The Legislatue Must Act Now on a Comprehensive Privacy Bill, in the form of the Massachusetts Data Privacy Act (S.2516, in Ways and Means)

Introduction

There is already a flood of data out there about each of us, that we don't own or control. We are newly at greater risk from AI systems that exploit and degrade that flood of data type casting each of us and siloing us into groups which may be as innocent as "likely to purchase organic foods", or as problematic as "those most likely to commit crimes".

CEO Arthur Sadoun of Publicis Groupe, a data broker, uses the example of a young woman he calls "Lola":

> '"At a base level, we know who she is, what she watches, what she reads, and who she lives with. Through the power of connected identity, we also know who she follows on social media, what she buys online and offline, where she buys, when she buys, and more importantly, why she buys.
>
> "We know that Lola has two children and that her kids drink lots of premium fruit juice. We can see that the price of the SKU she buys has

> been steadily rising on her local retailer's shelf. We can also see that Lola's income has not been keeping pace with inflation. With CoreAI, we can predict that Lola has a high propensity to trade down to private label."

The danger of this ability to profile consumers and predict their behavior is not limited to surveillance pricing that may lure them into buying pricey products, or increase a medication's price depending upon which customer walks by, based on whether they reliably have bought it in the past. The greater threat is the fact that our data is being sold to anyone who wants it at fire-sale prices. As a result, our national security is threatened by the ease with which sensitive personal data of American elected officials, civil servants and active-duty military personnel can be purchased by adversarial countries. Hacks of massive databases have become ever more profitable, frequent, and impactful with respect to the number of people whose data has been jeopardized. Decisions by our government are increasingly being made by opaque algorithms that depend on the purchase of data about the individuals being assessed. These algorithms impact: access to Medicaid, Medicare, and Social Security; determinations by criminal justice systems about prosecution, bail, sentencing, probation, and parole; access to unemployment compensation; decisions on who will be audited by the Internal Revenue Service and most importantly whether someone will be prosecuted for derogatory remarks about the government.

Federal, state and local law enforcement agencies are taking advantage of a statutory loophole to purchase databases and use them to investigate suspects without obtaining a warrant or even a court order or subpoena as required by the Fourth Amendment. The loophole results from two court cases in which defendants wanted to have bank transactions or phone logs excluded from evidence on the basis of their having been seized in illegal searches. The courts refused and established the "Third Party Doctrine," which stated that citizens do not have the right to an expectation of privacy in any information voluntarily provided to others.

In this testimony, we:

1. List the **features of the MA Data Privacy Act**.
2. Document the **national security threats** associated with the collection and sale of precise geolocation and sensitive personal data;
3. Describe many **violations of consumer data privacy** and recent enforcement actions taken by the Consumer Financial Protection Bureau (CFPB) and the Federal Trade Commission (FTC) against companies, and how these violations would be addressed by the MDPA;

4. Catalog some of the recent **data breaches** that have exposed our data and jeopardized our financial safety and medical privacy;
5. **Describe** the conditions likely to stifle further action by the CFPB and FTC to protect consumers from companies that violate their data privacy and take advantage of them through deceptive practices;
6. **Report** on the activities of the California and Texas Attorneys General (AGs) actions against companies in their respective states that have violated their comprehensive consumer data privacy laws; and
7. **Document** the extent to which our sensitive personal data is being sold to local, state, and federal law enforcement agencies, and the risks that this entails.

1. Provisions of the MDPA (S.2516)

Provisions of the MDPA (S.2516)	
Provision	Source/Details

Important Definitions	**Section 1. Definitions** (H) affirmative consent to an act or practice is not inferred from the inaction of the consumer or the consumer's continued use of a service or product provided by the controller. (2)"**Affirmative Consent**" has a lengthy definition that including among other things: a. it must be given as opposed to assumed by a lack of action; b. it must be revocable; c. there cannot be any misleading about exactly what the consumer is consenting to; d. the controller(C) must provide the specific categories of personal data (PD) that the C intends to collect, process, or transfer under each act or practice; e. it must be equally obvious and easy for the consumer to deny consent; f. consent must be given prior to any action taken by the controller ("C") Note: **Section 6. Actions of Controllers(a)(B)6** specifies that a C must cease its action within 15 days of a revocation of consent. (11) "**Controller**" means a person who, alone or jointly with others, determines the purpose and means of collecting or processing personal data. (37) "**Personal data"** means any information, including derived data and unique persistent identifiers, that is linked or reasonably linkable, alone or in combination with other information, to an identified or identifiable individual or a device that identifies or is linked or reasonably linkable to an individual. "Personal data" does not include de-identified data or publicly available information. (40) "**Processor**" means a person who collects, processes, or transfers personal data on behalf of, and at the direction of, a controller or another processor, or a Federal, State, Tribal, or local government entity.

	(48) **"Small business**" means a controller or processor that for the period of the 3 preceding calendar years a. Had an average annual gross revenue of no more than $20,000,000; b. Did not collect, process or retain the personal data of more than 200,000 individuals c. did not transfer personal data to a third party in exchange for revenue or other valuable consideration
The Massachusetts Data Privacy Act (MDPA) applies to all businesses, including non-profits that collect the personal data of at least 25,000 consumers in the preceding calendar year or that received revenue or other valuable consideration from the sale of any personal data. **However, MA residents may only bring a civil action against large businesses (a small business is defined above)**	**Section 2. Applicability.** The provisions of this chapter apply to persons that conduct business in this state or persons that produce products or services that are targeted to residents of this state and that during the preceding calendar year: (a) Collected or processed the personal data of not less than 25,000 consumers, excluding personal data controlled or processed solely for the purpose of completing a payment transaction, so long as all personal data collected or processed for such purpose was deleted or de-identified within 90 days, except when necessary to investigate fraud or as consistent with a business's return policy; or (b) derived revenue or other valuable consideration from the sale of personal data. **Section 12. Enforcement.** "(b) A violation of this chapter or a regulation adopted under this chapter with respect to the personal data of a consumer constitutes an injury to that consumer. The injured consumer may bring a civil action against the party that commits the violation, provided such party is not a small business. In a civil action brought under this subsection in which a plaintiff prevails, the court may award the plaintiff:"
Excluded Data	**From Section 13. Non-Applicability**

	Excludes: **data used in medical research and teaching.** **specific medical diagnostic data** **Excludes data specifically covered by:** Health Insurance Portability and Accountability Act of 1996 Gramm-Leach-Bliley Act, 15 U.S.C. 6801 Family Educational Rights and Privacy Act, 20 U.S.C. 1232g et seq. the Health Care Quality Improvement Act of 1986, 42 USC 11101 et seq. the Patient Safety and Quality Improvement Act, 42 USC 299b-21 et seq federal policy for the protection of human subjects under 45 CFR 46
Data Minimization: **A controller (C) may ot collect, process, or transfer private data (PD) unless the collection, processing, or transfer is limited to what is reasonably necessary and proportionate to provide the product or service requested by the consumer**.	**Section 6. Actions of Controllers. (a)(1) and (A)**
Right to opt-out of all transfers of personal data.	**Section 4. Consumer Rights.a(6)(B)**
A C may not collect, process, or transfer sensitive data (“SD”) unless the collection, processing, or transfer is limited to what is strictly necessary and proportionate to provide the product or service requested by that consumer.	**Section 6. Actions of controllers (a)(B)2**
A C may not sell sensitive data	**Section 6. Actions of controllers.(a)(B)3**

Each transfer of SD requires the opt-in consent of the person to whom the data belongs. **The C must disclose the processing purpose purpose for which the consumer's consent is sought**	**Section 6. Actions of controllers(a)(B)2**
Sensitive data includes precise geolocation information, biometric data, financial data, government-issued identifiers, medical data, private communications and data associated with them, online activities over time and across third-party websites or online services, protected classes, sex and gender identity, information that reveals the status of an individual as a veteran, or member of the military and more.	**Section 1. Definitions**, **(47) "Sensitive data"** for the complete list. The MDPA requires a separate privacy notice for biometric data**: Section 6. Actions of Controllers(c)(2)(vi)** The MDPA requires a separate privacy notice for precise geolocation data **Section 6. Actions of Controllers(c)(2)(vii)**
The MDPA includes Section 93N that provides for especially strong protections of geolocation data. **Controllers will only be allowed to collect location data for very limited purposes and before doing so they must share their purposes in a location privacy policy and get the consumer's permission for each purpose individually before collecting any location data. Permission may be revoked at any time..** **Companies are forbidden to sell, rent, trade, or lease location information to third parties** **93N. Includes a warrant requirement for sharing location data with any federal, state, or local government agency or official.**	**"Chapter 93N. Privacy Protections for Location Information Derived from Electronic Devices"** This chapter immediately follows the MA Data Privacy Act in the same document
Protects Minor's Data by prohibiting any sale of a child's data and any targeted advertising to a minor. **Requires all collection and processing of a minor's data to adhere to the Children's**	**Section 6. Actions of Controllers(a)(B)(5)** In the case of a known child, the C may not collect or process PD unless it is in accordance with the provisions of COPPA. **Section 6. Actions of (C)(a)(B)(7)**prohibits

Online Privacy Protection Act (COPPA). **Right of parent or legal guardian to exercise the rights of a minor child**	the sale of a minor's data and targeted advertising to a minor **Section 4. Consumer rights.(c)**
Prohibits combining data sets except for the limited purposes which are accepted and expected business activities.	**See Section 7. Responsibilities of processors and controllers.(b)(5)**
Requires Cs to set a limit on the length of time each category of data will be retained and disclose circumstances under which covered data will be deleted, de-identified, or otherwise modified in consideration of the purposes for which it was collected or processed and the sensitivity of the PD.	**See Section 6. Actions of controllers.(c)(1)(vi)** **Section 8.(g)(4) Data Protection Assessments.**
Any right to opt-out must be clear and conspicuous and as easily executed as to opt-in.	**Section 6. Actions of controllers.(c)**
Right to opt out of targeted advertising	**Section 4. Consumer rights.(a)(6)(A)**
Right to opt-out of profiling used for solely automated decisions that produce legal or similarly significant effects concerning the consumer.	**Section 4. Consumer rights.(a)(6)(C)(ix)**
Right to learn whether the C collected, or processed the consumer's data, including whether inferences were derived from that data and to obtain a copy of the consumer's PD that was collected or processed by the C and a list of any third parties to which the data was transferred in a portable usable format that allows the consumer to transmit the data to another C without hindrance.	**Section 4.Consumer Rights(a)(1,2 and5)** **Section 4.(d) but there are two(d)s in this section and this is in the second of these** **Section 4.Consumer Rights(e)(1)and (e)(2)**
Right to delete personal data including PD that the consumer provided to the C or that C obtained from another source, and derived data and to instruct a C or processor (P) to make reasonable efforts to notify all third parties (TPs) or Ps to which the controller has transferred the PD of the deletion request.	**Section 4.Consumer Rights.(a)(4)**
Right to correct inaccuracies in PD and to instruct a C or P to make reasonable	**Section 4.Consumer Rights.(a)(3)**

efforts to ask all TPs or Ps to which the controller has transferred the PD to correct these inaccuracies.	
Right to appoint an authorized agent to execute the consumer's rights	**Section 4. Consumer Rights.(c)** **Section 5. Authorized agent.**
Right to have any data broker (DB) operating in Massachusetts delete your personal data. **The MDPA requires that by January of 2027 the state implements an accessible deletion mechanism that allows a consumer to make a single verifiable request that every DB that maintains any personal data delete any personal data related to that consumer held by the data broker or associated service provider or contractor.** **Consumers will not be charged for making a deletion request. DBs will be required to implement the request within 45 days of receiving it and if they cannot verify the consumer's identity and choose not to delete the data, they must refrain from sharing or selling the data.**	**Section 16. Data Broker Opt Out.**
Protects against dark and deceptive practices in the presentation of consumers' choices to exercise their rights, in the mechanism used by the consumer to revoke their affirmative consent or in the platform, technology or mechanism that the C provides the consumer to exercise their right to opt out of targeted advertising, the sale of the their PD and, profiling for automated decisions.	**Section 1. Definitions. Affirmative Consent under "Affirmative Consent" does not include(D), (14) "Dark pattern or deceptive design"** **Section 4. Consumer Rights(e)(2)** **Section 6. Actions of controllers.(a)(B)(6) And (e) (2)(II)**
A C or P may not collect, process, or transfer PD in a manner that discriminates against, or threaten to discriminate against, an individual or class of individuals, or otherwise makes unavailable the equal enjoyment of goods or services, on the basis of an individual's or class of individuals' actual or perceived	**Section 4. Consumer Rights(f)**

race, color, ethnicity, sex, sexual orientation, gender identity, gender expression, physical or mental disability, religion, genetic information, pregnancy or condition related to pregnancy, status as a veteran, ancestry, national origin, citizenship, immigration status, or any other basis protected by chapter 151B.	
Requires an easily accessible and understandable privacy notice provided directly to consumers and displayed online that includes: **1. An active email address for the controller(C) or other online mechanism to contact them concerning privacy or security concerns and their identifying information such as registered and assumed business names.** **2. a description of the C's collection, processing, selling, or sharing of personal data (PD) for training or use in AI;** **3. the categories of data collected, processed and transferred including a separate list of sensitive data;** **4. the purpose for collecting and processing each category of PD;** **5. the categories of third parties, if any, to which the controller transfers PD;** **6. the name of each data broker to whom data is transferred.** **7. how long data will be retained by the C;** **8. a clear and conspicuous description of any processing of PD by the C for the purposes of targeted advertising, sale of PD to third parties, or profiling the consumer in furtherance of decisions that produce legal or similarly significant effects concerning the consumer, and a procedure by which the consumer may opt out of this type of processing;**	**Section 6. Actions of Controllers(c)(1)(i)**

9. requires that any change to the privacy notice be communicated to the consumer before it is implemented	
Within a year of becoming a data broker (DB) the DB must register on a public site hosted by the Office of Consumer Advocacy and Business Regulation (OCABR) and list the following: **1. whether the DB permits a consumer to opt out of the DB's collection of brokered personal information, opt out of its databases, or opt out of certain sales of data:** **2. the method for requesting an opt-out;** **3. whether the opt-out applies to only certain activities or sales, which ones;** **4. a statement specifying the data collection, databases, or sales activities from which a consumer may not opt out;** **5. whether the DB implements a purchaser credentialing process;** **6. the number of DB security breaches that the data broker has experienced during the prior year, and if known, the total number of consumers affected by the breaches;** **7. a separate statement detailing the data collection practices, databases, sales activities, and opt-out policies that are applicable to the brokered personal information of minors;** **Enforcement of Registration:** **1. A DB that fails to register is liable to the Commonwealth for:** **a. a civil penalty of $125.00 for each day it fails to register;**	**Section 15. Data Brokers Annual Registration**

b. the fees due under this section during the period it failed to register; **c. other penalties imposed by law.** **d. A DB that omits required information must file an amendment that includes the omitted information within 30 business days following notification of the omission and is liable to the Commonwealth for a civil penalty of $1,000.00 per day of delay.** **e. a DB that files materially incorrect information in its registration:** **(i) is liable to the Commonwealth for a civil penalty of $25,000.00; and** **(i) if it fails to correct the false information within 30 business days after discovery or notification of the incorrect information, the DB must pay an additional civil penalty of $1,000.00 per day for each day thereafter that it fails to correct the information.** **All of the above is enforceable by the Attorney General.**	**Section 12. Enforcement.**
Data brokers(DBs) are required to vet the parties to whom they sell your data. 1. DBs must maintain reasonable procedures to ensure that the brokered personal data (PD) it discloses is used for a legitimate and legal purpose and must verify the identity of a prospective new user before sharing any PD with them. (2) Prospective users of the information must identify themselves, certify the purpose(s) for which they will use the PD, and that the information will only be used for this purpose(s). (4) A DB may not furnish brokered PD to any person if it has reasonable grounds to believe that the brokered PD will not be used for a legitimate and legal purpose.	**Section 17. Data Broker Credentialing.**

Requires that the AG enact rules and regulations to improve compliance and post a website where violations of this act can be reported and where all investigations of violations and their outcomes must be posted	**Section 11. Rulemaking.**
Enforcement **The Attorney General may bring a civil action against controllers (Cs) or processors (Ps) who violate the MDPA** **The AG can sue to enjoin (stop) the illegal action of the C or P or to:** **1. obtain damages, including punitive damages;** **2. recover any money or property that was obtained as a result of the violation;** **3. and disgorge any profits that resulted on behalf of the residents of the Commonwealth or individuals present in the Commonwealth;** **4. impose civil penalties of at least $15,000 per individual violation.** **5.recover the costs of investigation, attorney fees and litigation** **A violation of the MDPA or of a regulation adopted under it relating to the personal data of a consumer constitutes an injury to that consumer. The consumer can bring a civil action against a violator that is not a small business (i.e. against any business with greater than $20 million gross annual revenue annually).** **A plaintiff who prevails in court may be awarded:** **(1) Damages of not less than $15,000 per individual per violation, or actual damages, whichever is greater;**	**Section 12. Enforcement**

(2) punitive damages; **(3) injunctive relief, including an order that an entity retrieve any personal data transferred in violation of the MDPA.** **(4) declaratory relief; or** **(5) reasonable attorney's fees and litigation costs.** **In all cases, the court will consider the number of consumers whose rights have been violated, the sensitivity of the data,the risks from the non-compliance, the intent of the C or P, whether they took any precautions and their history of previous violations in MA, other states, at the federal level and internationally.** **Consumers may bring a private right of action against CEs, SPs and third parties which are large data holders.** **Includes punitive damages, liquidated damages, injunction and costs and attorney fees.** **Liquidated damages of 0.15% of the annual global revenue of the CE. or $15,000 per violation,whichever is greater.**	

2. National Security Threats Presented by Sale of Geolocation Data and Sensitive Personal Data

In 2023 reporter Justin Sherman and his colleagues, masquerading as American or foreign companies, purchased highly sensitive information, including name, home address, email address, gender, age, occupation, income, net worth, credit rating, homeowner or renter status, home value, marital status, presence of children in the home, political affiliation, health data, financial data, religion, and information about religious practices, on thousands of active-duty troops and veterans from data brokers for as little as 12 cents per record. They revealed that they could have also purchased geolocation data. These data were easily procured using an American or a .asia domain

name, so they could have been easily purchased by any foreign company and sold to our adversaries.

A 2024 investigation by WIRED, Bayerischer Rundfunk (BR), and Netzpolitik.org demonstrated that US special operations service members could be tracked from Fort Bragg and MacDill Air Force Base, through Turkey and ultimately to a known ISIS stronghold in northern Syria. Also, they easily tracked 40 devices associated with service members as they entered and exited Büchel Air Base in Germany, where it is believed that the U.S. stores nuclear weapons, and traced their travel to other locations including a brothel. They tracked an individual working at the Consolidated Intelligence Center, a state-of-the-art facility suspected to be used by the National Security Agency, located in Wiesbaden, Germany. All of this location information was purchased from a U.S.-based data broker who legally collected advertising data.

The MDPA — and *Chapter 93N. Privacy Protections for Location Information Derived from Electronic Devices* included in it — would prevent companies from collecting precise geolocation data unless strictly necessary for delivery of a requested product or service, and the precision of the collected data would be restricted to what is absolutely necessary for the specific purpose. Affirmative consent would be required each time a company wishes to share our location data after the company discloses the purpose in each instance. It also requires that each company provides a readily accessible and obvious way to opt-out of targeted advertising which entails the collection of geolocation data. If an individual opts out of location data collection, this would be permanent unless the individual changes their mind and again provides consent. It would be illegal for any company to sell, rent, trade, or lease location data to third parties: companies could not sell location data to data brokers. Even if the impact of the MDPA and Chapter 93N are limited to residents of Massachusetts, the passage of these bills alongside California's existing, very strong comprehensive data privacy law could create the impetus needed for Congress to pass comprehensive data privacy legislation, modelled on the American Data Privacy Protection Act (ADPPA) that was nearly passed in 2022. This would protect our troops, officials and members of Congress alongside every other American resident.

3. Violations of Data Privacy Revealed and Remedied by the CFPB and FTC

Privacy Violations Affecting Adults

The CFPB filed suit against Walmart and Branch Messenger in December, 2024. Branch is a financial technology company that offers a product called the Branch Account, which includes a deposit account at Evolve Bank & Trust which consumers access through a mobile application, and a debit card provided by Branch. Walmart employed drivers to deliver orders to customers through their Spark Driver program,

and required these drivers to receive their payments via a Branch Account. The CFPB determined that Walmart engaged in unfair, abusive, and deceptive practices because they compelled Spark Drivers to receive their compensation via Branch Accounts, opened Branch Accounts for Spark Drivers without their informed consent, in many cases did not receive any authorization from the drivers, and made deceptive statements about Branch to Spark Drivers. These practices would have violated the MDPA, because MDPA instructs that:

> (c) A covered entity or service provider shall not:
> (1) engage in deceptive advertising or marketing with respect to a product or service offered to an individual; or
> (2) draw an individual into signing up for or acquiring a product or service through:
> (i) the use of any false, fictitious, fraudulent, or materially misleading statement or representation; or
> (ii) the use of a dark pattern or deceptive design.

The CFPB filed a number of other lawsuits in 2024 against companies that engaged in deceptive representations of the services that they offered to consumers, including against Apple, Goldman Sachs, three companies that issued loans to students, and mortgage lenders.

In 2024, the CFPB took action against TD Bank in 2024 for its failure to correct inaccuracies transmitted to credit reporting agencies (CRAs), to timely investigate consumer disputes, and to implement reasonable written policies and procedures regarding the information furnished to CRAs. TD Bank was ordered to take steps to prevent future violations and to pay $7.76 million in redress to affected consumers and a $20 million civil penalty. The MDPA, would enable consumers to ask a bank to delete inaccuracies in the data that the bank has collected on them as long as they could demonstrate the veracity of their claim.

The CFPB in the same month issued an order against American Honda Finance Corporation (Honda Finance) which is the captive automotive finance company for American Honda Motor Co., Inc., the sole authorized distributor of Honda and Acura motor vehicles in the United States. Honda Finance failed to correct errors it made by reporting to CRAs that car owners who were issued deferrals of car loan payments during the COVID pandemic were delinquent in their payments during the mandated deferral period even after investigations had confirmed the allegations. This failure to correct inaccuracies in customer data would be a violation of the MDPA.

In December, 2024 the CFPB proposed a rule to control the widespread sale of Americans' sensitive personal and financial information by data brokers. This rule would restrict the sale of personal identifiers such as Social Security Numbers and phone numbers by the companies that collect them. It would also ensure that consumers' financial data is only shared when necessary for specific applications, such as mortgage approval, and would not be sold to scammers taking advantage of a person's financial situation. It would classify data brokers that sell certain sensitive consumer information as "consumer reporting agencies" under FCRA, compelling them to adhere to accuracy standards, allowing consumers access to their information, and implementing safeguards to prevent prohibited uses of consumer data.

In 2024, the FTC prohibited the data broker X-Mode Social and its successor Outlogic from sharing or selling any sensitive location data in a settlement of allegations that the company sold precise location data that could be used to track people's visits to sensitive locations such as medical and reproductive health clinics, places of religious worship, and domestic abuse shelters exposing users to potential discrimination, physical violence, emotional distress, and other harms. In fact, not only did X-Mode Social/Outlogic sell the geolocation data it had collected from its own and third-party apps, and purchased from other data brokers and aggregators, but it curated custom audience segments based on characteristics of consumers that were highly sensitive and sold these to companies engaged in enterprises ranging from real estate to finance, as well as to private government contractors. For example, X-Mode provided a private clinical research company with a list of people who visited internal medical facilities and then pharmacies or specialty infusion centers within a certain radius in the Columbus, Ohio area so that the company could advertise their products to these individuals. X-Mode often failed to receive the consent of users for the collection and sale of their location data. It provided a privacy policy to third-party apps which failed to disclose to users to whom their location data was being sold, so even when consent was obtained it was without the user appreciating the risks.

The settlement with the FTC compelled X-Mode/Outlogic to create and maintain a comprehensive list of sensitive locations, and ensure that it would not share, sell, or transfer location data associated with these locations. It also required the company to delete or destroy location data linking individuals to providers of services to LGBTQ+ individuals or to attendance at public gatherings, including marches or protests, unless it obtains consumer consent or ensures the data has been de-identified or rendered non-sensitive. As described above, the MDPA and Chapter 93N would protect individuals from the collection and transfer of their location data without their specific consent for each transfer. The MDPA also allows individuals to opt out of any profiling by companies, including automated profiling.

In September, 2024, the FTC issued a report castigating social media and video streaming companies, including Meta, Snap, ByteDance, X, YouTube and Amazon, because they collected, retained and sold both users' and non-users' personal data, including their sensitive data, without either adequately informing them or implementing any protections or limitations on these practices.The MDPA would require data minimization and grant consumers and users the right to correct inaccuracies in their data, delete their data, and opt-out of targeted advertising and profiling. It would also require these large companies to establish data retention policies. They would be required to disclose to users the purpose for any transfer of their sensitive data, and obtain users' affirmative opt-in consent before transferring that data.

The FTC took action against Gravy Analytics and its subsidiary Venntel in December of 2024 because these companies tracked and sold sensitive location data from users, including selling data about consumers' visits to health-related locations and places of worship, even after learning that these individuals had not given consent to location data collection. Gravy Analytics sold non-anonymized data, including geolocation data and sensitive characteristics such as health or medical decisions, political activities, and religious viewpoints, that they ascertained from consumers' location data. Gravy Analytics was alleged to have deployed geofences in order to capture lists of consumers who traveled within certain geographical perimeters associated with their medical conditions and places of worship. The company also sold other lists that linked individual consumers to their sensitive characteristics. Venntel and Gravy Analytics collected, processed and curated data from 1 billion devices daily.

The FTC's proposed order prohibited Gravy Analytics and Venntel from selling, licensing, transferring, sharing, disclosing, or using sensitive location data except in contexts of national security or law enforcement. The companies would have to create a program listing sensitive locations including: medical facilities, religious organizations, correctional facilities, labor union offices, schools or childcare facilities, services supporting people based on racial and ethnic backgrounds, services sheltering homeless, domestic abuse, refugee or immigrant populations, and military installations; and prevent the use, sale, license, transfer, sharing, or disclosure of consumers' visits to these locations. Gravy Analytics and Venntel would have to either delete, de-identify, or render non–sensitive the data they collected within the previous three years unless consumers agreed to have it retained. All of these practices by Gravy Analytics and Venntel that were condemned by the FTC would be illegal under the provisions of the MDPA, and would be enforceable through both private action and the AG.

In January of 2025 the FTC released its findings that Mastercard, Revionics, Bloomreach, JPMorgan Chase, Task Software, PROS, Accenture, and McKinsey & Co. all improperly used highly sensitive data, such as precise location, web browsing history, and transaction history, to help businesses target individual consumers with different prices for the same goods and services. The study found that these data were used to elevate prices either when a consumer was clearly in need of a product or regularly purchased it, and to reduce prices for someone who was assessed to be unlikely to purchase the product without an incentive. The MDPA would prevent "surveillance pricing" by only allowing companies to collect data that is reasonably necessary (in the case of personal data) or strictly necessary (in the case of sensitive personal data) to deliver the requested service. The consumer would have to be informed of the need for the increased price and would have to confirm that they still desired the product or service despite any additional cost. Any incentive program offered by a company would have to disclose what data the company collects and why and allow the consumer to opt-out of the program.

Violations of Children's Privacy

This past August, the Department of Justice sued TikTok because, in violation of the Children's Online Privacy Protection Act (COPPA) and the Children's Online Privacy Rule, the company knowingly allowed children under 13 years old to sign up for a TikTok account without a parent's knowledge or consent, and then proceeded to collect extensive data from the children. When parents became aware of this and asked that their children's accounts be taken down and their data deleted, TikTok failed to take action. The MDPA protects all data of children as sensitive, and requires parental consent for the collection of any child's data. Any collection of children's data must be strictly necessary for a company to deliver the product or service that a parent has requested, and a parent's permission would be required for any transfer of this data. No child's data may be sold by any company.

The FTC was responsible for bringing TikTok's violation of children's privacy to light, and has also taken action against a number of other companies that failed to comply with The Children's Online Privacy Protection Act Rule (COPPA).

The educational technology company Edmodo created and hosted platforms and apps that enabled teachers to hold virtual classrooms in which 600,000 children participated. Students had to provide their names and email addresses, and sometimes their date of birth, phone number, and other identifying information. Edmodo was responsible for notifying schools about their data collection, who in turn were responsible for notifying the children's parents. The FTC found that not only did Edmodo fail to do this, but that it also illegally targeted the students with advertisements. Upon learning of the FTC's

investigation, Edmodo halted its operations in the U.S. In addition to requiring parental consent for the collection of a minor's data, the MDPA prohibits targeted advertising to minors.

The FTC alleged that Microsoft collected the data of children who used Xbox gaming products without obtaining parental consent. Microsoft belatedly requested parental consent, but the FTC found that the company retained the data of children whose parents declined consent, in some cases for years. This violated the COPPA rule requiring that companies retain children's data for no longer than reasonably necessary to deliver the requested product or service. Microsoft settled with the FTC for $20 million. The MDPA requires that any company which collects data must evaluate the length of time that the covered data will be retained, and identify the circumstances under which it would be deleted, de-identified, or otherwise modified in consideration of purposes for which it was collected or processed and the sensitivity of the covered data. The company's responsibility is heightened with respect to a minor's data because that data is classified as sensitive.

Amazon agreed to pay a $25 million civil penalty and to abide by a permanent injunction from the Department of Justice after the FTC alleged that Amazon violated COPPA by retaining children's voice recordings by default, instead of only as long as was reasonably necessary to fulfill the requested service. They also deceived parents by failing to abide by their promises that Alexa users could delete their or their children's voice recordings, audio files, transcripts, and geolocation information. The MDPA provides enforcement by private right of action or the Attorney General against any company that fails to honor the request of a consumer to have their data deleted.

In the most egregious violation of children's data privacy identified by the FTC, EPIC Games collected the full names, email addresses, usernames, and other personal information of many children under the age of 13 who played Fortnite without obtaining a parent's consent. According to the FTC, "EPIC used privacy-invasive default settings and deceptive interfaces that tricked Fortnite users, including teenagers and children… Fortnite's counterintuitive, inconsistent, and confusing button configuration led players to incur unwanted charges based on the press of a single button. For example, players could be charged while attempting to wake the game from sleep mode, while the game was in a loading screen, or by pressing an adjacent button while attempting simply to preview an item. These tactics led to hundreds of millions of dollars in unauthorized charges for consumers."

The FTC also alleged that EPIC allowed children to purchase V-Bucks for in-game purchases "by simply pressing buttons without requiring any parental or card holder

action or consent. Some parents complained that their children had racked up hundreds of dollars in charges before they realized EPIC had charged their credit card without their consent." When charges were disputed, EPIC froze the accounts. When parents asked them to unlock the accounts, EPIC threatened to close them if any future charges were disputed.

In its settlement with the FTC, EPIC was compelled to pay $245 million to consumers to settle charges that the company used dark patterns to trick players into making unwanted purchases and let children rack up unauthorized charges without any parental involvement. The FTC alleged that EPIC violated the COPPA and EPIC agreed to pay a $275 million penalty for that violation. In addition to all the protections that the MDPA provides to minors, it also protects consumers from being drawn "into signing up for or acquiring a product or service through:

i. the use of any false, fictitious, fraudulent, or materially misleading statement or representation; or
ii. the use of a dark pattern or deceptive design."

4. Data Breaches

According to the Identity Theft Research Center's 2024 Annual Data Breach Report, 3,158 data compromises affected Americans in 2023 necessitating 1,350,835,988 victim notifications owing to the large number of victims affected by several of these breaches. In the last year, a cyberattack on UnitedHealth Group's tech unit, Change Healthcare, compromised the personal information of 190 million people and resulted in the cancellation of many medical appointments, as doctors were unable to bill for their services. The data of 122 million people was leaked on a popular hacking forum after a breach of the data aggregator, DemandScience. A breach of data that AT&T stored with an insecure cloud storage company affected 110 million people. The compromised records of calls and texts included information about who users called and texted, when, and for how long. AT&T cellular customers, mobile virtual network operators customers using AT&T's network, and, AT&T landline customers who interacted with these cellular numbers were all impacted. The data breach of the background check firm MC2 exposed 106,316,633 records that included full names, email addresses, IP addresses, dates of birth, partial payment details, home addresses, phone numbers, employment and legal histories, property records, family, relatives, and neighbors' data.

The above data breaches do not even include the many cyber breaches of federal government databases executed by foreign actors likely affiliated with the governments of China, North Korea, and Russia. Nonetheless, most Americans' data has been jeopardized, and the only way that we can protect Americans going forward is by enacting comprehensive data privacy legislation to stem the flow of data. MDPA's core provisions on data minimization, and its limits on data retention, will dramatically cut

down on the volume of data accessible to bad actors, which will in turn make hacking less valuable as less data will be available to the hacker and impersonation to steal assets would be a lot more difficult.

5. Changes in Federal Agencies Will Limit Investigations of Data Privacy Violations and New Rulemaking to Increase Privacy Protections

In a leaked April, 2024 memo to President Trump, current FTC Chairman Andrew Ferguson declared that under his leadership the agency would "stop abusing FTC enforcement authorities as a substitute for comprehensive privacy legislation." His statement is consistent with the opinion he expressed in his concurrence and dissenting statement in response to the FTC's decision to penalize Gravy Analytics and Mobilewalla for their practices of collecting data from real-time bidding streams (that case is described below). He opined that the Section 5 of the FTC Act does not authorize the agency to prevent these companies from collecting data on an individual's "sensitive characteristics including race, ethnicity, gender, gender identity, sexual orientation, pregnancy, parenthood, health conditions, religion, and attendance of a political protest, among others." Second, he stated that the agency cannot compel companies to disclose criteria for how long they will retain this data or even geolocation data: "nothing in Section 5 forms the basis of standards for data retention." In addition, Ferguson opposed the release of the FTC's report on surveillance pricing described above, and when he ascended to the Chairmanship he immediately withdrew the request issued by the FTC a month prior for public comment on how people were impacted by surveillance pricing. According to a March 3, 2025 report from The Verge, at least a dozen probationary staff members at the FTC were fired, including workers from its Bureau of Consumer Protection. President Trump fired Rebecca Kelly Slaughter and Alvaro Bedoya, the two Democrats on the FTC, who consistently voted to rein in corporate abuses of private data. He also issued an executive order that would prevent any "independent" agency from spending federal funds on any activities or projects that were inconsistent with his priorities and required that the FTC get his approval for any proposed regulations. Any rules to prevent the collection of sensitive data about race, ethnicity and gender would be prohibited by the President's executive order eliminating DEI.

Meanwhile the activities of the CFPB have been terminated. Russel Vought, who was assigned to be its acting Chief, terminated CFPB funding and ordered staff to "cease all supervision and examination activity." He has also rescinded the CFPB's plan to enact rules that would limit the sale of Americans' sensitive data by data brokers. FTC Chairman Ferguson recently expressed his priorities for the Commission: investigating possible violations of antitrust laws, the over-use of non-compete, no-poach agreements and non-hire clauses, and regulating mergers. Unfortunately we can no longer depend

on the CFPB and FTC to protect consumers' private data, so we must enact a strong and readily enforceable comprehensive data privacy act in Massachusetts.

6. Enforcement of State Data Privacy Bills

The California Consumer Privacy Act (CCPA) took effect in July 2020. The CA Attorney General immediately began notifying companies of their compliance violations. Forty violations that were corrected by companies in 2021 and 2022 are listed on the CA AG Office's website, including for example: failing to process a consumer's request to opt-out of web tracking technologies; operating loyalty programs that offered financial incentives for the collection of consumers' personal information without informing consumers and obtaining their opt-in consent; not posting a privacy policy that listed consumer rights and the methods available to consumers to exercise their CCPA rights; a people search website had a "Do Not Sell My Personal Information" link that worked only on certain browsers and directed consumers to a confusing webpage that required several additional steps to submit CCPA requests; and a mobile app game installed software from a third-party mobile advertising platform that collected the personal information of players, including minors aged 13- to 15-years-old and did not provide any mechanisms for adults to opt-out or for minors to opt-in. All of these violations would also be prohibited by the MDPA. The requirement under the MDPA that the AG annually post reported violations by companies on their office's website encourages people to file complaints and enables repeated offenses to be addressed not only through civil action by the AG but by private right of action, potentially in class action suits.

The CA AG pursued enforcement actions against several companies.

The company Tilting Point Media LLC agreed to pay a penalty of $500,000 because the age screen for its popular mobile games app, "SpongeBob: Krusty Cook-Off", did not ask a user's age in a neutral manner, so children were discouraged from entering their age correctly, preventing them from being directed to a child-version of the game. Tilting Point also inadvertently misconfigured third-party software development kits (SDKs); consequently, collection and sale of minors' data occurred without parental consent. Dark practices, the failure to obtain parental consent, and the sale of minors' data would all be punishable under the MDPA.

Blackbaud, Inc., in a stipulated judgment, paid $6.75 million after violating consumer protection and privacy laws which resulted in a data breach. Non-profit organizations used Blackbaud's products and services and stored names, social security numbers, bank account information, and medical information, as well as other information in Blackbaud's databases. Blackbaud's failures to implement reasonable data security

practices, such as ensuring that old backup databases were deleted and implementing multi-factor authentication, enabled the illegal access of consumer data. In its settlement, Blackbaud agreed to improve its security to safeguard personal and protected health information. The MDPA enables enforcement against companies that fail to "ensure the data security and integrity of covered data in accordance with chapter 93H." It also requires that covered entities (CEs) include a general description of their own and any service providers' (SPs') data security practices in their privacy policy, and requires them to provide CE and SP contact information so that consumers can make inquiries about their data security practices.

DoorDash paid a settlement of $375,000 for selling the private information of its customers without giving them the opportunity to opt-out. The company was required to take steps to prevent future unlawful misconduct, which included reviewing contracts with marketing and analytics vendors, employing technology to assess whether the company sells or shares consumers' personal information, and furnishing annual reports to document any potential unapproved transfer of consumers' personal information.

Google paid $93 million in a settlement over allegations that it failed to secure the consent of its users before collecting, storing, and using their location data for consumer profiling and advertising. The company was compelled to prevent future violations by being transparent with and providing more information to its users whenever it enabled location-related account settings, by subjecting its location tracking practices to regular review by its internal Privacy Working Group, and by documenting the oversight group's approval of all material changes to location-setting and ads personalization disclosures that materially impact privacy.

The CA AG settled with Sephora, Inc., which paid $1.2 million in response to allegations that the company violated the CCPA by failing to disclose to consumers the sale of their personal information, and failing to process consumer opt-out of sale requests. Sephora was required to improve the clarity of its online disclosures and privacy policy, implement mechanisms for consumers to opt-out of the sale of personal information, revise its service provider agreements to comport with the CCPA's requirements, and provide reports to the AG. The MDPA has extensive requirements for contracts between covered entities and their service providers, and the same requirements apply to any companies with which the service provider chooses to subcontract its work.

In 2024, the Texas Attorney General launched investigations of Sirius XM, a subscription entertainment service, the weather app MyRadar, Miles, a travel rewards app, Tapestri, a data-purchasing app, and National Public Data, a data broker that

suffered a massive data breach, all for sharing sensitive user data without proper notice and consent.

He has also sued Allstate Insurance Company, and its subsidiary data analytics company, Arity, for collecting, using, and selling geolocation data of Texas drivers without their consent. Arity paid developers to incorporate software that it created into apps, which tracked the driving data of 45 million consumers countrywide.

A New York Times investigation revealed that companies including Ford, General Motors, and Kia/Hyundai were selling vehicle data to LexisNexis, who in turn sold it to insurance companies. Although the companies claimed that they had drivers' consent, the investigation revealed that the companies often did not get consent and in the cases where they had, the request for consent was in fine print in "murky privacy policies that few read." The MDPA requires privacy policies to be readily understandable, clearly displayed on the homepage of a company's website, and available in the language with which the company typically communicates with the consumer. Companies are required to get their customer's unambiguous affirmative consent for each instance of their data being transferred, but only after they have communicated to the consumer the purpose of the data transfer. Declining consent must be as easy as executing consent. The MDPA would enable the Massachusetts AG to launch investigations and civil suits against companies that abuse users' data, and would also allow consumers themselves to sue companies for damages, penalties, and injunctions.

7. Local, State and Federal Agency Use of Data Brokers and Social Media Monitoring Companies

As we catalog the pervasive use of data-mining programs by law enforcement it is important to recognize that artificial intelligence predictions about human behavior have been demonstrated to be deeply flawed.

Local and State Law Enforcement Agencies

Our own Massachusetts State Police contracted software from the company ShadowDragon. Without any warrant, the agency accessed a decade's worth of data from 120 online platforms which included social media, other internet sources, Amazon, dating apps, and the dark web, in order to use artificial intelligence to identify suspicious persons and their networks in Boston, Lawrence, Brockton, Worcester, New Bedford, and Springfield. The contract was paid for by the DOJ through Project Safe Neighborhoods. The software, according to ShadowDragon, can also be "automatically

adjusted to predict future violence and unrest". (This is just the kind of general warrant that James Otis' railed against in the colonial days of Massachusetts.)

During the Black Lives Matter protests, Dataminr, a databroker that monitors posts on Twitter, supplied law enforcement agencies and fusion centers countrywide with tweets and other social media content about the protests, including the geolocation data of those who posted the highlighted tweets.

The Brennan Center and Data for Black Lives (D4BL) reviewed 160,000 documents obtained in response to FOIA requests to the Washington, D.C. Metropolitan Police Department (MPD). They learned that, since 2015, the Washington Regional Threat Analysis Center, which is a nearby fusion center, had contracts with the data analytics company Babel Street and provided the MPD with social media information in response to search requests for terms including "protest," "demonstration," "rally," "armed," and "evacuation." The fusion center also prepared a spreadsheet listing social media accounts that were "geo-located in both Ferguson [Missouri] and Baltimore during times of unrest."

In 2017, before it purchased licenses for Dataminr, the MPD piloted the company's "First Alert" program and compiled information related to "riots" during President Trump's inauguration and the Women's March. During the same time period, the MPD Fusion Center piloted the social media monitoring tool, Sprinklr, to surveil anti-Trump protests using search terms that included #DisruptJ20, #RefuseFascism, #ResistTrump, #Anticapitalist, and #Antifa. Following President Trump's inauguration the MPD requested the use of additional search terms. A universal list contained the keywords "Active Shooter," "Evacuation," "Protests," "Terrorism/Terrorist," and "ISIS," and an additional list, targeting the DC area and focused on criminal activity, included terms ranging from "Graffiti" to "Stabbing" and "Shooting." The Brennan Center and D4BL reviewed 700,000 pages of emails from 2020 through 2022 sent by Dataminr to the MPD which contained "First Alerts" concerning "protests," including information captured in real time even when there was no apparent risk to public safety.

From 2022 through 2024, the MPD contracted with Transunion for use of its TLOxp service that tracks "addresses, emails, phones, assets, places of employment, bankruptcies and liens, criminal histories and more. TLOxp links subjects with license plate recognition data and social media profiles" and includes information for "over 95% of the U.S. population." MPD also contracted with LexisNexis, whose Accurint service boasts that it will enable law enforcement to "Quickly identify people, locations, and assets with our vast data sets."

A report by the Stop LAPD Spying Coalition in 2020 revealed the predictive policing practices employed by Los Angeles Police Department (LAPD). There was massive public outcry in response to the methods LAPD was using, which included a practice of investigating the social media of anyone who police stopped or questioned, even when those individuals were not charged with any crime. The people's names, birthdates, and social security numbers were written on Field Interview (FI) cards, and then their social media was surveilled in order to access social media friend lists and to determine who appeared in photos with the person online. This would lay the groundwork for prosecutions that alleged conspiracies or could identify people suspected of participating in a gang. However, Craig Uchida, who led the police consulting firm Justice and Security Strategies and created Operation LASER, LAPD's 2012 "predictive policing" program, admitted that LAPD did not necessarily conduct stops in order to investigate a crime. With respect to police stops and the generation of FI cards he professed "Most of the time it didn't lead to anything, but it was…data that went into the system, and that's what I wanted: more data about what was happening, who they were stopping and why." The practice of creating FI cards was terminated, but documents that the Brennan Center received from the LAPD after a lawsuit revealed that LAPD conducted and continued extensive social media monitoring by employing the services of Dataminr, Geofeedia, Media Sonar, and Voyager. Particularly disturbing was that, in discussing terms for a possible contract, Voyager claimed that its software would reveal the online network of thousands of a suspect's "friends" and monitor these accounts. **The company further professed to be able to determine people's motivations and ideologies, and to ascertain who in the network was the most vehemently dedicated to these beliefs**. Upon learning that Voyager was actually setting up fake Facebook accounts as part of their monitoring activity, Meta sued Voyager in 2023; the case is ongoing.

Federal Agencies

In the 2022 report of the Office of the Director of National Intelligence, DNI Avril Haines revealed that intelligence agencies were purchasing large quantities of commercially available information (CAI), and she warned that "It can be misused to pry into private lives, ruin reputations, and cause emotional distress and threaten the safety of individuals. Even subject to appropriate controls, CAI can increase the power of the government's ability to peer into private lives to levels that may exceed our constitutional traditions or other social expectations." Although she did not disclose the companies with which the intelligence companies contract, the source of all of the data from these data brokers is the information that companies collect from Americans who make purchases or use their services.

404 Media reported on its review of a trove of documents that the ACLU obtained through a lawsuit for FOIA information from the Immigration and Customs Enforcement Agency (ICE). The documents revealed that the agency has been using Giant Oak Search Technology (GOST), a social media monitoring program, both to identify immigrants who post derogatory information about the U.S. to inform enforcement decisions, and to screen non-immigrant visitors' social media posts, as ICE considers their visa applications and “through admission to the United States, and during their time in the United States.” In other words, derogatory posts from a visitor to the U.S. while they are here can lead to the revocation of their visa.

ICE has also had contracts with ShadowDragon and purchased its SocialNet software. Shadow Dragon surveils over 200 sites for ICE, including social networks, apps, and global services along with more obscure ones such as those that appeal to furries, car owners (Honda, Nissan, Toyota, Volkswagen, Subaru, Stellantis, and General Motors are all on the list), bodybuilders, book readers, users of multiple dating sites, house hunters, porn watchers, and technology-oriented sites like YCombinator and Github. Also on the list (somewhat surprisingly): TruthSocial and Rumble. ICE, Customs and Border Patrol, and other agencies within the Department of Homeland Security (DHS) purchase location data collected by the companies Venntel and Babel Street to track individuals’ movements. They can easily find specific undocumented immigrants through their real-time location data. In addition it was recently reported by 404 Media that ICE has requested the services of private companies to help it with "real-time threat mitigation and monitoring services," including the ability to assess "behavioral and social media sentiment" and "**track "negative references to ICE found in social media.”** This use of social media companies likely infringes on the free speech rights of Americans.

An article in FedScoop documented that the Secret Service purchased online contact records from companies including Zignal Labs and AT&T, and licensed a social media threat monitoring program from Creative Radicals. The Secret Service also purchased location data from Locate X.

The Department of Defense purchased location data from several sources including Babel’s Locate X and X-Mode. Data brokers specifically compiled location data on Muslims from a Muslim prayer app and a Muslim dating app. Once they identified users of these apps, they could supplement their data feed by collecting location information from other apps used by the same individuals, including a Craigslist app, an app for following storms, and a “level” app that is used, for example, to evenly install shelves.

In 2020, the Internal Revenue Service's (IRS's) enforcement division contracted with Digital Envoy for use of its NetAcuity location tracking program. After the company acquired X-Mode, the IRS signed a contract to use that service.

Politico reported that over 20 federal agencies contract with data brokers to verify the information that Americans are required to supply to them via Login.gov. Although the data brokers are not collecting the information from Login.gov, the lucrative federal contracts that they receive from the government are fueling their own data collection. The Politico article also revealed that the Department of Labor has a $528 million dollar contract with LexisNexis to help it identify fraud in state unemployment programs, and a contract for a blanket purchase agreement with TransUnion for fraud detection. The Department of Veterans Affairs employs Acxiom to conduct identity verification. While the latter agencies may not be directly involved in launching criminal investigations of Americans, it is very concerning that the information in their databases is being accessed by the Department of Government Efficiency (DOGE) affiliates of Elon Musk who have never had a required Tier2 background check nor received the compulsory GSA's Cyber Security and Privacy Training, and are not subject to discipline and penalties for violating the rules of behavior for employees and contractors who have access to Federal information. 21 original members of the U.S. Digital Service (USDS) (renamed DOGE by the current administration) resigned because they observed Musk's team to be "mishandling sensitive data" and "breaking critical systems." In a letter to White House Chief of Staff Susan Wiles, they wrote that: "We will not use our skills as technologists to compromise core government systems, jeopardize Americans' sensitive data, or dismantle critical public services."

Conclusion

All of the above demonstrate the urgency of enacting comprehensive data privacy legislation. The Massachusetts Data Privacy Act is an excellent bill largely based upon the American Data Privacy Act, which would have been enacted by Congress had it not preempted the California Data Privacy Act. It contains the additional invaluable provision that enables consumers to have their data removed from the databases of all data brokers operating in MA via a free automated mechanism and provides for the enforcement of these requests.

The California Consumer Privacy Act (CCPA) was the first comprehensive data privacy legislation to be enacted by a state, and while it was good, it was subsequently amended and strengthened in 2023 by the California Privacy Rights Act. Eighteen other states have enacted comprehensive privacy legislation, but these laws are significantly less effective than California's as a result of extensive lobbying by big tech companies, which have either directly originated bills or demanded legislatures to water them down or governors to veto them. Much of this lobbying was done by a man named Andrew

Kingman who is funded by the tech industry group the State Privacy & Security Coalition. He speciously enlists small businesses located throughout each state and asks them to contact their state legislators in opposition to the data privacy bill, making this opposition appear to be a grassroots movement rather than one promoted by Amazon, Google, Facebook, and other large data holders. By enacting a strong, comprehensive data privacy act in Massachusetts with a private right of action, we will stem the tide of data being collected, profiled, and sold by data brokers and by empower MA residents to have their data deleted from data broker's databases we will ensure that it is neither abused in the future nor leaked in a data breach.