suitable procedure to obtain compensation. I am sure that what Illinois offers is unsuitable.

Sec. 10, definitions
"Written release" is the only definition in the Illinois act (sec. 10) worth considering. Written release needs to apply to collection of biometric information. It would not apply to transfer of biometric information because transfer of biometric information will be illegal. We need to incorporate written release into chapter 62 for other data elements, too. Vermont needs to require opt-in provisions for biometric information. Opt-in should be required for all other data elements, too.

Provisions on biometric information need to apply to governmental units. (Illinois excludes them.)

Sec. 5, findings and intent. I doubt that we need findings and intent. There have been seven acts that deal with chapter 62. Only one (the data broker bill) has findings and intent. Those are not incorporated into the chapter.

I agree with Illinois' findings (c) and (f) (both quoted on p. 3). Finding (g) (serving public welfare, security, and safety) is only partially achieved by Illinois' act. I do not know the accuracy of the other findings.

Sec. 25, construction
Protection of biometric information in Illinois is excluded in multiple instances.
- admission or discovery
- other specified acts and rules are not superseded by the Illinois act, even if those acts and rules do not protect biometric information to the same extent as the BIPA.
- financial institutions or their affiliates, even if those institutions are not required to protect biometric information to the same extent as the BIPA.
- contractors, subcontractors, and agents when working for a State, etc. are not required to destroy all of the data (or return it to the State, etc.) when the work is complete or the contract is over or whatever the appropriate period is. After a contract is complete, the contractor is allowed to retain the information. A subject never knows that the contractor has possession of the biometric information.

Vermont should adopt none of these constructions.

Summary
I believe that the Illinois act was developed for its time and place. I believe that act provides more protection to entities (private or governmental) that use biometric information than it provides to individuals. Clearly, I do not support Vermont's use of the Illinois act as a model. Vermont must, for all of the reasons offered above, avoid the stated problems with the Illinois act.

Review of Washington's Statutes on Biometric Identifiers and on Facial Recognition

Statute on Biometric Identifiers
Washington's Chapter 19.375 RCW has nothing worth replicating in Vermont. The entire chapter fails to protect individuals and their biometric information. If we patch up all the problems, we might as well not have started from Washington. It is less protective of individuals than the statutes of either California or Illinois.

There is so much wrong with Washington's statute that it will take three or more pages going over the statute point by point to cover all the deficiencies. Here are some of the problems.
- Stores (and other establishments) may gather biometric identifiers from all who enter with neither notice nor consent.
- Transfers of biometric identifiers are regulated only if the transfer is for sales or marketing purposes.
- Individuals have no control over their biometric information and little control over biometric identifiers. A biometric identifier may be transferred for marketing or sales purposes with neither notice to the individual nor consent. All that is needed is a mechanism to prevent subsequent use for a commercial purpose. The loopholes which allow transfer without consent are enormous.
- There is no regulation of governmental units that have biometric identifiers.
- Biometric patterns and characteristics are not protected; only data generated from them are regulated, and that feebly.
- The chapter has multiple internal contradictions
- The exceptions (to what little regulation there is) are so numerous that there is little protection of individuals.

Individuals in Vermont deserve better protection than Washington's biometric identifiers gives its individuals.

Statute on Facial Recognition
Vermont should adapt much of the concept of Washington's Chapter 43.386 RCW. The concept is regulating use of facial recognition by sub-State governmental units (Counties and municipalities in Vermont's broad definition).

Applying standards for use of facial recognition by sub-State governmental units fills a void in Vermont's data protection standards.

Adaptations would include:
- expanding to include all biometric information (and perhaps other data elements)
- putting into statute some common elements of the report: notification of data breaches being one
- placing additional restrictions on the use for surveillance, real-time identification, or persistent tracking
- creating a crime of surveillance, real-time identification, and persistent tracking by any entity
- reducing the potential plethora of governmental units developing programs. (In Montpelier they could be the City, the School District, the County, the regional planning commission, the solid waste management district, and the fire district (if it wasn't eliminated when the City took over its functions))
- authorizations by individuals to collect information and to disseminate it

Protecting Individuals through Prohibitions and Protections of Biometric Information, including Facial Recognition

This section contains features that are intended to protect individuals and their biometric information. These features result from the concerns presented above. Individuals will be protected even more if these features also apply to other data elements.

Create a separate definition of biometric data, using the one for "unique biometric data . . . " as a starting point.

Use the same definition in each of the information categories which contain biometric information.

Provisions on biometric information apply to all entities that collect biometric information.

Biometric information belongs to the individual.
- The individual may license use of that information to a specific entity for a specific purpose.
- The individual is to be compensated for the use of the information.
- All biometric information is collected directly from the individual.

All biometric information is collected on an opt-in basis directly from the individual. The Illinois requirements on obtaining consent seem to be appropriate.

Biometric information may not be used for commercial or consumer transactions or purposes. (This is all in a broad sense.) This goes along with the non-retaliation concept from California.

Add biometric information to the prohibitions on acquisitions in §2431.

Establish a crime of data trafficking (a new §2432, perhaps) involving
- transfer of biometric information
- selling, etc. (see Illinois act) biometric information
- other data elements could be included

Individuals and biometric information is protected by all the California rights. (By this, I mean the concepts. I have not evaluated whether the rights as implemented in California are sufficient or workable.)

Regulate use of facial recognition (better yet, all biometric information) by adapting Washington's statutes.

Establish a crime of surveillance, real-time identification, and persistent tracking (a new §2433), perhaps

Breach includes all unauthorized acquisitions of biometric information in all media and all formats.

Each individual whose biometric information has been breached receives direct notice, regardless of cost. Biometric breach notices to be sent within 24 hours of the discovery. Notices also include all data elements breached, even if they would not be in individual direct notices otherwise.

Full liability by the entity that was breached. Period. No excuses. No court cases for recovery. Part of the liability is to provide recovery assistance to the individuals whose information was breached. (Maybe something like traffic tickets or environmental ticketing, if that still exists?)

Remove biometric information from the category of brokered personal information. (If a broker sells or licenses biometric information, that will be data trafficking.) Require all data brokers in the registry (active, inactive, cancelled, withdrawn) to certify to the Secretary of State that they have destroyed all their records of biometric information of Vermonters. Require them to provide to the Secretary of State a list of all third parties to whom they have sold or licensed biometric information of Vermonters.

Biometric information may not be transferred as a part of a merger or acquisition or spinoff.

Biometric information cannot be considered an asset in bankruptcy proceedings or otherwise, because it cannot be transferred.

It would be useful for the attorney general's office to reach out to the writers of the Act 89 (2020) report to determine their logic in omitting the three items (genetic information, health records . . . , and medical diagnosis . . .). And to find out what would have been needed for the authors to include them in the report.

Protections that Better Address the Privacy Concerns of Vermonters

Individuals can be more strongly protected by adopting these features. These features go beyond those needed for biometric information. Provisions relating to biometric information are contained in the previous section.

Categories of information
Restrict the dissemination of personally identifiable information.

Expand the definitions of PPI and BPI to include all media and all formats.

Expand the definition of login credentials to include biometric information if used as a credential.

Expand the prohibitions of section 2431, "acquisition of brokered personal information; prohibitions" to all six categories of information.

The consequences for violating §2431 need to be increased. Violating the provisions of § 2431 is now an unfair and deceptive act in commerce. The remedies are assurances of discontinuance, bring civil actions, and take other steps in accordance with subchapter 1 of chapter 63. Other agencies rarely take action against violations, in my experience. And the penalties of those assurances of discontinuance are too small to be a deterrent.

"Record" has two definitions: in §2430 (definitions, applicable to all of chapter 62, including §2445) and in §2445 (destruction of records). Remove the definition of record from §2445 and work it into the definition of §2430.

Require governmental units to comply with more of the provisions of chapter 62. They are now exempt from the provisions of BPI and PI.

Develop a system to compensate individuals for use or dissemination of data elements. Individuals are not compensated for the dissemination or use of their data.

Data brokers
Use the data broker registry to determine what additional restrictions to place on them. The data broker registry is not an end in itself. It was established to learn how data brokers operate and to get an idea of how many there are. As of early November, the number of data brokers registered with the Secretary of State is large: 379 total. (166 active, 209 expired, 3 cancelled, none inactive, and 1 lost in cyberspace). Even the 166 active are beyond the capability of individuals to monitor. We need to evaluate the information in the data broker registry and provide stricter regulation of data brokers.

Bring data brokers under the provisions of §2445 (destruction of records). Data brokers are not currently required to destroy records of Vermonters when their registrations are no longer active. Data brokers shall be required to destroy the records of Vermonters when their registrations expire, are cancelled or become inactive.

Require data brokers to protect all data elements in their possession. Data brokers have a duty to protect personally identifiable information (§2447). That duty does not extend to the components of brokered personal data that are not also included in personally identifiable data.

Require data brokers to provide notices of data broker security breaches. Data brokers are not required to provide notice of data broker security breaches. They merely need to put into the annual registration the number of breaches and the number of Vermont residents affected in the previous year. The notice requirements of §2435 apply only to breaches involving personally identifiable information and login credentials. This means that residents receive notice of a security breach only when the breach involves elements of brokered personal information that also are elements of personally identifiable information. Vermonters never learn of data broker security breaches in the past year if the broker does not renew the registration.

Require data brokers to offer opting out. Better yet, require them to use opting in. Data brokers are not required to allow opting out. The registry reveals only whether they allow opting out.

Require data brokers to register before operating. Data brokers may operate up to one year before registering. Most professions require registration before being allowed to practice, in part because they have the ability to harm the public. Data brokers also have the ability to harm the public. (I am not suggesting that data brokers be regulated as professionals.)

Deficiencies pointed out by the Act 89 (2020) report: "Data Privacy; State Government" January 15, 2021
The general assembly directed that the report contain an inventory "that shall address the collection and management of personally identifiable information".

Three elements of personally identifiable information were intentionally omitted from the report. The three are: (1) genetic information; (2) health records or records of a wellness program or similar program of health promotion or disease prevention; and (3) health care professional's medical diagnosis or treatment of the consumer.

The definition of PII is given in chapter 62.

> " 'Personally identifiable information' means a consumer's first name or first initial and last name in combination with one or more of the following digital data elements, when the data elements are not encrypted, redacted, or protected by another method that renders them unreadable or unusable by unauthorized persons:" followed by the list of data elements.

The writers of the report do not state their reasons for the omission. They provide two hints. On page 7 of the report, they recommend amending the definition to remove "the specificity of discrete digital data elements". On page 45 they write "This inventory *does not include* non-data elements that were added to the definition of personally identifiable information in 9 V.S.A. § 2430 by Act 89, specifically:" the three elements.

The writers also did not cover federal laws or regulations on the grounds that the COVID-19 pandemic hampered their ability to prepare the report.

Changes to Vermont's security breach notice act.
Expand the requirements for direct notice to consumers whose data have been breached. Reduce the number of outcomes in which the public receives no notice.

Vermonters never receive notice of too many breaches. They never receive notice of unauthorized acquisitions that are not security breaches. The security breach notice act has ten possible outcomes when an entity handling information discovers an unauthorized acquisition of information. These outcomes are shown on exhibit 2.
- Only two of the outcomes lead to direct notice to individuals whose information has been breached.
- In two more (cost of notice exceeds $10,000 or the collector lacks sufficient contact information), notices are distributed through the media, requiring individuals to take steps to find out if their information has been breached. One might never learn of the breach if one misses the media reports.

- The other six outcomes provide no public notice. Three outcomes are that an unauthorized acquisition is not a security breach (neither PPI nor the narrow definition of media and format). Two more are that notice only goes to the attorney general or department of financial regulation (the breach is a trade secret or law enforcement never allows notice to be given). The sixth is that someone has to submit a public records request to find out if a breach has occurred (because the collector determines that "misuse is not reasonably possible").

Notices are not provided quickly enough. Notice may be withheld 45 days or even forever.

Conclusion

Vermonters are vulnerable to injury from permitted uses of biometric information and other information. We are vulnerable to unauthorized acquisitions of our data.

Vermont's data protection statutes need major changes in order to protect biometric information. I have provided a set of features for protection of biometric information. Many of the protections for biometric information should be applied also to other data elements. If these features are inadequate to protect individuals, then we should prohibit the collection of biometric data (for any purpose other than specific medical purposes, in which case all data must remain between the individual and the health care provider).

In addition, I have provided other features that will more strongly protect individuals and their non-biometric information.

Exhibit 1 - data elements classified in 9 V. S. A. chapter 62
As amended by Act 89,of 2020
prepared by Thomas Weiss
November 12, 2021

PII (data collectors)	LC (data collectors)	BPI (data brokers)	CI (student privacy)	SSN (use of SSN)	PI (destruction of records)
§2430: definition of PII applies to §2430 through 2447 (all of chapter 62)	§2430: definition of LC applies to §2430 through 2447 (all of chapter 62)	§2430:definition of BPI applies to §2430 through 2447 (all of chapter 62)	§2443: definition of CI applies to §2443 only	§2440: there is no definition	§2445: definition of PI applies to §2445 only
form of information: non-encrypted- digital	(all formats)	non-encrypted-digital; categorized or organized for dissemination to third parties	not publicly available or publicly available through a specific federal act. in any media or format	(all formats)	any material, regardless of the physical form
entities handling the information: person (in the legal jargon sense); the State, State agencies, political subdivisions	person (in the legal jargon sense); the State, State agencies, political subdivisions	commercial entity (profit or non-profit); financial institution, and its parent, affiliate or subsidiary: excludes any governmental entity of the State; excludes vendors acting solely at the direction of the State	operator of services or applications used primarily for PreK through 12 students.	commercial entity (profit or non-profit); financial institution, and its parent, affiliate or subsidiary: separate provisions for the State, political subdivisions, and agents or employees of the State.	businesses (definition specific to §2445) that destroy records of their customers. Entities in the business of disposing of personal financial information.
first name or first initial and last name plus any other(s)		name	first and last name		
social security number		social security number	social security number	social security number	social security number
driver's license number		other government issued ID number			driver's license number
non-driver State ID card number		other government issued ID number			State ID card number
individual taxpayer ID number		other government issued ID number			
passport number		other government issued ID number			passport number
military ID card number		other government issued ID number			
other government issued ID number commonly used to verify identity for a commercial transaction		other government issued ID number			
financial account number, credit card number, or debit card number that could be used without passwords, access codes, or additional identifying information					bank account number
					credit card or debit card number (whether or not in can be used without passwords, access codes, or additional identifying information
					insurance policy number
					any other financial information
password, PIN, or other access code for a financial account					
	user name or e-mail address combined with a password or security answer				
unique biometric data . . . used . . . to identify or authenticate the consumer, such as a fingerprint, retina or iris image, or other physical representation or digital representation of biometric data		unique biometric data . . . used . . . to identify or authenticate the consumer, such as a fingerprint, retina or iris image, or other physical representation or digital representation of biometric data	biometric information		physical characteristics or description
genetic information					
health records			health records		
records of a wellness program or similar program of health promotion or disease prevention					
health care professional's medical diagnosis or treatment					
			medical records		
health insurance policy number					
		address	home address		
		name or address of immediate family or household member			

PII (data collectors)	LC (data collectors)	BPI (data brokers)	CI (student privacy)	SSN (use of SSN)	PI (destruction of records)
		date of birth			
		place of birth			
		mother's maiden name			
					signature
		other information that, alone or in combination, with the other information is linked or linkable to the consumer that would allow a reasonable person to identify the consumer with reasonable certainty			
			telephone number		
			electronic mail address		
			other information that allows physical or online contact		
			information in the student's education record or electronic mail, discipline records, test results, special education data, juvenile dependency records, grades, evaluations, criminal records, disability status, socioeconomic information, food purchases, political affiliations, religious information, text messages, documents, student identifiers, search activity, photos, voice recordings, or geolocation information.		
			personal information or material, or information that is linked to personal information or material that a student (or parent or guardian) creates or provides to an operator of certain online activities	\	
		excludes publicly available information to the extent that it is related to a consumer's business or profession.			

Shaded data elements are part of personally identifiable information.

The following data elements might be added to chapter 62.

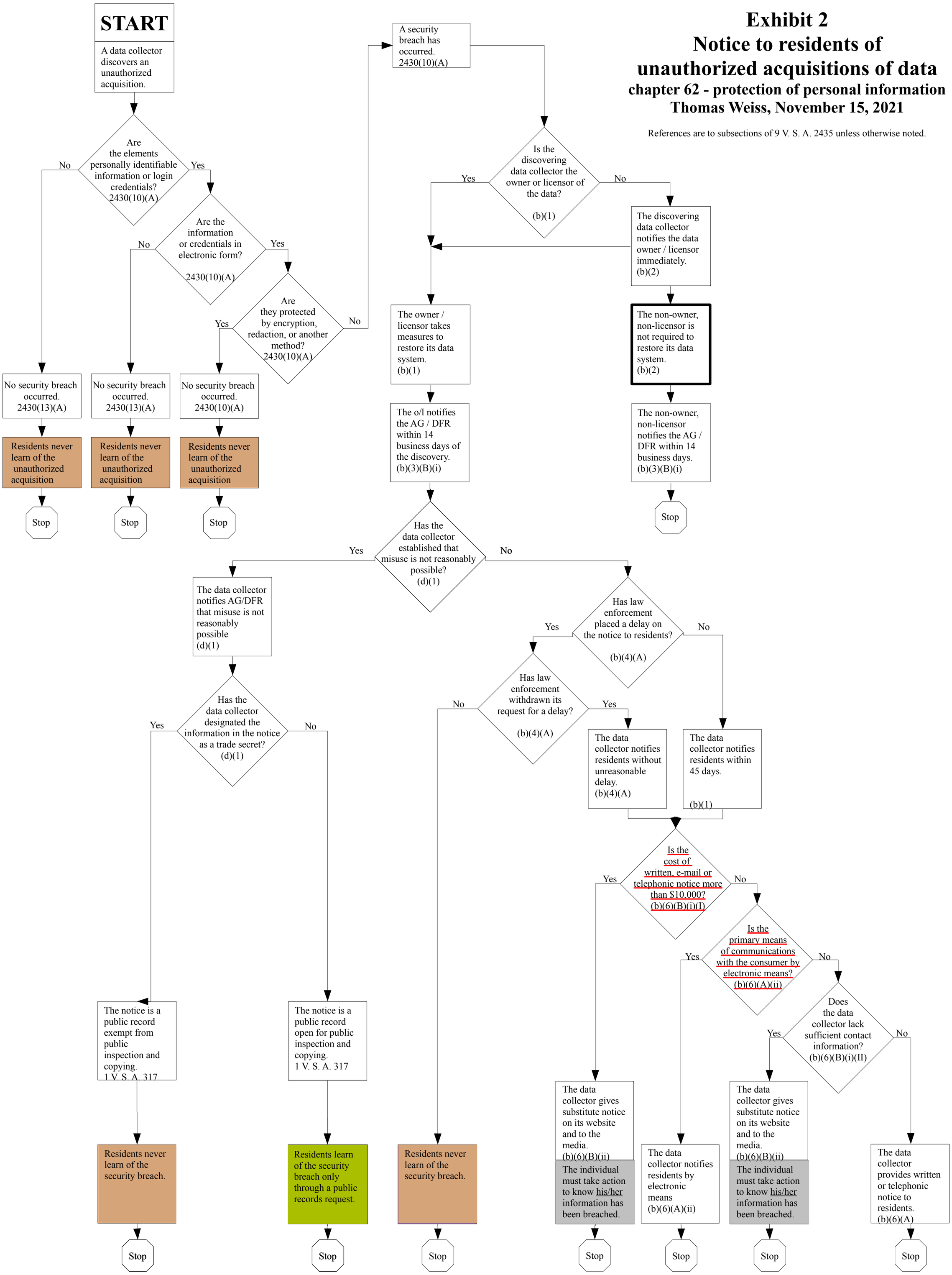
data element	PII	BPI	CI	PI
credit report	no	no	no	no
internet browsing history	no	no	no	no
online purchases	no	no	no	no
location data	no	no	yes	no
loyalty programs	no	no	no	no
subscription information	no	no	no	no

Vermont requires notice to consumers only for the unauthorized acquisition of PII (personally identifiable information) , and only in some cases. Vermont does not require notice to consumers for unauthorized acquisition of all other information.

PII - personally identifiable information
LC - login credentials
BPI - brokered personal information
CI - covered information
SSN - social security number protection
PI - personal information

Exhibit 2
Notice to residents of unauthorized acquisitions of data
chapter 62 - protection of personal information
Thomas Weiss, November 15, 2021

References are to subsections of 9 V. S. A. 2435 unless otherwise noted.



MAYER | BROWN

Mayer Brown LLP
350 South Grand Avenue
25th Floor
Los Angeles, CA 90071-1503
United States of America

T: +1 213 229 9500
F: +1 213 625 0248

mayerbrown.com

Philip Recht
Partner
T: +1 213 229 9512
F: +1 213 576 8140
PRecht@mayerbrown.com

December 6, 2021

BY U.S. MAIL AND EMAIL

The Honorable Thomas J. Donovan, Jr.
Attorney General of Vermont
Attn: My-Lanh Graves
109 State Street
Montpelier, VT 05609

State of Vermont Department of Public Service
Attn: Commissioner June E. Tierney
112 State Street
Montpelier, VT 05620-2601

Re: Vermont Data Privacy Working Group

Dear Attorney General Donovan and Commissioner Tierney:

Our firm represents a coalition of companies (i.e., Spokeo, PeopleFinders, MyLife, Truthfinder, BeenVerified, and PeopleConnect) that provide background check, fraud detection, and other people search services. Our clients qualify as "data brokers" under Vermont law and are registered as such. We have participated in, and are grateful for, the privacy hearings held by your offices, as well as the opportunity to submit these written comments. We write to address a single issue of paramount concern in any comprehensive data privacy law, namely, the protection of publicly available data as free speech under the U.S. constitution.

I. Our clients. Our clients provide background check, fraud detection, and other people search services. They do so, like others in the data industry, by collecting data mostly from publicly available sources, organizing the data into usable products (such as reports), and offering the reorganized data for sale to customers. Unlike businesses that collect personal information directly from consumers and then sell that information, our clients collect the information they sell only from third-party sources.

Our clients' services are widely used and highly valued by an array of public and private entities and individuals. Law enforcement agencies use the services to identify and locate suspects and witnesses, and to serve subpoenas. Welfare agencies use the services to find parents evading child support awards. The Veterans Administration uses the services to locate next-of-kin of fallen soldiers. Businesses use the services to detect order fraud, and update customer and prospect databases. Consumers use the services to find lost relatives and friends, plan family reunions, check out relationship prospects and online marketplace sellers, and to root out scams.

Mayer Brown is a global services provider comprising an association of legal practices that are separate entities including Mayer Brown LLP (Illinois, USA), Mayer Brown International LLP (England), Mayer Brown (a Hong Kong partnership) and Tauil & Chequer Advogados (a Brazilian partnership).

II. Our comments. Our clients support the enactment of comprehensive data privacy laws. Clear and consistent data privacy practices not only protect consumers, but benefit businesses through enhanced consumer trust and stable compliance regimes. Indeed, our clients supported California's data broker registration law, working closely with its author from introduction to enactment in 2019, and our clients are registered as data brokers in both California and Vermont. Moreover, our clients have long voluntarily provided rights such as opt-out that have been made mandatory by recently enacted laws in California, Virginia, and Colorado. Our comments are meant to inform the Working Group and Vermont Legislature and to ensure any potential data privacy laws are constitutionally sound and align with laws enacted in other states.

Protection for publicly available data is of paramount importance in any data privacy law or regulation, owing to venerable Constitutional principles and established Supreme Court precedent. The First Amendment prohibits laws that abridge freedom of speech. Commercial speech—i.e., speech that proposes a commercial transaction (e.g., a billboard advertisement)—may be limited by laws that are necessary to directly advance a substantial government interest. *Cent. Hudson Gas & Elec. Corp. v. Pub. Serv. Comm'n of New York*, 447 U.S. 557, 566 (1980).

However, content-based restrictions on non-commercial speech, such as on the use and sale of consumer information that has already entered the public domain, are presumptively unconstitutional and may only be allowed if they meet the so-called "strict scrutiny test"—i.e., if they are narrowly tailored to promote a compelling government interest. *United States v. Playboy Entm't Grp., Inc.*, 529 U.S. 803, 813 (2000); *see also Sarver v. Chartier*, 813 F.3d 891, 903 (9th Cir. 2016) (holding that statute that restricts the commercial use of people's personal identifying information "clearly restricts speech based upon its content").

Assumedly in recognition of these constitutional protections, the Data Broker Law excludes from the definition of "personally identifiable information" (PII), and thus from the law's scope, "publicly available information that is lawfully made available to the general public from federal, State, or local government records." 9 V.S.A. § 2430(10)(B). The Law further exempts "publicly available information to the extent that it is related to a consumer's business or profession" from the definition of "brokered personal information" (BPI). 9 V.S.A. § 2430(1)(B).

These definitions would need to be the starting point for any comprehensive data privacy law or amendment to the Data Broker Law considered by the Legislature. But any law or amendment expanding restrictions on the use and sale of PII equally would need to expand its definitions and protections for public available data, which, as a constitutional matter, includes far more than government records.

The Data Broker Law does not restrict the use and sale of PII or BPI, except when used or acquired for fraud, unlawful discrimination, stalking, or harassment. 9 V.S.A. § 2431(a). Such narrowly drawn prohibitions in furtherance of a compelling interest in curtailing fraud, discrimination, and harassment arguably satisfy the strict scrutiny test and the First Amendment, even if they sweep in publicly available data beyond government records, as the Data Broker

Law otherwise only imposes registration, information security, and breach notification requirements (without restricting use or sale for other purposes).

However, any comprehensive restrictions on the use and sale of PII for less pernicious purposes would need to encompass two categories of constitutionally protected public data beyond government records, specifically, information lawfully made available to the general public (1) by the consumer or from widely distributed media (e.g., a newspaper, TV or radio program), and (2) by a person to whom the consumer has disclosed the information without restriction to a specific audience (e.g., a public Facebook page). Indeed, the comprehensive laws now enacted in California, Virginia, and Colorado, as well as the Uniform Personal Data Protection Act (UPDPA) drafted by the Uniform Law Commission (ULC),[1] all protect and exempt each of these three categories of publicly available data.

The need to exempt publicly available information, and the risk posed to laws that do not, is reflected in the history of the California privacy laws. As initially enacted in 2018, the California Consumer Privacy Act (CCPA)—like the Data Broker Law—exempted only government record data publicly available information.[2] The California Privacy Rights Act (CPRA), enacted in 2020, was intended to strengthen the consumer protections, and otherwise remedy the perceived flaws, in the CCPA. Foremost among those perceived flaws was the limited nature of the CCPA's public data exemption. Since this improper limitation was rooted in definitional provisions that, if successfully challenged in court, could not be easily severed from the rest of the CCPA, the CCPA's proponents feared this flaw could lead to the invalidation of the CCPA in its entirety.

To cure the problem, the CPRA amended the CCPA to provide that "'personal information' does not include publicly available information **or lawfully obtained, truthful information that is a matter of public concern**;" and further, that publicly available information means:

> "information that is lawfully made available from federal, state, or local government records**, or information that a business has a reasonable basis to believe is lawfully made available to the general public by the consumer or from widely distributed media…; or information made available by a person to whom the consumer has disclosed the information if the consumer has not restricted the information to a specific audience**."

Cal. Civ. Code § 1798.140(v)(2) (revisions to former section 1798.140(o)(2) in bold).

---

[1] The ULC, also known as the National Conference on Commissioners on Uniform State Laws, is comprised of retired judges, law professors, and practicing attorneys representing all 50 states. It is perhaps best known for developing the Uniform Commercial and Uniform Probate Codes. A committee of the ULC began its work on the model state privacy law in 2019, and the full ULC approved the UPDPA in July 2021. The UPDPA already has been proposed as legislation in Washington, D.C.

[2] Specifically, the CCPA only exempted publicly available data that was "lawfully made available from federal, state, or local government records." Cal. Civ. Code Sec. 1798.140(o)(2).

The recently enacted Virginia Consumer Data Protection Act (VCDPA), the first comprehensive data privacy law enacted by a state after California, similarly excludes not only government records data but also data voluntarily made available by consumers and through widely distributed media. Specifically, the VCDPA provides that "publicly available data" exempt from regulation under the law includes:

> "information that is lawfully made available through federal, state, or local government records, or information that a business has a reasonable basis to believe is lawfully made available to the general public through widely distributed media, by the consumer, or by a person to whom the consumer has disclosed the information, unless the consumer has restricted the information to a specific audience." VA Code section 59.1-571.

Likewise, the Colorado Privacy Act (CPA) enacted in July 2021 defines (and exempts) publicly available information as "information that is lawfully made available from federal, state, or local government records and information that a controller has a reasonable basis to believe the consumer has lawfully made available to the general public" (Col. Rev. Stat. section 6-1-1303(17)(b)), and defines "sale" to exclude (among other things) information "intentionally made available by the consumer to the general public via a channel of mass media" (Col. Rev. Stat. section 6-1-1303 (23)(b)(V)(B)). This latest data privacy law thus aligns with the prior laws in Virginia and California.

The ULC's UPDPA contains a similar, though more illustrative, definition of publicly available data. The UPDPA's drafters explain in comments to the model law that "[t]he processing of publicly available information is excluded from the act" because "[t]here are significant First Amendment implication for placing limits on the use of public information." Sec. 3 cmt. As such, section 2(15) of the UPDPA provides:

> "'Publicly available information' means information: (A) lawfully made available from a federal, state, or local government record; (B) available to the general public in widely distributed media, including: (i) a publicly accessible website; (ii) a website or other forum with restricted access if the information is available to a broad audience; (iii) a telephone book or online directory; (iv) a television, Internet, or radio program; and (v) news media; (C) observable from a publicly accessible location; or (D) that a person reasonably believes is lawfully made available to the general public if: (i) the information is of a type generally available to the public; and (ii) the person has no reason to believe that a data subject with authority to remove the information from public availability has directed the information to be removed."

For all of these reasons, we strongly request and recommend that any comprehensive data privacy law proposal, or amendment to the Data Broker Law imposing additional restrictions on the use and sale of personal information, exclude constitutionally protected, public domain data. Doing so would align such proposals with the California, Virginia, and Colorado privacy laws and any laws patterned thereon or on the UPDPA—thus serving to create uniformity among the major state privacy laws. As important, appropriately protecting publicly available data would eliminate a significant risk of legal invalidation in any proposed law or amendment.

We hope this information is helpful. Please let us know if you have any questions about it. Otherwise, we would welcome the opportunity to speak to you further about the issues discussed herein.

Yours sincerely,

Philip Recht
Partner

TECHNET
THE VOICE OF THE
INNOVATION ECONOMY

TechNet Northeast | Telephone 774.230.6685
One Beacon Street, Suite 16300, Boston, MA 02108
www.technet.org | @TechNetNE

November 15, 2021

Attorney General TJ Donovan
109 State Street
Montpelier, VT 05609

Re: Biometric Privacy Legislation

Dear Attorney General Donovan and Staff:

I write to provide comments regarding Illinois' Biometric Information Privacy Act (BIPA) as part of your office's series of privacy forums. Respectfully, BIPA is the wrong model for Vermont. The law, passed in Illinois in 2008, has resulted in a deluge of devastating, frivolous lawsuits with little benefit to consumers or their privacy rights.

TechNet is the national, bipartisan network of technology CEOs and senior executives that promotes the growth of the innovation economy by advocating a targeted policy agenda at the federal and 50-state level. TechNet's diverse membership includes dynamic American businesses ranging from startups to the most iconic companies on the planet and represents over four million employees and countless customers in the fields of information technology, e-commerce, the sharing and gig economies, advanced energy, cybersecurity, venture capital, and finance. TechNet has offices in Austin, Boston, Chicago, Denver, Olympia, Sacramento, San Francisco, Silicon Valley, and Washington, D.C.

TechNet believes that privacy laws should provide strong safeguards for consumers, while allowing the industry to continue to innovate. We respect your office's interest in protecting the data of Vermonters, but any recommended legislation based on BIPA will be fundamentally flawed. BIPA does not identify and protect against specific privacy harms, instead utilizing a definition of "Biometric identifier" that is overbroad and difficult to implement, which, paired with a private right of action, would open the floodgates to costly litigation against well-meaning Vermont businesses and stifle innovation in the state.

In Illinois, BIPA has been used as a cudgel by class-action law firms seeking large payouts from companies leveraging this technology to benefit consumers, or in many cases from providers of support systems that never even interact with consumers. The net effect of BIPA in IL has been to create a cottage industry of class action law firms and to prevent companies and consumers from developing or accessing pro-consumer, pro-privacy uses of biometric data like building security, user authentication, fraud prevention, and more.

TECHNET
THE VOICE OF THE
INNOVATION ECONOMY

Vermont residents and employers deserve privacy protections that safeguard sensitive data while promoting innovation, security, and job creation. We would welcome the opportunity to work with your office to address issues of privacy protection without these severe unintended consequences. Please consider TechNet's members a resource in this effort.

Thank you for your consideration of this testimony. We hope that any recommendations from your office recognize the fatal flaws of BIPA and do not import them to the Green Mountain State. Please do not hesitate to contact me if I can provide any additional information.

Sincerely,

Christopher Gilrein
Executive Director, Northeast
TechNet
cgilrein@technet.org

TECHNET
THE VOICE OF THE INNOVATION ECONOMY

TechNet Northeast | Telephone 774.230.6685
One Beacon Street, Suite 16300, Boston, MA 02108
www.technet.org | @TechNetNE

November 15, 2021

Attorney General TJ Donovan
109 State Street
Montpelier, VT 05609

Re: Comprehensive Data Privacy Legislation

Dear Attorney General Donovan and Staff:

I write on behalf of TechNet's member companies to provide comments regarding comprehensive data privacy legislation as part of your office's series of privacy forums.

TechNet is the national, bipartisan network of technology CEOs and senior executives that promotes the growth of the innovation economy by advocating a targeted policy agenda at the federal and 50-state level. TechNet's diverse membership includes dynamic American businesses ranging from startups to the most iconic companies on the planet and represents over four million employees and countless customers in the fields of information technology, e-commerce, the sharing and gig economies, advanced energy, cybersecurity, venture capital, and finance. TechNet has offices in Austin, Boston, Chicago, Denver, Olympia, Sacramento, San Francisco, Silicon Valley, and Washington, D.C.

Our member companies place a high priority on consumer privacy. The technology industry is fully committed to securing privacy and security for consumers and engages in a wide range of practices to provide consumers with notice, choices about how their data is used, as well as control over their data. TechNet supports a federal standard that establishes a uniform set of rights and responsibilities for all Americans. The global nature of data demands a federal policy, and even the most well-designed state statute will ultimately contribute to a patchwork of different standards across the country, resulting in steep compliance costs and consumer confusion.

In the absence of a uniform standard, TechNet urges states considering their own legislation to consider interoperability with existing models as the default position. Each new concept or definitional change could result in consumer confusion and significantly increase compliance costs for businesses. The California Department of Finance in 2019 estimated the one-time compliance costs of the state's first privacy law at over $55 billion. Small and midsize companies face $50,000-$100,000 to come into compliance with vague and ever-changing requirements.

TechNet members believe that privacy legislation should connect specific remedies to specific privacy harms. A truly effective privacy law is as explicit as possible – it should be clear what is expected of companies and what rights consumers can avail themselves of. The California process left significant details and crucial definitions to be determined through subsequent rulemaking procedures and additional legislation. More recent experiences in states like Virginia show the value of clearly outlining what lawmakers determine to be riskier practices and the necessary compliance procedures those practices require.

TechNet believes that Attorney General enforcement of state privacy policies ensures that justice is meted out fairly and uniformly, and that enforcement actions target real and intentional harms. A private right of action – even in limited cases as in the California statute - could result in ruinous liability for Vermont companies for even unintentional violations. Time and time again, we have seen private rights of action in privacy statues leveraged to extract significant settlements from companies with little or no actual value delivered to the consumer. Conversely, a July report from the CA Attorney General's office reported that 75% of companies notified of an alleged violation came into compliance within the statutory cure period. The remaining 25% were either still within the cure period at the time of the report or were under active investigation. The statutory grace period allows the office to target its resources to actors causing real harm while allowing companies the opportunity to come into compliance without the cost and delay of litigation.

Thank you again for your consideration of TechNet's policy principles regarding data privacy legislation. Please consider TechNet's member companies a resource as your office continues to develop recommendations to the Legislature.

Sincerely,

Christopher Gilrein
Executive Director, Northeast
TechNet
cgilrein@technet.org

COALITION FOR GENETIC DATA PROTECTION

November 18, 2021

Charity Clark
Ryan Kriger
Vermont Attorney General Office
109 State Street
Montpelier, Vermont 05609

RE: Potential Vermont Biometric Data Privacy Act

Dear Ms. Clark and Mr. Kriger –

On behalf of The Coalition for Genetic Data Protection[1], a national coalition of the leading consumer genetic testing companies including 23andMe and Ancestry – we are writing to offer our thoughts on a potential Vermont Biometric Information Privacy Act, particularly as it pertains to genetic information.

Our companies have always carefully considered the privacy and data protection issues incumbent with direct-to-consumer genetic testing services, and we support having safeguards in place that ensure consumers are aware of our privacy practices, have control over their data, and have the opportunity to provide affirmative consent before their data is shared – regardless of which genetic testing service they use.

We have developed model language based on the Future of Privacy Forum's *Privacy Best Practices for Direct-to-Consumer Genetic Testing Services* – a document that has broad support across industry, consumer and privacy advocates, and other key stakeholders on Capitol Hill. That model bill requires all the following:

- Separate express consent before DNA is extracted from a biological sample and analyzed.
- Separate express consent before a biological sample is stored.
- Separate express consent for genetic data to be used for research purposes.
- Separate express consent for genetic data to be shared with a third party.
- Separate express consent for genetic data to be used for marketing purposes.
- Genetic testing companies to not share genetic data with employers or providers of insurance for any reason.
- Genetic testing companies to provide consumers with a means to delete their genetic data from their database and close their accounts without unnecessary steps.
- Genetic testing companies to delete a consumer's biological sample within 30 days of a request.
- Genetic testing companies to provide clear and complete information about their privacy practices and protocols.

In considering a potential law in Vermont to address biometric data privacy, we strongly urge the exclusion of DNA and genetic information from any such legislation. Our companies are

[1] https://geneticdataprotection.com/

CGDP

not opposed to having genetic data privacy regulated; however, genetic data is used in a very different context than the other technologies that fall under the umbrella of biometric data. Specifically, genetic data is not used to:

- Unlock a personal phone or computing device
- Gain access to a secured building
- Identify individuals in photographs or video in a public setting

Retina scans, facial recognition, fingerprint identification and so on are used in an immediate way to identify individuals, sometimes without their consent or knowledge. Genetic data from direct-to-consumer genetic testing services, on the other hand, is never used in an immediate manner to identify an individual for any of those contexts. Thus, requiring genetic data to be assessed for disparate outcomes or to restrict its utilization in such contexts would not be necessary.

The only state to enact a Biometric Information Privacy Act so far is Illinois. In that case, DNA and genetic data were **not** included in the scope of the BIPA law. Rather, Illinois enacted a parallel bill – the Genetic Information Privacy Act – to deal with the privacy concerns incumbent with DNA and genetic data separately. While we have concerns with the enforcement mechanisms in the Illinois statutes, we agree that keeping biometric data and genetic data separate is the correct approach.

Our Coalition is eager to work with Rep. Barbara Rachelson and your office to amend her short form bill (H.233) with our model legislation referenced above. This approach has broad consensus among regulators, industry, and consumer and privacy advocates alike. It has received bipartisan support in states as conservative as Arizona and Utah and as progressive as California. If passed in Vermont, it would afford your citizens the strongest privacy protections for genetic data as the consent requirements in our model go further than both HIPAA and the Common Rule.

We are proud of the work we have undertaken to provide our customers with straightforward privacy policies that empower them to control how their genetic data is used. We thank you for your leadership on this important issue and appreciate the productive engagement we have had with you and your staff. We hope that we can enact a strong, privacy protective measure in Vermont for genetic data in the coming session.

Sincerely,

Eric Heath
Chief Privacy Officer
Ancestry

Jacquie Cooke Haggarty
VP, Deputy General Counsel & Privacy Officer
23andMe