6 Wayne St. U. J. Bus. L. 1

Wayne State University Journal of Business Law
2023
Michelle Mayfield
The Journal of Business Law
Wayne State University Law School

TALK DATA TO ME: WHY MICHIGAN SHOULD ADOPT A COMPREHENSIVE DATA PROTECTION STATUTE

***2 TABLE OF CONTENTS**

***3 I. INTRODUCTION**

In today's economy, the reliance on data has increased astronomically. From e-commerce to cryptocurrency, the use of data is becoming a key part of our businesses and our culture. This is the case in Michigan, where the state is seeing an increase in jobs from technology companies. [1] Despite the growth of data in our economy, there is currently no federal comprehensive data protection law. In 2016, the European Union (EU) Parliament passed the General Data Protection Regulation (GDPR), [2] which provides increased privacy protections for individuals and new regulations for businesses, public entities or persons that process personal data. Since the passage of the GDPR, states across the U.S. have passed comprehensive data protection legislation, as have other countries. [3]

In the U.S., California was the first state to pass comprehensive data privacy legislation. [4] This legislation led to the passage of additional statutes in Virginia [5] and Colorado. [6] This trend ***4** continued as Utah [7] and Connecticut [8] passed laws mirroring the statutes in Virginia and Colorado. In July 2021, the Uniform Law Commission (ULC) revealed the Uniform Personal Data Protection Act (UPDPA), a uniform privacy statute geared towards eliminating the ever-growing patchwork of state privacy laws in the U.S. [9] However, the ULC's proposed law has not been widely adopted and is still in the early stages. It also faces

challenges where businesses and state legislatures are more familiar with other statutes such as the GDPR and California's privacy bill.

As various states consider adopting their own legislation, there has been growing pressure on the U.S. Congress to create an overarching federal data privacy standard. In the Summer of 2022, the American Data Privacy and Protection Act (ADPPA) advanced out of the House Energy and Commerce Committee. [10] Members on both sides of the aisle supported the bill but it did not become law during the 117th Congress. The proposed law reached an impasse due to a lack of support from key members of Congress such as Senator Maria Cantwell and the California Congressional delegation. [11] A major stumbling block has been the issue of ***5** preemption, where there are conflicting opinions about whether national legislation should be considered a ceiling or a floor. [12]

This article will explain why Michigan should adopt a comprehensive data privacy statute as soon as possible. There is growing momentum across the country as more states are drafting their own comprehensive data privacy laws. [13] Both chambers of the Michigan legislature introduced their own data privacy bills. In April 2022, Michigan House Democrats introduced the Michigan Consumer Privacy Act. [14] A few months later, Michigan Senate Democrats introduced the Michigan Personal Data Privacy Act. [15] Neither bill made it out of their referred committees but they still have a chance to be reintroduced in the 2023 legislative session.

This note will begin by providing a brief overview of the provision that changed the trajectory of data privacy: GDPR. Then the note will address the various options that Michigan could replicate. These options include various state statutes across the country and the UPDPA. The note will also address the possibility of the passage of a federal comprehensive data privacy statute. The note will then provide an analysis on each of these options, explaining the relevant considerations involved in both drafting a statute or maintaining the status quo and waiting for the federal government to act. The note will conclude by providing the best option for Michigan to take moving forward.

***6 II. BACKGROUND**

A. The Paradigm: The General Data Protection Regulation

The EU has historically regulated the use of personal data by private companies. In 1995, the European Data Protection Directive was passed to address privacy and human rights. [16] This directive went into effect on October 24, 1998, and was the main law addressing the processing of personal data for over a decade. [17] On May 19, 2009, the European Commission contemplated the possibility of creating a new privacy law addressing the ongoing challenges with data protection in an increasingly globalized world. [18] Over the next six years, various stakeholders in the EU discussed and negotiated the creation of a new provision managing the processing, sale, and use of personal data. [19] Through this process, the GDPR was formed, receiving overwhelming support from members of the Permanent Representatives Committee. [20] In April 2016, after the EU Parliament passed the GDPR, it was adopted by the EU and went into effect on May 25, 2018. [21]

This statute was revolutionary because it was the first to address the use of data in a comprehensive way. The GDPR places individuals in the driver's seat, empowering them to monitor the use of their data and putting the onus on data holders (called "controllers") to make sure that they have a legal basis to collect personal data, often through the individuals' consent. ***7** Individual rights include but are not limited to the right to access data, the right to be forgotten (i.e., deletion), and the right for consumers to ask that their data be corrected. [22] The GDPR primarily protects citizens of European Union member-states, but businesses across the world are required to comply with this regulation as well. [23] Specifically, the GDPR applies to:

> 1) the processing of personal data in the context of an establishment of a controller or a processor in the Union, regardless of whether the process takes place in the Union or not

> 2) the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to
>
> a. the offering of goods or services, irrespective of whether a payment of the data subject is required to such data subjects in the Union, or
>
> b. the monitoring of their behavior as far as their behavior takes place within the Union
>
> 3) the processing of personal data by a controller not established in the Union, but in a place where Member State law applies by virtue of public international law [24]

This means that if a business provides services to a citizen of the EU, then they have to comply with the regulation.

The GDPR has since put pressure on businesses across the world, including in the United States. Many businesses have hired data protection officers and firms that specialize in creating data breach response plans to ensure compliance with this regulation. [25] The GDPR also set the stage for new debates on consumer privacy in the U.S. After the GDPR passed, California created its own comprehensive data privacy scheme.

*8 *B. The California Model*

The California Consumer Privacy Act (CCPA) went into effect on January 1, 2020. [26] This statute is the first of its kind in the United States, and it originated as a ballot initiative. It requires companies to notify users regarding the monetization and use of their data. [27] The CCPA principally applied to entities that conduct business in California and either processed the data of at least 50,000 consumers or made annual gross revenues in excess of 25 million dollars in the proceeding calendar year. [28] Businesses are required to disclose the information they collect to consumers, what information they share with third parties, if any, and the consumer's rights to delete their data, among other requirements. [29] In addition to these rights, California deviates from other privacy legislation by granting consumers a private right of action. [30] This action is limited, however, to consumers bringing a data breach claim against companies. [31]

In November 2020, California voters approved the California Privacy Rights Act (CPRA), a second ballot initiative addressing potential shortfalls of the CCPA. [32] The CPRA makes significant changes to the CCPA, impacting both businesses and consumers. The changes in the CPRA include alterations to the threshold requirements for businesses subject to the statute (such ***9** as increasing the processing threshold for businesses to 100,000 consumers or more), expanding the definition of personal information, and creating a new concept called "sharing" to close a perceived loophole where data was transferred to third parties for consideration other than money. [33] Additionally, the CPRA requires relevant businesses to monitor the personal information that is shared amongst third parties in the context of behavioral advertising. [34] The CPRA also creates the California Privacy Protection Agency (CPPA), the first of its kind in the state dedicated to privacy enforcement. [35] The CPPA is governed by a five-member board and will enforce the CPRA, assess administrative fines, and advise the California Legislature on privacy-related legislation. [36] The CPRA is now in effect as of January 1, 2023, effectively replacing the CCPA. [37]

C. The Virginia/Colorado Model

Following the passage of the CCPA, the Virginia Consumer Data Protection Act (VCDPA) and the Colorado Privacy Act (CPA) became law.

When Governor Ralph Northam signed the VCDPA into law on March 2, 2021, Virginia became the second state to enact a comprehensive privacy statute.[38] This legislation applies to entities that conduct business in Virginia.[39] The legislation also applies to entities that produce ***10** products or services that target Virginia residents.[40] This legislation will provide consumers the right to opt-out of having their personal data processed for targeted advertising, similar to the CCPA.[41] This law also applies to businesses that control or process the data of at least 100,000 consumers annually, or collect more than 50 percent of gross revenue from the sale of personal data while processing the personal data of at least 25,000 consumers.[42] A key distinction between the Virginia bill and the California bill is the lack of any private right of action.[43] Instead, the VCDPA provides the state's Attorney General with exclusive enforcement authority.[44]

On July 8, 2021, Governor Jared Polis signed the CPA into law, becoming the third U.S. state to enact comprehensive privacy legislation.[45] This statute is similar to the CCPA and VCDPA in that the bill applies to entities that conduct business in the state and/or provide products and services to the residents of Colorado.[46] However, the CPA differs from both the CCPA and the VCDPA because it applies to both for-profit and not-for-profit organizations while the other bills do not.[47]

***11** A key distinction between the CPA (and the VCDPA[48]) from California's statute is that the CPA does not include any revenue thresholds.[49] Another notable distinction is the lack of a private right of action for consumers (just like the VCDPA).[50] Instead, the Colorado Attorney General will handle all cases against businesses on behalf of consumers.[51] The CPA provides five main rights to consumers: 1) right of access, 2) right to correction, 3) right to delete, 4) right to data portability, and 5) right to opt-out.[52] The CPA will go into effect in July 2023 while the CPRA and the VCDPA are now in effect.[53]

D. The Uniform Model

Since 2019, the ULC has been working on a draft uniform data privacy statute. This uniform statute became available to state legislatures in early 2022, with some states introducing the bill in their respective legislative bodies.[54] Harvey Perlman, the Chair of the UPDPA Committee, explained that the purpose of this uniform statute is to balance the interests of consumers and businesses.[55] Mr. Perlman also recognized that we are currently ***12** living in a data economy and that the purpose of this bill is not to "disrupt the economy," but to recognize the various benefits of business data practices.[56] Finally, Mr. Perlman emphasized the importance of creating a statute that would not be impracticable for businesses to implement. He explained that if the statute is not onerous on businesses, then it is likely that businesses would comply and that more consumers would be protected.[57]

The UPDPA uses different terms when addressing consumer privacy. For instance, the bill addresses two types of controllers: collecting controllers and third-party controllers.[58] Collecting controllers are the entities that receive personal data directly from data subjects.[59] Third-party controllers collect the data from the collecting controllers and then determine the purpose and means of any additional processing of this data.[60]

Moreover, the UPDPA provides rights to consumers similar to those of other statutes such as the right to access and correct any data about them online.[61] The UPDPA also provides states with the latitude to decide whether consumers should have a private right of action.[62] At the same time, the UPDPA operates under the assumption that the states' Attorneys General will lead enforcement efforts and that any claim addressing data privacy will be brought under the states' consumer protection act.[63]

***13** However, the UPDPA has several distinctions from its data privacy counterparts. First, consumers do not have the right to request that businesses delete their data. [64] Jane Bambauer, a Reporter for the UPDPA Committee, explained that the committee made this decision because it was concerned about creating a broad deletion right. [65] She also expressed concern with a lack of guidance from the U.S. Supreme Court on the applicability of statutes that provide these broader protections, such as the CCPA. [66] Second, the UPDPA requires the creation of voluntary consent standards. [67] These standards are not equivalent to industry standards. Instead, voluntary consent standards are procedures created and overseen by the various stakeholders involved in data privacy. [68] This process is meant to mirror federal operations of data privacy statutes, such as the Children's Online Privacy Protection Act. [69]

Third, this proposed uniform law creates three categories of data practices that businesses need to be aware of: compatible, incompatible, and prohibited. [70] This tripartite system is different from other state statutes because the drafters determined that some data practices can be used without consumer consent (i.e., compatible), while other data practices should be barred, even if there is consent (i.e., prohibited). [71] Incompatible data practices address a middle ground of novel data uses. [72] If a data practice is considered incompatible, it may be ***14** permitted if there is some sort of notice. [73] Finally, the UPDPA does not allow consumers to opt-out of behaviorally targeted advertising (which is a major contrast from the other state privacy laws). [74] The Committee stressed the importance of not disrupting the economy and was not willing to ban a practice without knowing how it could impact the status quo. [75]

E. The Federal Model

A final option for Michigan to consider is doing nothing. Michigan could forego pursuing a state comprehensive bill in favor of federal regulation. Since the passage of the GDPR and the CCPA, members of Congress have proposed several comprehensive data privacy bills. Previous legislative proposals have been pushed on partisan lines, such as the Consumer Online Privacy Rights Act (COPRA) [76] and the Setting an American Framework to Ensure Data, Access, Transparency, and Accountability (SAFE Data) Act. [77]

However, in June 2022, the House Energy and Commerce Committee introduced the ADPPA. [78] The ADPPA was believed to be broader than the current state privacy bills, including the CPRA. [79] For instance, the most recent version of the statute covers data (i.e., information), that "is linked or reasonably linkable, alone or in combination with other ***15** information," to a particular person or entity. [80] Additionally, the ADPPA would apply to any entity, company, and/or nonprofit organization that is subject to the Federal Trade Commission (FTC) Act. [81] The inclusion of nonprofit organizations is an important change since nonprofits are typically not subject to the FTC Act. [82]

Moreover, the ADPPA classifies some entities as either large data holders or third-party collecting entities. [83] Large data holders are covered entities or service providers that recently had annual gross revenue of $250 million or more and either collected, processed, or transferred the covered data of more than 5 million individuals or devices along with the sensitive covered data of more than 200,000 individuals. [84] Third-party collecting entities are entities whose main source of revenue comes from "processing or transferring the covered data that the covered entity did not collect directly" from the individuals associated with the data. [85] Additionally, small businesses may qualify as covered entities under the ADPPA, contrary to current state privacy laws. [86]

Members of the House Energy and Commerce Committee voted 53-2 in favor of the ADPPA. [87] In the bill's most recent form, most state privacy laws (with the exception of ***16** Illinois' Biometric Privacy Act (BIPA) and the private right of action provided by the CCPA for certain types of data breaches, among other laws governing nuanced data issues) would be expressly preempted. [88] This means that if the ADPPA becomes law, virtually all state data privacy laws would become moot. Finally, if

the ADPPA is passed, the regulations will largely be enforced by the FTC and State Attorneys General. [89] However, pending passage, the ADPPA would allow individuals to bring a private right of action two years after the law is in effect. [90]

III. ANALYSIS

A. The Federal Model

Many data privacy practitioners believe that the best way to resolve our current data privacy conundrum is for Congress to create a federal standard. Advocates of a federal standard have explained that a federal statute would do two things: 1) provide consumers with more control over their personal data and 2) be able to comply with the requirements of international data privacy regulations such as the GDPR. [91] Additionally, proponents of a federal standard believe it will simplify compliance for businesses by getting rid of the hodgepodge of state statutes. [92]

However, these proponents are not acknowledging that there is precedence for states to create laws addressing data where no comparable federal law exists. In the early 2000s, California ***17** became the first state to adopt a data breach notification statute. [93] As of 2022, all 50 states, the District of Columbia, Guam, Puerto Rico, and the Virgin Islands have data breach notification laws. [94] These laws have similar provisions such as who must comply with the law, the method of notice, and what constitutes a breach. [95] Yet some states have distinct provisions such as requiring notification of breaches involving non-encrypted information (e.g., New York) or requiring companies to notify affected individuals within a particular timeframe, such as 30 days (e.g., Florida) or 60 days (e.g., Delaware). [96] Even though there are some differences in how the states enforce these laws, the main purpose is the same: to require companies to notify affected individuals of data breaches. The data breach notification laws created a precedent for a 50-state model outside of the federal government. This shows that laws involving data can operate without the need for a federal statute. States can create laws to protect their own citizens without waiting for the federal government to intervene. This is often necessary because the increasing gridlock in Congress prevents well-meaning bipartisan laws from moving forward.

Even though the House Energy and Commerce Committee voted in favor of the ADPPA, the bill was stalled due to a lack of support from Senator Maria Cantwell, Chair of the Committee on Commerce, Science, and Transportation. [97] Senator Cantwell would only support the ADPPA if ***18** there were tougher enforcement actions included such as limits on forced arbitration and a private right of action equivalent to California's law. [98] Additionally, the California delegation opposed the ADPPA because if passed, it would preempt California's data privacy laws, which the California delegation claimed were more stringent than ADPPA. [99] There have been no hearings or bill markups in the Senate since the ADPPA committee vote in the House. [100]

As Congress convenes for a new legislative session in 2023, it seems unlikely that the ADPPA will pass in its most recent form. [101] The remainder of the 117th Congress has focused on funding the government, codifying the rights to same-sex and interracial marriage, and passing the National Defense Authorization Act (NDAA). [102] The top legislative priorities for 2023 include resolving the impending debt ceiling to prevent the U.S. from going into default and passing the Farm Bill before it expires at the end of the year. [103] Technology advocates have low expectations for substantive congressional action on data privacy laws in 2023. [104] In fact, many believe that a comprehensive federal privacy statute such as the ADPPA is unlikely to move forward due to the key differences between Democrats and Republicans and the inability of both parties to come to a compromise. [105]

***19** Even as Congress was drafting and debating the ADPPA, other states passed their own comprehensive data privacy laws. In March and May of 2022, Utah [106] and Connecticut [107] became the fourth and fifth states to enact their own respective consumer data privacy laws. New Jersey, Ohio, and Pennsylvania are among other states that have proposed their own data privacy statutes and referred them to the appropriate committees. [108] Therefore, Michigan should not be deterred by the prospect of a federal data privacy standard and should pass their own law instead.

B. The Ideal Michigan Statute

Creating a comprehensive data privacy statute is important for Michigan since our economy is transitioning to a data-based one that relies on the use, collection, and sharing of data. Michigan is slowly transitioning toward becoming a new technology hub, attracting both established firms such as Microsoft, Amazon, and Google and unique companies such as Duo Security, Rivian, and StockX. [109]

The ideal Michigan statute would balance the needs and interests of both businesses and consumers. It would provide baseline rights for consumers while providing clear guidance to businesses on what they can and cannot do with consumers' data.

***20** *1. Private Right of Action*

Giving consumers a private right of action in a comprehensive privacy statute is one of the biggest--if not the biggest--areas of disagreement in this field. A private right of action is when private individuals, as opposed to the state Attorney General, are allowed to sue other private parties for violating statutory provisions. In this case, if an individual is allowed a private right of action, then the individual may be able to sue a company for violating one or more provisions of a data privacy statute. This is generally perceived to be unfriendly to business.

The proposed laws drafted by the Michigan House and Michigan Senate differ on the issue of private right of action. The Michigan Consumer Privacy Act provides exclusive enforcement authority to the Attorney General. [110] However, the Michigan Personal Data Privacy Act assigns enforcement provisions to the Attorney General and provides consumers with a private right of action. [111] Michigan's statute should not provide consumers with a private right of action. Instead, it should provide the state Attorney General with the power to enforce the statute, sue on behalf of residents and enforce penalties against companies that are not in compliance.

Providing individuals with a private right of action could lead to increased court costs for businesses and negatively impact state courts. If an individual brings a case (or a class action), businesses could be subject to unmeritorious claims and face high discovery ***21** costs. [112] Additionally, state courts--courts of general jurisdiction--could be overwhelmed by privacy litigation. [113]

The impact of costly litigation has been demonstrated with Illinois' Biometric Information Privacy Act (BIPA). [114] BIPA provides a private right of action and in 2019, the Illinois Supreme Court held that individuals can show a technical violation of the statute instead of proving harm. [115] As a result, many of the lawsuits brought under BIPA have been settled out of court. Companies deciding to settle include Google [116] and Facebook. [117] Software facial recognition company Clearview AI also settled its own BIPA case, [118] but not before the company left the state of Illinois. [119]

The current litigation woes of businesses in Illinois show the downside of providing consumers with a private right of action. Even though the companies listed above are large, the settlement numbers suggest the increasing threshold involved in settling cases ***22** where a private right of action is permitted. Instead, Michigan should place all enforcement power within the state Attorney General. The state Attorney General is best suited to oversee any litigation surrounding this growing area. Providing the Attorney General sole enforcement authority will consolidate institutional knowledge and mitigate costs against businesses--while providing consumers with the necessary legal protections regarding their data. It will also allow for filtering out of some unmeritorious actions before they reach courtrooms. State Attorneys General are already empowered to sue companies on behalf of residents regarding related consumer protection violations and have done so in the past. [120] [121] Plus, the state Attorney General can assess damages on behalf of residents, place injunctions on adverse conduct and oversee the regulations addressing data privacy protections. As such, disallowing a private right of action while placing all direct authority within the state Attorney General will best advance the rights of consumers.

*23 *2. Compliance*

Another key issue the ideal Michigan statute should address is the issue of compliance. This is an important issue for businesses because these new requirements are costly and often require businesses to contract with other parties. Some key compliance costs include developing information governance programs, drafting privacy policies, and hiring or consulting chief privacy officers. [122]

A Michigan statute should focus on lessening the cost of regulatory compliance for businesses. This is especially important because a large part of Michigan's economy is fueled by small businesses, [123] which are highly susceptible to large compliance costs. Unlike larger companies, smaller businesses may not have the capital to hire data protection officers or the infrastructure to easily adhere to these regulatory requirements. They may also handle significantly less personal data. Larger companies that do business overseas and/or in more active markets such as California are likely to have the means and framework to address compliance. However, smaller companies are more likely to be less equipped to handle "complex regulatory compliance mandates." [124]

The California Model is illustrative of how expensive privacy legislation can be. In 2019, the Attorney General issued an economic impact assessment of the CCPA, which ***24** found that companies were estimated to pay $55 billion in initial compliance costs. [125] This assessment was issued before the bill became law and provided a range of potential costs companies could face to both obtain and maintain compliance. [126] The researchers who conducted this impact assessment estimated that firms with fewer than 20 employees could expect to pay $50,000 at the outset to become compliant while firms with more than 200 employees could expect to pay $2 million in initial costs. [127] Additionally, they estimated that 75% of California businesses earning less than $25 million in revenue would be impacted by this legislation. [128] This impact assessment is an important consideration for Michigan to look into; however, it is important to note that California has more residents and a larger economy than the state of Michigan. So even though these numbers are helpful to see how costly a comprehensive data statute could be, they may not necessarily correlate to the creation of this type of statute in Michigan.

Compliance costs are not avoidable; however, the key is to create a statute that focuses on limiting the impact on businesses, especially those with limited resources. Accordingly, Michigan needs to keep this in mind when choosing a model to replicate for its own comprehensive data privacy statute. The following discussion will explain which model is the best for Michigan to adopt.

*25 *C. The California Model*

California has the longest running data privacy statute in the U.S., making it an important model to consider. Many of the provisions mirror those created by the GDPR. [129] Additionally, many of the largest tech giants are present in the state, meaning that these companies--specifically their legal departments--have familiarity with the state's privacy statutes.

Less than a year after the CCPA went into effect, California residents voted in favor of the CPRA. [130] California voters chose to adopt a bill that reconstructs the CCPA. [131] This means that companies had to make sure that they understood the CPRA changes while maintaining compliance with the CCPA during the transition period. The constant changes and complexity associated with the California Model is a warning sign to Michigan. The increased probability of regulatory change only adds uncertainty for businesses and consumers alike. Michigan should also recognize the financial implications of the California model, as addressed above.

Additionally, the CPRA mandates that the CPPA will oversee all fines committed by companies. These regulatory and enforcement changes could present excessive burdens on companies to remain compliant. These changes could also make it harder to foster an environment that balances the needs of consumers while mitigating compliance costs.

***26** In conclusion, Michigan should not adopt the California Model because it has generated prolonged uncertainty. Furthermore, it does not make sense for Michigan to replicate a statute with high estimated regulatory costs.

D. The Uniform Model

The UPDPA is another model to address since the goal of the statute is to create a universal paradigm for data privacy protections. This proposed statute is focused on limiting compliance costs, especially as more and more states focus on adopting their own data privacy standards. The UPDPA has some benefits, such as strongly encouraging the respective state's Attorneys General to enforce the statute and providing flexibility to determine violation costs. The UPDPA also applies to a wide array of businesses, instead of adhering to thresholds traditionally required by other state statutes. But despite the proposal's best efforts, Michigan should not adopt the UPDPA.

Unlike its predecessors, the UPDPA does not provide consumers with all of the fundamental privacy rights. Specifically, the UPDPA omits the right to be forgotten. In the comments section on controller and processor responsibilities, the drafters explain that allowing consumers to ask companies to delete their data would be difficult due to the way that data is stored and processed. [132] The drafters go on to say that it would be difficult to ensure that any particular subject's data is deleted. However, the drafters fail to recognize that these statutes create processes for individuals to petition companies to access, transfer, or change their individual data. These requests can only occur if companies have access to the applicable individual data.

***27** To suggest that a company would be unable to properly delete an individual's data is irreconcilable with the fact that these companies can access and alter the consumer's data in other ways. If the drafters intended to express that once something is posted online it can never be truly deleted, that would make sense. But this is not what is stated in the comments. Regardless, it does not make sense for a data privacy proposal to divert from the paradigm established by the GDPR. Denying individuals the right to be forgotten would greatly limit privacy rights that have been established as the norm. [133] If Michigan adopted the Uniform Model, then the state would curtail privacy protections for Michigan residents. It could also place an unnecessary burden on businesses both inside and outside of Michigan, because the companies would have to create separate policies addressing different privacy rights instead of policies that would address the same privacy rights.

Additionally, the UPDPA is not a statute Michigan should replicate due to its stance on targeted advertising. The UPDPA goes against the status quo by allowing companies to conduct targeted advertising as a compatible data practice. [134] From the outset, allowing this practice would be beneficial for businesses. However, there is a growing call to allow consumers to decide how their data will be used (hence the creation of these broader statutes in the first place). Additionally, as a compatible data practice under the UPDPA, a company would be able to engage in targeted advertising without an individual's consent.

The GDPR, the California Model and the Virginia/Colorado Model do not prevent companies from engaging in targeted advertising; they simply state that consumers can optout ***28** of targeted advertising practices. The Uniform Model drastically differs from the current precedent by not allowing consumers the option to opt-out of targeted advertising. The Uniform Model's position on this issue would be an outlier. Additionally, this would negatively impact businesses since consumers want more control over the use of their data.

Finally, the UPDPA goes against its stated goal of eliminating fragmented state statutes by allowing for the creation of voluntary consent standards. Voluntary consent standards allow stakeholders in different industries to create their own implementation plans. [135] The drafters of the UPDPA believe that this process will allow businesses and other relevant stakeholders to come together and address the key issues involved in carrying out a comprehensive bill, thereby mitigating compliance costs. The draft legislation provides that any voluntary consent standards have to be approved by the state Attorney General. [136] The problem with this approach is that it provides an opening for different industries to create their own standards for implementation. This means that instead of having one bill addressing all companies, there is a strong probability that each industry could decide how to implement the bill for their respective industries. The stakeholders creating these voluntary consent standards will likely be those represented by trade associations or lobby groups.

For smaller companies and for consumers, the creation of various voluntary consent standards could lead to confusion over compliance along with a fragmented approach when applying the statute. What if companies are part of multiple industries? Can a company pick and choose which voluntary consent standard applies to them? Also, would every voluntary consent standard be easily accessible for consumers to find? Would the voluntary consent ***29** standards be easy to understand and clearly address both the obligations of the businesses along with the rights consumers have in addressing violations of the statute? The voluntary consent standard would likely do more harm than good in this scenario. Instead of providing flexibility and openness for businesses to comply, it would create a disorderly regulatory system where the privacy of data would depend on each industry. Instead of applying the same rules to all companies, consumers and smaller businesses would struggle with the complexity of the statute along with differing applications surrounding compliance.

In sum, Michigan should not replicate the UPDPA because the proposed law veers away from the paradigm set up by prior data protection statutes. Additionally, the proposed bill seeks to limit the protections provided to consumers and institute voluntary consent standards that will not only create more fragmented laws but also add additional compliance costs for businesses.

E. The Virginia/Colorado Model

The Virginia/Colorado model is the best option for Michigan to replicate because it provides consumers with the baseline privacy protections established by the GDPR while mitigating potential compliance costs for businesses. Both statutes provide consumers with fundamental privacy rights, such as the right to access data, the right to receive notice, and the right to correct data.

Additionally, the Colorado statute is transparent and straightforward. The Colorado statute explains that the goal of the legislation is "to build a world where technological innovation and privacy can coexist." [137] The Colorado law also aims to both provide transparency for consumers and strengthen compliance and accountability for businesses that ***30** engage in the collection and use of personal data. [138] The Virginia/Colorado Model is focused on balancing the privacy interests of consumers while making sure that these interests are feasible for the businesses that have to provide consumers with information pursuant to a request.

Both statutes also place exclusive enforcement authority in their respective state Attorney General to sue companies regarding violations of their respective statutes. This maintains the current practice used by many states against companies for widespread data breaches. This process is beneficial for small companies that do not have to worry about frivolous cases and the associated burden of legal fees. Additionally, the Virginia/Colorado Model is beginning to build a bandwagon effect, with the recent passage of privacy laws in Utah and Connecticut.

There are a few key differences between the bills that Michigan should consider when drafting its own statute. Michigan can either expressly state what a business should pay if they violate the statute or can refer to the state's consumer protection act when deciding how to remedy a violation. The VCDPA expressly provides that companies in violation of the statute have to pay up to $7500 for each violation while the CPA states that a violation constitutes a deceptive trade practice under their respective consumer protection statute. [139] The provision in the CPA is an acceptable practice; however, it may be easier for companies to have the consequences specifically delineated in the statute. Therefore, Michigan should follow the Virginia statute so businesses know what to expect if they are noncompliant.

***31** Another difference from Virginia is that the Colorado bill explicitly preempts local government laws and regulations. [140] This section is important for Michigan to adopt because it would clearly explain to both residents and businesses that the comprehensive statute governs. It would also clarify any potential confusion surrounding related ordinances, statutes, or other regulations regarding data privacy.

Two comprehensive data privacy bills were introduced in Michigan but neither made it out of committee before the end of the legislative session. The Michigan Consumer Privacy Act mirrors the Virginia/Colorado model, especially in its decision

to give exclusive enforcement authority to the Attorney General. [141] The Michigan Personal Data Privacy Act seems to adopt provisions from a variety of state privacy laws, including providing a private right of action. [142] Whether Michigan reintroduces either bill or drafts a new alternative, the comprehensive data law should provide exclusive authority in the Attorney General and limit the cost of regulatory compliance.

Overall, the best option for Michigan is to adopt the Virginia/Colorado model. Both statutes are very similar, focusing on providing consumers with commonly-accepted privacy rights while providing businesses with clear expectations regarding regulations and compliance.

*32 IV. CONCLUSION

Michigan should adopt a comprehensive data privacy statute. Michigan can no longer sit on the sidelines as other states create laws addressing emerging data privacy issues. Instead, Michigan legislators need to come together and pass legislation that will both provide consumers with fundamental privacy rights as well as provide businesses with clear rules regarding regulatory compliance. The best option moving forward is for Michigan to pass a comprehensive data privacy statute that adheres to the Virginia/Colorado Model.

Footnotes

1 Grace Turner, *Silicon Valley's LinkedIn Moves into Bigger Detroit Office*, Dbusiness Magazine: Daily News (Apr. 25, 2019), https://www.dbusiness.com/daily-news/silicon-valleys-linkedin-moves-into-bigger-detroit-office/ (Lists other technology companies that have moved to Detroit including Google, Waymo, Uber Pinterest, Snap, Twitter, and Amazon)

2 Ben Wolford, *What is GDPR, the EU's new data protection law?*, DATA PROT. REGUL. COMPLIANCE GUIDELINES, http://gdpr/edu/what-is-gdpr/ (last visited Oct. 24, 2021).

3 Mike Davis, *U.S. must catch up with the rest of the world on data privacy*, ROLL CALL: OP. (Oct. 14, 2021, 6:00 AM), https://rollcall.com/2021/10/14/us-must-catch-up-with-rest-of-the-world-on-data-privacy/ (Brazil's General Data Protection Law and China's Personal Information Protection Law).

4 Devin Coldewey, *The California Consumer Privacy Act officially takes effect today*, TECHCRUNCH+ (Jan. 1, 2020, 9:01 AM), https://techcrunch.com/2020/01/01/the-california-consumer-privacy-act-officially-takes-effect-today/?guccounter=1.

5 Sarah Rippy, *Virginia Passes the Consumer Data Protection*, IAPP: PRIV. TRACKER (Mar. 3, 2021), https://iapp.org/news/a/virginia-passes-the-consumer-data-protection-act/.

6 Sarah Rippy, *Colorado Privacy Act Becomes Law*, IAPP: THE PRIV. ADVISOR (Jul. 8, 2021), https://iapp.org/news/a/colorado-privacy-act-becomes-law/.

7 Taylor Kay Lively, *Utah becomes fourth U.S. state to enact comprehensive consumer privacy legislation*, IAPP: THE PRIV. ADVISOR (Mar. 25, 2022), https://iapp.org/news/a/utah-becomes-fourth-state-to-enact-comprehensive-consumer-privacy-legislation/.

8 Taylor Kay Lively, *Connecticut enacts comprehensive consumer data privacy law*, IAPP: THE PRIV. ADVISOR (May 11, 2022), https://iapp.org/news/a/connecticut-enacts-comprehensive-consumer-data-privacy-law/.

9 Pollyanna Sanderson, *Uniform Law Commission Finalizes Model State Privacy Law*, FUTURE OF PRIV. F.: BLOG (Jul. 21, 2021), https://fpf.org/blog/uniform-law-commission-finalizes-model-state-privacy-law/.

10 Lauren Feiner, *Tech industry's critical policy issues likely tabled as Congress heads for recess*, CNBC (Aug. 5, 2022, 10:17 AM), https://www.cnbc.com/2022/08/05/critical-tech-policy-issues-likely-tabled-as-congress-heads-for-recess.html?__source=sharebar%7Ctwitter&par=sharebar.

11 Margaret Harding McGill, *Online privacy bill faces daunting roadblocks*, AXIOS: TECH. (Aug. 4, 2022), https://www.axios.com/2022/08/04/online-privacy-bill-roadblocks-congress.

12 *Id.*

13 Anokhy Desai, *US State Privacy Legislation Tracker*, IAPP, https://iapp.org/resources/article/us-state-privacy-legislation-tracker/ (last updated Oct. 7, 2022).

14 H.B. 5989, 101st Leg. (Mich. 2022).

15 S.B. 1182, 101st Leg. (Mich. 2022).

16 Ernst Oliver Wilhelm, *A brief history of the General Data Protection Regulation (1981-2016),* IAPP (Feb. 2016), https://iapp.org/resources/article/a-brief-history-of-the-general-data-protection-regulation/.

17 *Id.*

18 *Id.*

19 *Id.*

20 *Id.*

21 Andrew Rossow, *The Birth of GDPR: What It Is And What You Need To Know*, Forbes (May 25, 2018, 7:32am), https://www.forbes.com/sites/andrewrossow/2018/05/25/the-birth-of-gdpr-what-is-it-and-what-you-need-to-know/?sh=5e92614355e5

22 Mark K. Kaelin, *GDPR: A cheat sheet*, Security: TechRepublic (May 23, 2019, 12:47am), https://www.techrepublic.com/article/the-eu-general-data-protection-regulation-gdpr-the-smart-persons-guide/

23 Rossow *supra* note 21

24 Council Regulation 2016/679, art. 3, 2016 O.J. (L 119) 32, 33 (EU)

25 Rossow, *supra* note 21

26 Coldewey, *supra* note 4

27 *Id.*

28 *Data Collection & Mgmt., Comparison Table--Privacy Law FAQs: Comparing GDPR with laws from California, Virginia, Colorado*, Privacy & Data Sec.: Bloomberg Law (2021), https://www.bloomberglaw.com/product/privacy/document/XE94Q6GK000000 (Additionally, the CCPA also applies to companies that have a revenue threshold greater than $25 million along with making at least 50% of revenue from selling data).

29 Coldewey, *supra* note 4

30 *Data Collection & Mgmt., supra* note 28

31 *Id.*

32 Mark Smith, *ANALYSIS*: *California Voters Strike Back with New Privacy Law*, Bloomberg Law (Nov. 23, 2020), https://www.bloomberglaw.com/product/privacy/bloomberglawnews/bloomberg-law-analysis/X18QN768000000

33 *Id.*

34 *Id.*

35 Shoeb Mohammed, *The First Privacy Agency*, CalChamber: Capitol Insider (Feb. 22, 2021), https://capitolinsider.calchamber.com/2021/02/the-first-privacy-agency/

36 Lydia del la Torre & Glenn Brown, *What is the California Privacy Protection Agency?*, IAPP (Nov. 23, 2020), https://iapp.org/news/a/what-is-the-california-privacy-protection-agency/

37 Mark Smith, *ANALYSIS*: *Stealth Conn. Privacy Bill Nearly Slipped Past Radar*, Bloomberg Law (June 18, 2021), https://www.bloomberglaw.com/product/privacy/bloomberglawnews/bloomberg-law-analysis/X2DARHCS000000

38 Rippy, *supra* note 5

39 *Id.*

40 *Id.*

41 Rebecca Klar, *Virginia governor signs comprehensive data privacy law*, The Hill (Mar. 3, 2021), https://thehill.com/policy/technology/541290-virginia-governor-signs-comprehensive-data-privacy-law?rl=1

42 *Id.*

43 *Id.*

44 *Id.*

45 Rippy, *supra* note 6

46 *Id.* The statute specifically impacts businesses that control or process the personal data of at least 100,000 consumers or more during a calendar year along with businesses that collect revenue or receive a discount on the price of goods or services from the sale of personal data and processes or controls the personal data of 25,000 consumers or more.

47 *Id.*

48 Rippy, *supra* note 5

49 *Id.*

50 *Data Collection & Mgmt., supra* note 28

51 *Id.*

52 Rippy, *supra* note 6

53 *Id.*

54 *Personal Data Protection Act*, Uniform Law Comm., (last updated Feb. 8, 2022), https://www.uniformlaws.org/committees/community-home?CommunityKey=28443329-e343-4cbc-8c72-60b12fd18477

55 *The Uniform Personal Data Prot. Act (UPDPA): A Practical Response to Personal Response to Data Privacy Legislation*, Zoom (Oct. 15, 2021), https://uniformlaws.zoom.us/rec/play/pm2TZkoVn37F3xa5CAW3IVTtfpi75TdAfdpc7IQ-4WE0I4yynvvR4wtkgpBfoU7qiFnyewJkQzlZ1vlU?autoplay=true&startTime=1634317233000

56 *Id.*

57 *Id.*

58 *Id.*

59 Unif. Personal Data Protection Act § 2 (1) (Unif. Law Comm'n, Proposed Official Draft 2021)

60 Unif. Personal Data Protection Act § 2 (21) (Unif. Law Comm'n, Proposed Official Draft 2021); *See also The Uniform Personal Data Protection Act (UPDPA) supra* note 55

61 *The Uniform Personal Data Protection Act (UPDPA), supra* note 55

62 Unif. Personal Data Prot. Act § 16 note on applicability of consumer protection act (Unif. Law Comm'n, Proposed Official Draft 2021)

63 *Id.*

64 *The Uniform Personal Data Prot. Act (UPDPA) supra* note 55

65 *Id.*

66 *Id.*

67 Unif. Personal Data Protection Act § 12 (Unif. Law Comm'n, Proposed Official Draft 2021)

68 *Id.*

69 *Id.*; *See also The Uniform Personal Data Prot. Act (UPDPA) supra* note 55

70 *The Uniform Personal Data Prot. Act (UPDPA) supra* note 55

71 *Id.*

72 *Id.*

73 *Id.*

74 Unif. Personal Data Prot. Act § 7 (c) (Unif. Law Comm'n, Proposed Official Draft 2021)

75 *The Uniform Personal Data Prot. Act (UPDPA) supra* note 55

76 Adam Schwartz, *Sen. Cantwell Leads with New Consumer Data Privacy Bill*, Elec. Frontier Found. (Dec. 3, 2019), https://www.eff.org/deeplinks/2019/12/sen-cantwell-leads-new-consumer-data-privacy-bill

77 *Wicker, Thune, Fischer, Blackburn Introduce Consumer Data Privacy Legislation*, U.S. S. Comm. on Commerce, Sci., & Transp. (Sep. 17, 2020), https://www.commerce.senate.gov/2020/9/wicker-thune-fischer-blackburn-introduce-consumer-data-privacy-legislation

78 Jonathan M. Gaffney et al, CONG. RESEARCH SERV., LSB10776, Overview of the Am. Data & Privacy Prot. Act., H.R. 8152 (2022).

79 Stacey Gray, *The Bipartisan House Privacy Bill Would Surpass State Protections*, Lawfare (July 21, 2022), https://www.lawfareblog.com/bipartisan-house-privacy-bill-would-surpass-state-protections

80 H.R. 8152, 117th Cong. (2022).

81 *Id.*

82 Cobun Zweifel-Keegan, *Understanding the Scope of the draft Am. Data Privacy & Prot. Act*, IAPP (Jun. 9, 2022), https://iapp.org/news/a/understanding-the-scope-of-the-draft-american-data-privacy-and-protection-act/

83 *See Supra* note 78

84 *Id.*

85 *Id.*

86 Hugo Loriot, *What the Am. Data & Privacy Prot. Act means for marketers*, Marketing Dive: Opinion (Jul. 19, 2022), https://www.marketingdive.com/news/what-american-data-and-privacy-protection-act-means/626890/

87 Margaret Harding McGill, *Online privacy bill faces daunting roadblocks*, Axios: Tech. (Aug. 4, 2022), https://www.axios.com/2022/08/04/online-privacy-bill-roadblocks-congress#

88 H.R. 8152, 117th Cong. (2022)

89 *Id.*

90 *Id.*

91 Karen Schuler, *Fed. data privacy reg. is on the way--That's a good thing*, IAPP (Jan. 22, 2021), https://iapp.org/news/a/federal-data-privacy-regulation-is-on-the-way-thats-a-good-thing/.

92 *Id.*

93 Safe Computing, *History of Privacy Timeline*, University of Michigan: Info. & Tech. Services (2022), https://safecomputing.umich.edu/privacy/history-of-privacy-timeline

94 *Security Breach Notification Laws*, Nat'l Conference of State Leg. (Jan. 17, 2022), https://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx

95 *Id.*

96 Chris D. Linebaugh, Cong. Research Serv., LSB10210, WHAT LEGAL OBLIGATIONS do INTERNET COMPANIES HAVE to PREVENT & RESPOND to a DATA BREACH (2018)

97 Orion Donovan-Smith, *McMorris Rodgers, House Democrats back compromise to pass historic privacy bill. But will Cantwell let it pass?,* The Spokesman-Review (July 25, 2022), https://www.spokesman.com/stories/2022/jul/25/historic-data-privacy-law-could-be-within-reach-if/

98 *Id.*

99 Gray, *supra* note 79.

100 Margaret Harding McGill, *Online privacy bill faces daunting roadblocks*, Axios: Tech. (Aug. 4, 2022), https://www.axios.com/2022/08/04/online-privacy-bill-roadblocks-congress#

101 Frank Konkel, *The Only Certainty in Next Split Congress is Uncertainty, Experts Say*, Nextgov (Nov. 17, 2022), https://www.nextgov.com/policy/2022/11/only-certainty-next-split-congress-uncertainty-experts-say/379890/

102 James Brandell et al, *Fall 2022 Congressional Outlook*, Dykema (Oct. 17, 2022), https://www.dykema.com/a/web/2JGenU5ye3HYGC3tRUayZG/4sm7Kx/117thoutlook_v7.pdf

103 *Id.*

104 Konkel, *supra* note 101.

105 *Id.*

106 Taylor Kay Lively, *Utah becomes fourth U.S. state to enact comprehensive consumer privacy legislation*, The Privacy Advisor: IAPP (Mar. 25, 2022), https://iapp.org/news/a/utah-becomes-fourth-state-to-enact-comprehensive-consumer-privacy-legislation/

107 Taylor Kay Lively, *Connecticut enacts comprehensive consumer data privacy law*, IAPP: The Privacy Advisor (May 11, 2022), https://iapp.org/news/a/connecticut-enacts-comprehensive-consumer-data-privacy-law/

108 Anokhy Desai, *US State Privacy Legislation Tracker*, IAPP, https://iapp.org/resources/article/us-state-privacy-legislation-tracker/ (last updated Oct. 7, 2022).

109 Courtney Overbey, *Michigan: the Next North American Tech Hub*, Mich. Econ. Dev. Corp. (June 21, 2021), https://www.michiganbusiness.org/news/2021/06/michigan-the-next-north-american-tech-hub/.

110 H.B. 5989, § 13, 101st Leg. (Mich. 2022)

111 S.B. 1182, §§ 19, 21, 101st Leg. (Mich. 2022)

112 Teresa Milano, The BIPA Litigation Landscape & What Lies Ahead, WOODRUFF SAWYER : Insights (Apr. 1, 2021), https://woodruffsawyer.com/cyber-liability/bipa-litigation-landscape/

113 *Id.*

114 *Id.* Biometric analysis is not discussed in this note due to the complexity and constant changes involved in the technology. If Michigan were to adopt a statute addressing this type of privacy concern, it should be passed separate from a comprehensive data protection statute.

115 *Id.*

116 Emma Roth, *Google to pay $100 million to Illinois residents for Photos' face grouping feature*, THE VERGE : Tech (Jun. 6, 2022), https://www.theverge.com/2022/6/6/23156198/google-class-action-face-grouping-biometric-information-illinois-privacy-act.

117 Taylor Hatmaker, *Facebook will pay $650 million to settle class action suit centered on Illinois privacy law*, TECHCRUNCH (Mar. 1, 2021), https://techcrunch.com/2021/03/01/facebook-illinois-class-action-bipa/.

118 Taylor Hatmaker, *Clearview AI banned from selling its facial recognition software to most U.S. companies*, TECHCRUNCH (May 9, 2022), https://techcrunch.com/2022/05/09/clearview-settlement-bipa/.

119 Hatmaker *supra* note 117.

120 Kevin McCoy, *Target to pay $18.5M for 2013 data breach that affected 41 million consumers*, USA TODAY: Money (May 23, 2017, 4:10pm), https://www.usatoday.com/story/money/2017/05/23/target-pay-185m-2013-data-breach-affected-consumers/102063932/ (In 2017, Target settled with 47 states and the District of Columbia in the wake of the 2013 data breach affecting more than 41 million customers. The retail company paid $18.5 million in a multistate settlement and agreed to new industry standards regarding processing payments from debit and credit cards along with maintaining confidential information about customers.);

121 *Michigan Joins $39.5M Multistate Settlement over 2014 Anthem Data Breach*, Dept. of Att'y Gen. (Oct. 1, 2020), https://www.michigan.gov/ag/news/press-releases/2020/10/01/michigan-joins-39m-multistate-settlement-over-2014-anthem-data-breach. *See also 50 Attorneys General Secure $600 Million from Equifax in Largest Data Breach Settlement in History,* Dept. of Att'y Gen. (July 22,

2019), https://www.michigan.gov/ag/news/press-releases/2019/07/22/50-attorneys-general-secure-600-million-from-equifax-in-largest-data-breach-settlement-in-history.

122 Stephen J. Bigelow & Ben Cole, *What is Privacy Compliance & Why is it Important?*, TECHTARGET (Sep. 2022), https://www.techtarget.com/searchcio/definition/privacy-compliance.

123 MI New Econ., *Support Small Bus*. MI DEPT. OF LAB. AND ECON. OPPORTUNITY (last visited Nov. 26, 2022), https://www.michigan.gov/mineweconomy/support-small-businesses.

124 Bigelow, *supra* note 122.

125 Lauren Feiner, *California's new privacy law could cost companies a total of $55 billion to get in compliance*, CNBC: Tech (Oct. 5, 2019, 10:38am), https://www.cnbc.com/2019/10/05/california-consumer-privacy-act-ccpa-could-cost-companies-55-billion.html.

126 *Id.*

127 *Id.*

128 *Id.*

129 *Data Collection & Mgmt., supra* note 28.

130 Smith, *supra* note 32.

131 *Id.*

132 Unif. Personal Data Protection Act § 4 cmt. lines 21-27 (Unif. Law Comm'n, Proposed Official Draft).

133 Maureen Mahoney, *The Unif. Law Comm. privacy model bill is a disaster*, CONSUMER REPORTS: DIGITAL LAB (Aug. 13, 2021), https://digital-lab-wp.consumerreports.org/2021/08/13/the-uniform-law-commission-privacy-model-bill-is-a-disaster/.

134 Unif. Personal Data Prot. Act, *supra* note 67.

135 Unif. Personal Data Prot. Act § 12 (Unif. Law Comm'n, Proposed Official Draft 2021).

136 *Id.*

137 COLO. REV. STAT. § 6-1-1302(1)(b)(I) (2021).

138 COLO. REV. STAT. § 6-1-1302(1)(c)(II)(B) (2021).

139 *Data Collection & Mgmt., supra* note 28.

140 COLO. REV. STAT. § 6-1-1302.

141 Divonne Smoyer & Hubert Zanczak, *Mich. Atty. Gen. Nessel on strengthening consumer prot., right to privacy*, IAPP: The Privacy Advisor, (Aug. 23, 2022), https://iapp.org/news/a/michigan-attorney-general-nessel-on-strengthening-consumer-protections-right-to-privacy/.

142 *Mich. lawmakers introduce comprehensive privacy bill*, IAPP (Sep. 28, 2022), https://iapp.org/news/a/michigan-lawmakers-introduce-comprehensive-privacy-bill/

6 WNSUJBL 1

End of Document