Consumer Federation of America
1620 I Street, N.W., Suite 200 * Washington, DC 20006

Testimony of Susan Grant, Director of Consumer Protection and Privacy
Consumer Federation of America
To the Massachusetts Legislature Joint Committee on Advanced Information Technology, the Internet and Cybersecurity
October 12, 2012

On behalf of Consumer Federation of America (CFA), an association of nonprofit consumer organizations across the United States, including in Massachusetts, I am submitting testimony in support of S. 46,[1] an Act establishing the Massachusetts Information Privacy Act (MIPA) and H. 136,[2] an Act relative to privacy. Founded in 1968 to advance consumers' interests through research, education, and advocacy, CFA strongly supports states' efforts to enact privacy legislation. A seminal survey conducted two years ago by the Pew Research Center showed that, by large majorities, adults in the U.S. feel they have little or no control over the data companies collect about them, are concerned about how their data are used, and believe that the potential risks of such data collection outweigh any benefits they may derive from it. A strong majority also say that they have little or no understanding of what companies do with their data. Seventy-five percent said that there should be more government regulation over what companies can do with their personal information.[3]

It's is not surprising that many people are in the dark about companies' privacy practices because the system of commercial surveillance that has developed in the absence of comprehensive state or federal privacy laws is largely invisible to individuals. In many cases data is being collected about them by entities with which they have no direct relationship – for instance, by third-party "ad tech" companies that lurk on the websites they visit and data brokers that obtain information about them from public records and proprietary databases. Even entities with which people interact directly, such as Google and Facebook, are engaged in much more extensive tracking and profiling than users may realize though that is changing as more scandalous revelations come out, seemingly weekly, about their data collection

[1] S. 46, available at https://malegislature.gov/Bills/192/S46.
[2] H. 136, available at https://malegislature.gov/Bills/192/H136.
[3] Brooke Auxier, Lee Rainie, Monica Anderson, Andrew Perrin, Madhu Kumar and Erica Turner, *Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information*, Pew Research Center (November 15, 2019), https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/.

and use. A recent petition by the organization Accountable Tech asking the Federal Trade Commission (FTC) to initiate a rulemaking on "surveillance advertising" provides an excellent explanation of Google's and Facebook's business models and describes the commercial surveillance system more broadly.[4] To help policymakers understand this type of advertising and the concerns it raises, CFA has created factsheets and other materials, which are available at a central hub, https://consumerfed.org/surveillance-advertising-factsheets/.

It is not necessary to know individuals' names, physical addresses or phone numbers in order to collect their personal data and draw inferences about them and their households. As CFA's factsheet on tracking for surveillance advertising[5] explains, people can be tracked in a variety of ways without their knowledge as they go about their daily lives. Even when individuals are aware of the ubiquitous tracking that takes place in the commercial surveillance system, it is extremely difficult for them to avoid it and the profiling that it facilitates.

These profiles may not be accurate. For instance, a person could be shopping and doing other errands for an elderly relative, or researching a problem that a friend is experiencing, but the data that are collected through these activities may be linked to that person, not the relative or friend, through the device that is being used, an associated account, location data or some other type of information. Even if the assumptions made about the person are accurate, however, they may be unfair or undesirable. CFA's fact sheet on surveillance advertising and discrimination[6] provides examples of how profiling can result in opportunities for employment, housing and credit being presented to some individuals and not others, or some people being charged more than others for the same products or services. As CFA's general fact sheet about surveillance advertising[7] explains, these data practices can also be used to promote unhealthy products, encourage gambling, perpetrate fraud, and for other purposes that are very concerning. Furthermore, the enormous stores of personal data collected in the commercial surveillance system put individuals at risk for exposure, identity theft, and more malicious tracking. In addition, their 4th Amendment rights may be eroded, as government agencies can purchase data that otherwise requires a warrant.

---

[4] *See* https://accountabletech.org/media/accountable-tech-petitions-ftc-to-ban-surveillance-advertising-as-an-unfair-method-of-competition/.
[5] *See* https://consumerfed.org/consumer_info/factsheet-surveillance-advertising-how-tracking-works/.
[6] *See* https://consumerfed.org/consumer_info/factsheet-surveillance-advertising-discrimination/.
[7] *See* https://consumerfed.org/consumer_info/factsheet-surveillance-advertising-what-is-it/.

It is important to understand how this system works in order to develop public policies that effectively protect individuals from harm and ensure their fundamental rights to privacy are respected. Without that understanding, legislation can result in only the illusion of privacy. For instance, the Consumer Data Protection Act (CDPA)[8] enacted earlier this year in Virginia gives people the ability to opt-out of "sale" of their personal data, but "sale" is narrowly defined as the exchange of personal data for monetary consideration by the controller to a third party.[9] That is not how the commercial surveillance system generally works. It is not individuals' personal information that is for sale (except by data brokers, who may provide additional information to enrich their profiles) but the ability for companies to have advertisements for their product or services delivered to people who meet certain profiles, which are created by tracking them over time and space. CFA's diagram of how surveillance advertising works[10] illustrates this. Therefore, Virginians' right to opt-out of sale has little practical effect.

The right to opt-out of targeted advertising in the Virginia law also provides less privacy protection than one might assume. By excluding advertisements based on activities within a controller's own websites or online applications from the definition of targeted advertising,[11] Google and Facebook are not covered, despite the fact that their business models are based on collecting huge amounts of personal data from tracking their users' activities across their many websites and apps, profiling them, and delivering targeted ads to them on behalf of other companies. The CDPA has many other several serious shortcomings as well.[12]

Having to opt-out of specific data practices places far too heavy a burden on individuals to understand the implications and take steps to exercise the options they are provided. But even Virginia residents who make the effort to opt-out of sale of their data, targeted advertising, and/or profiling (another very

[8] CDPA, Code of Virginia, Title 59, Chapter 52, §59.1-571 through §59.1-581, available at https://lis.virginia.gov/cgi-bin/legp604.exe?212+ful+CHAP0036+pdf.
[9] *Id.* §59.1-571.
[10] *See* https://consumerfed.org/consumer_info/factsheet-surveillance-advertising-diagram/.
[11] CDPA §59.1-571.
[12] CFA has pointed these out in a number of letters, press releases and opinion pieces. *See* https://consumerfed.org/press_release/virginia-legislature-ignoring-consumer-groups-steamrolls-bad-privacy-bill-toward-enactment/, https://consumerfed.org/testimonial/cfa-and-other-groups-weigh-in-on-va-privacy-bill/, https://www.virginiamercury.com/2021/02/16/we-need-real-privacy-protection-in-virginia/, https://roanoke.com/opinion/columnists/leech-grant-and-mierzwinski-privacy-law-isnt-strong-enough/article_ef16e92c-7d4c-11eb-a448-9f3858a2eb94.html, https://consumerfed.org/press_release/consumer-and-privacy-groups-urge-virginia-governor-to-veto-or-send-privacy-bill-back-to-legislature/, https://consumerfed.org/testimonial/cfa-urges-va-legislative-work-group-to-recommend-changes-to-strengthen-data-protection-law/.

limited right the law provides) will not have the privacy protection they are led to expect because, with its narrow definitions, numerous exemptions and exceptions, and reliance on notice and opt-out rather than privacy by default, the CDPA does not change the way the commercial surveillance system works.

The Massachusetts legislature is taking a better, more informed approach. Both S. 46 and H. 136 are worthy of consideration. The MIPA recognizes that monetization is at the heart of the commercial surveillance system and that the issue is not whether individuals' personal information changes hands but how it is used.[13] There is no carve-out from the definition of targeted advertising for Google and Facebook. It puts individuals' privacy interests first by stressing the need for covered entities and data processors to be honest about what they're doing with personal data, adequately secure the data, refrain from using the data in ways that benefit them to the detriment of individuals or is harmful, unexpected or offensive, and ensure that entities with which they share the data fulfill the same duties of care, loyalty and confidentiality.[14] It gives individuals basic rights to access, port, correct and delete their data,[15] to know what data will be collected and how it will be used,[16] and to consent – that is, to opt-in to their data being collected and processed for specific purposes.[17] Coercion and manipulation to obtain consent are prohibited, and individuals cannot be refused goods or services, forced to pay more for them, or receive lower-quality goods or services if they do not provide consent. There are reasonable exceptions for data collection and uses that are necessary to fulfill individuals' requests and for bona fide loyalty programs.

The MIPA also gives individuals the right to know to whom their data will be disclosed and refuse that disclosure.[18] No disclosure could be made to third parties without individuals' consent, nor could personal data from third-parties be processed without their consent. There could be no surreptitious surveillance through cameras, microphones, sensors and the like – collecting and transmitting audio, video or certain other types of data would require consent.[19] Children's privacy would be protected as it is under federal law.[20] Collecting and processing individuals' biometric and location information, which are especially sensitive, would require obtaining consent through a special procedure and be subject to

[13] MIPA Section 1.
[14] *Id.* Section 2.
[15] *Id.* Section 3.
[16] *Id.* Section 4.
[17] *Id*. Section 5.
[18] *Id*. Section 6.
[19] *Id*. Section 7.
[20] *Id*. Section 8.

specific retention, deletion, and disclosure requirements.[21] This section also prohibits monetizing those types of data.

Individuals would have the right not to be subject to processing of their data that results in unlawful discriminatory actions and would also be protected from various discriminatory practices.[22] Covered entities that process personal information would be subject to Massachusetts chapter 93A and barred from engaging in unfair and deceptive trade practices such as taking advantage of individuals' lack of understanding about the risks, costs or conditions of processing their personal information.[23]

Crucially, the MIPA would create a Massachusetts information privacy commission to conduct research, issue studies and other publications, adopt regulations, carry out investigations, hold adjudicatory proceedings, impose civil penalties for violations, refer cases to appropriate authorities for criminal prosecution, educate the public, and carry out other oversight functions.[24] CFA strongly supports this provision and has also advocated for a federal data protection authority, as exists in most other nations around the world, because data protection requires special expertise in order to understand complex issues and evolving technology, and dedicated resources to ensure that problems are addressed quickly when they arise, everyone understands their rights and responsibilities, and the rules are followed.

Of course, the civil administrative penalties[25] provided for in the bill are very important, but equally important are the judicial enforcement rights it would provide to the attorney general's office and individuals.[26] Some problems with noncompliance will be able to be resolved informally, as is already done in many cases when it appears that there may be violations of consumer protection laws. There is nothing to prevent the Massachusetts information privacy commission or the attorney general's office from reaching out to businesses to discuss issues that arise and how they might be addressed. But the government and individuals must be able to take formal action when they deem it necessary to enforce people's rights and obtain redress.

This is very important because one of the arguments that Massachusetts legislators are sure to hear from big tech companies and the advertising industry is that there should be a "right to cure." That is, businesses should be entitled to receive warnings that they may not be in compliance and have a certain

[21] *Id*. Section 9.
[22] *Id.* Section 10.
[23] *Id.* Section 11.
[24] *Id.* Section 12.
[25] *Id*. Section 13.
[26] *Id*. Section 14.

amount of time to change their errant practices. If they do so, no formal action may be initiated against them. The right to cure is not commonly provided for violations of other consumer protection laws and there is no reason why there should be such a right here.

The first comprehensive privacy law to be enacted in state, the California Consumer Privacy Act (CCPA), includes a right to cure,[27] but voters decided last year to replace that law with the Consumer Privacy Rights Act[28] which, when it takes effect in 2023, will not include that provision. Unfortunately, the right to cure is in the Virginia privacy law and some privacy bills in other states. It is a terrible idea for several reasons: it allows companies to avoid penalties, even for egregious violations, if they claim to have stopped engaging in the violations and promise not to commit them again; it provides no public transparency in regard to companies' errant behavior; it results in no redress for individuals who have been harmed; it creates no legal precedents to guide enforcement agencies and businesses; and it provides no reimbursement for the costs of investigations, which can be substantial.

The MIPA sets out reasonable exceptions to certain requirements; for instance, consent for processing personal information is not necessary to execute a specific transaction that the individual wants to make, as long as the data are not used for other purposes.[29] There are good provisions for transparency about legal requests for individuals' data[30] and for non-applicability to certain types of personal information, such as specific data collected by health care providers and used for specific purposes.[31]

It is important to ensure that any exemptions or exceptions are as narrow as possible because they can create huge loopholes for privacy protection and an uneven playing field for businesses. For example, the Virginia law exempts financial institutions that are covered by the federal Gramm-Leech-Bliley Act[32] even though that law does not provide equivalent or stronger privacy rights. This leaves individuals less protected in regard to the personal information that banks, insurance companies and other financial

[27] *See* CCPA §1798.155. https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5.
[28] See text of Proposition 24, the California Privacy Rights Act, which will replace the CCPA, https://vig.cdn.sos.ca.gov/2020/general/pdf/topl-prop24.pdf.
[29] MIPA Section 16.
[30] *Id*. Section 17.
[31] *Id*. Section 18.
[32] *See* Code of Federal Regulations, Title 17, Chapter 1, Part 160, available at https://www.ecfr.gov/current/title-17/chapter-I/part-160.

institutions collect, use, share and retain, and places greater privacy obligations on retailers and other types of businesses than financial institutions have.

Finally, the MIPA would not preempt local or state laws that provide stronger privacy protections for individuals and would apply to businesses that are subject to federal laws to the extent that it provides stronger privacy protections than those laws do (absent federal preemption). Massachusetts residents should be able to expect that their privacy will be respected and protected no matter what types of businesses are involved.

H. 136 would also create a dedicated agency, the Massachusetts Data Accountability and Transparency Agency.[33] Its duties would include ensuring that data practices are fair, just and nondiscriminatory, provide public education; collecting, researching and responding to complaints; examining the social, ethical, economic, and civil rights impacts of high-risk data practices and proposing remedies; conducting rulemaking; enforcing the law, and coordinating with other state agencies that have responsibilities to protect privacy.[34]

One of the most interesting aspects of the bill is that it would require the agency to set up a publicly available website and database through which "data aggregators," which are defined in Section 1 as any person that collects, uses, or shares personal data that is not de minimis (this does not apply to individuals who collect, use or share personal data solely for personal reasons) would report the types of personal data they collect, use and share, and individuals would be able to exercise their rights.[35] There would also be a searchable list of complaints (with individuals' personal data removed). This transparency is much needed in light of the invisibility of data practices.

The heart of H. 146 is the concept of permissible purposes.[36] Data aggregators would not be allowed to collect, use, or share personal data, or cause personal data to be collected, used or shared, unless they can demonstrate that it is strictly necessary to do so carry out a purpose such as providing a good or service an individual has requested, engaging in journalism or in certain research (with some caveats), employing an individual (again, with some limitations), detecting and responding to security incidents, and for other well-defined operational purposes. Use of data for contextual advertising – that is, showing ads to individuals based on the content of the websites, online services, or apps they are using

[33] https://malegislature.gov/Bills/192/H136, Section 2.
[34] *Id.* Section 3.
[35] *Id.* Section 6.
[36] *Id.* Section 9.

at that moment, not on personal data collected about them from previous interactions, tracking their behavior over time and space, or profiles that have been created about them – is permissible. As CFA's factsheet about contextual advertising versus surveillance advertising[37] explains, contextual advertising does not raise the privacy concerns that surveillance advertising does and is as effective and less costly for advertisers.

There is a reasonable exception for tracking individuals' purchases for purposes of offering discounts or free goods or services under loyalty reward programs. It would be unlawful to charge individuals higher prices, refuse to provide or degrade products or services, or otherwise retaliate against them for exercising their rights under the law. There are also strong provisions against illegal discrimination, intimidating, threatening or coercing individuals with the intent of depriving them of the rights provided by the law, and using personal data in a manner that deprives or defrauds, or attempts to deprive or defraud, individuals of their voting rights.

H. 136 has provisions similar to those in S. 46 in regard to the disclosures that must be made in data aggregators' privacy policies and individuals' rights to see the personal data collected about them, to know the sources of such data, to know the purposes for which the data have been collected, used or shared, to correct their data, to port their data, and to delete the data if they are not needed.[38] Furthermore, for any material decisions that data aggregators make about individuals based on automated processing of their personal data, the aggregators must inform them of what personal data were used and provide them with an easily available mechanism to request human review of the decisions. There are also strong provisions for ensuring that personal data are adequately secured and not retained longer than it is needed for a permissible purpose.[39]

The bill provides for a private right of action,[40] corporate accountability,[41] penalties for CEOs and Boards of Directors in certain situations,[42] and whistle blower protections.[43] These are essential in order to provide the law with real teeth.

---

[37] *See* https://consumerfed.org/consumer_info/factsheet-surveillance-advertising-contextual-is-good-alternative/.
[38] https://malegislature.gov/Bills/192/H136, Section 11.
[39] *Id*. Section 12.
[40] *Id*. Section 14.
[41] *Id*. Section 15.
[42] *Id*. Section 16.
[43] *Id.* Section 17.

H. 136 is in many ways simpler and more privacy-protective for individuals than S. 46 because there is no need for them to take action to protect their personal data from unwanted collection, use and sharing. Both bills are likely to be attacked by big tech companies and the advertising industry, however, because they would change the paradigm from the ineffective notice and opt-out approach that underpins self-regulatory programs and privacy laws such as Virginia's. They will claim that this will be the end of the Internet as we know it. That is nonsense. They will say that individuals will no longer be offered services for free because those services are supported by advertising, without acknowledging that there are different forms of advertising and that contextual advertising works just fine. They will contend that people are willing to trade their privacy for discounts or other benefits. But as a study[44] conducted by Professor Joe Turow and colleagues at the University of Pennsylvania showed, people are not happy about making such trade-offs:

- 91 percent disagreed (77 percent of them strongly) that "If companies give me a discount, it is a fair exchange for them to collect information about me without my knowing."
- 71 percent disagreed (53 percent of them strongly) that "It's fair for an online or physical store to monitor what I'm doing online when I'm there, in exchange for letting me use the store's wireless internet, or Wi-Fi, without charge."
- 55 percent disagreed (38 percent of them strongly) that "It's okay if a store where I shop uses information it has about me to create a picture of me that improves the services they provide for me."

They concluded that conduct which has been misconstrued as trade-off behavior is actually due to the fact that "a large pool of Americans feel resigned to the inevitability of surveillance and the power of marketers to harvest their data."

Massachusetts can change that by enacting legislation that doesn't force individuals to trade their privacy for the ability to shop, search for information, enjoy entertainment, find their way, connect to others, get the services they need, and do other things that are integral to their daily lives.

---

[44] Joseph Turow, Michael Hennessy, and Nora A. Draper, *The Tradeoff Fallacy - How Marketers Are Misrepresenting American Consumers and Opening Them up to Exploitation*, University of Pennsylvania Annenberg School of Communication (June 2015), available at https://repository.upenn.edu/cgi/viewcontent.cgi?article=1554&context=asc_papers.