Testimony of Willmary Escoto, U.S. Policy Analyst at Access Now
To the Joint Committee on Advanced Information Technology, the Internet and Cybersecurity
In Support of S.46 (Massachusetts Information Privacy Act) and S.48 (Internet Freedom Act)
October 15, 2021

Dear Senator Finegold, Representative Campbell, and members of the committee:

Thank you for holding this week's hearing on bills related to data use, data privacy, the Internet, and broadband access. I am writing on behalf of Access Now in support of S.46, An Act establishing the Massachusetts Information Privacy Act ("MIPA") and S.48, An Act to ensure a free and open internet in the commonwealth, also known as the Internet Freedom Act ("IFA"), both of which provide critical protections.

Access Now is an international organization that defends and extends the digital rights of users at risk around the world. By combining innovative policy, user engagement, and direct technical support, we fight for a free and open internet that fosters human rights. As part of this mission, we operate a global helpline for at-risk populations to mitigate online threats. Additionally, we work directly with lawmakers at local, national, and international levels to ensure policy decisions are focused on the rights of people, particularly underrepresented populations. As an organization, we have focused extensively on data protection and connectivity issues.[1]

Access Now Supports MIPA

MIPA is a strong comprehensive privacy bill and this committee should move it forward. States should be enacting privacy protections given the failure of Congress to pass a federal comprehensive privacy law. Below, I argue that privacy is a fundamental human right and of critical importance in today's society. Then, I describe specific aspects of MIPA that empower online autonomy and choice, and increase overall privacy protection.

Privacy Is a Fundamental Right and Is Important to People

Privacy is a fundamental human right, but most people do not understand how their data is mined and used by companies all over the world, and similarly have minimal control over those practices.[2] Companies discreetly collect, process, store, and disclose unprecedented quantities of private, personal information about every one of us. Such extensive and granular data collection reveals a lot about a person, and this is especially dangerous for historically marginalized individuals and communities. While data minimization (the concept that a company shall collect only as much data as is necessary to provide its service) has been a core privacy principle for decades, very few companies take it seriously.[3]

---

[1] *See* https://www.accessnow.org/issue/privacy and https://www.accessnow.org/issue/net-discrimination.
[2] Brooke Auxier *et al*., *Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information*, Pew Research Center (Nov. 15, 2019), https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/.
[3] *See generally* Eric Null, Isedua Oribhabor, and Willmary Escoto, *Data Minimization: Key to Protecting Privacy and Reducing Harm*, Access Now (May 2021), https://www.accessnow.org/cms/assets/uploads/2021/05/Data-Minimization-Report.pdf.

The public dislikes these data practices and wants the government to do something about it, and rightfully so.[4] "Nearly three-quarters of Americans want the federal government to establish national privacy standards."[5] According to a poll released last month, nearly 60 percent of people believe their social media activity and location information is not safe.[6]

Private information is susceptible to breaches and leaks, more than ever before, and can cause irreparable harm to people, especially communities of color. For example, one recent study revealed that women, black people, indigenous people, and people of color are more likely to be victims of cybercrimes, particularly identity theft.[7] A few years prior, the Federal Trade Commission found similarly that "African American and Latino consumers were more likely to be fraud victims than non-Hispanic whites."[8]

Over twenty states have already introduced their own privacy bills while Congress has not found common ground to pass a national privacy framework.[9] A survey of Republicans and Democrats showed people of both parties want state legislatures and Congress to prioritize privacy legislation, with 75% of respondents placing responsibility on state legislatures to act, and 72% saying Congress should act.[10]

Major hacks of social media platforms are becoming more and more common and affecting millions of people, necessitating stronger privacy protections to help avoid such exposure. In January 2021, a Chinese social media management company called Socialarks exposed information gathered from 214 million Facebook, Instagram, and LinkedIn profiles—information like full names, subscriber data, country of residence, phone numbers, and other contact information.[11] In April 2021, the credit

---

[4] Emily A. Vogels, *56% of Americans support more regulation of major technology companies*, Pew Research Center (July 20, 2021), https://www.pewresearch.org/fact-tank/2021/07/20/56-of-americans-support-more-regulation-of-major-technology-companies/;

[5] Chris Mills Rodrigo, *Majority of Americans support national data privacy standards: poll*, The Hill (Sept. 16, 2021), https://thehill.com/policy/technology/572607-majority-of-americans-support-national-data-privacy-standards-poll. According to the Pew Research Center, 56% of Americans think major technology companies should be regulated more than they are now, which is a 9-point increase year over year, and 68% believe these firms have too much power and influence in the economy. Vogels, *supra*.

[6] Rodrigo, *supra*.

[7] Tonya Riley, *Cybercrime is hitting communities of color at higher rates, study finds*, Cyberscoop (Sept. 27, 2021), https://www.cyberscoop.com/cybercrime-demographics-bipoc-malwarebytes/.

[8] *Combating Fraud In African American & Latino Communities: The FTC's Comprehensive Strategic Plan: A Federal Trade Commission Report To Congress*, FTC (June 15, 2016), https://www.ftc.gov/system/files/documents/reports/combating-fraud-african-american-latino-communities-ftcs-comprehensive-strategic-plan-federal-trade/160615fraudreport.pdf at i.

[9] Sam Sabin, *States Are Moving on Privacy Bills. Over 4 in 5 Voters Want Congress to Prioritize Protection of Online Data*, Morning Consult (Apr. 27, 2021), https://morningconsult.com/2021/04/27/state-privacy-congress-priority-poll/.

[10] *Id*.

[11] *Chinese start-up leaked 400GB of scraped data exposing 200+ million Facebook, Instagram and LinkedIn users,* Safety Detectives (Jan. 11, 2021), https://www.safetydetectives.com/blog/socialarks-leak-report/.

reporting agency Experian got hacked, compromising the private credit reports of millions of people.[12] Recently, in August 2021, T-Mobile learned that a bad actor illegally accessed and acquired personal data and compromised over 50 million customers, former customers, and prospective customers, including SSN, name, address, date of birth, and driver's license.[13]

Massachusetts residents cannot control their own digital identity without a modern data protection law. MIPA can lead the way and set an example for other states to follow.

MIPA Includes Several Provisions that Empower Choice and Protect Privacy

Massachusetts should enact strong data protection legislation for its people to remedy the shortcomings in U.S. law. MIPA provides a comprehensive privacy framework that would significantly change the privacy landscape in the state, particularly on protections for biometric and location data, consumer rights, and civil remedies. Below, I focus on four important provisions in MIPA that should be retained.

MIPA gives users more power over their data. MIPA gives people the right to access, correct, transfer, and delete their personal information. Currently, people who use online services generally must fully agree with the company's data practices, or they cannot use the service. There is no in-between. MIPA would at least give people more control over the data companies collect about them, allowing them to better control their online identities. Specifically, MIPA would allow people to access the data a company has collected about them, and if that person finds errors, or simply wants that data deleted or moved to another service, they are entitled to take those actions. These provisions offer important rights that are often missing, or difficult to take advantage of, online.

Data portability is important for increasing online competition as well. By allowing individuals to obtain and move their data across different services, MIPA increases individuals' agency over their information and choices and promotes "competition by allowing new entrants to access data they otherwise wouldn't have, enabling the growth of competing platforms and services."[14] A few large players have a significant advantage over small start-ups, namely, "massive data sets collected over

[12] Becky Bracken, *Experian API Leaks Most Americans' Credit Scores*, Threatpost (Apr. 29, 2021), https://threatpost.com/experian-api-leaks-american-credit-scores/165731/; *see also* Scott Kieda, *Another Data Leak for Experian; Credit Scores of Americans Were Available to Anyone Due to API Security Issue*, CPO Magazine (May 3, 2021), https://www.cpomagazine.com/cyber-security/another-data-leak-for-experian-credit-scores-of-americans-were-available-to-anyone-due-to-api-security-issue/.

[13] Mike Sievert, *The Cyberattack Against T-Mobile and Our Customers: What Happened, and What We Are Doing About It*, T-Mobile (Aug. 27, 2021), https://www.t-mobile.com/news/network/cyberattack-against-tmobile-and-our-customers.

[14] Lesley Fair, *Data portability is the topic at September 22nd FTC workshop*, FTC (Mar. 31, 2020), https://www.ftc.gov/news-events/blogs/business-blog/2020/03/data-portability-topic-september-22nd-ftc-workshop.

years, if not decades."[15] The ability for people to transfer data histories directly to those smaller competitors increases their ability to compete.

MIPA heightens protections for biometric and location data. MIPA would require covered entities to inform in writing and obtain handwritten consent by individuals when collecting and processing location or biometric data and additional consent to disclose it to third parties. Covered entities would also be required to establish a retention schedule and guidelines for permanently destroying biometric or location data, and the bill places limits on the data's monetization.

The collection and use of biometric data, particularly face data, poses significant risks to individuals.[16] Processing biometric data can lead to error and present extreme risks to privacy and civil rights. Data collection and processing can "reduce opportunities for Black, Hispanic, Indigenous, and other communities of color, or actively target them for discriminatory campaigns and deception."[17] Biometric surveillance is becoming an all-encompassing tool for the companies to track where we are, what we are doing, and who we are with, regardless of whether we are suspected of a crime. For example, a mobile analytics company called Mobilewalla collected location data, device IDs, and browsing histories from over 16,000 devices in Black Lives Matter protests in several major cities across the USA. With that data, Mobilewalla used "artificial intelligence" to predict people's demographics like race, age, gender, and zip code.[18] The protestors likely had no idea the company was collecting and processing data in such an intrusive way.

The collection of location data is also particularly harmful. Recently, the Federal Communications Commission took enforcement action against the then-four major wireless providers because they were selling location data to third parties.[19] Those third parties in turn sold that data to a variety of other entities, including bounty hunters.[20] Not only can location data lead to physical harm like data being sold to bounty hunters, but can also be used to target people in private situations, such as when

---

[15] Eric Null & Ross Schulman, *The Data Portability Act: More User Control, More Competition*, Open Technology Institute (Aug. 19, 2019), https://www.newamerica.org/oti/blog/data-portability-act-more-user-control-more-competition.

[16] Access Now and over 175 civil society organizations, activists, and researchers from across the globe are calling for a ban on uses of facial recognition and remote biometric recognition that enable mass and discriminatory targeted surveillance, https://www.accessnow.org/civil-society-ban-biometric-surveillance/.

[17] Null *et al.*, *Data Minimization: Key to Protecting Privacy and Reducing Harm*, *supra*; *see also* Cameron F. Kerry, *Federal privacy legislation should protect civil rights*, Brookings Institute (July 16, 2020), https://www.brookings.edu/blog/techtank/2020/07/16/federal-privacy-legislation-should-protect-civil-rights.

[18] C. Fisher, *Demographic report on protests shows how much info our phones give away*, Engadget (June 25, 2020), https://www.engadget.com/mobilewalla-data-broker-demographics-protests-214841548.html; *see also* Caroline Haskins, *Almost 17,000 Protesters Had No Idea A Tech Company Was Tracing Their Location*, Buzzfeed News (June 25, 2020), https://www.buzzfeednews.com/article/carolinehaskins1/protests-tech-company-spying.

[19] Press Release, *FCC Proposes over $200 Million in Fines against Four Largest Wireless Carriers for Apparently Failing to Adequately Protect Consumer Location Data*, FCC (Feb. 28, 2020), https://docs.fcc.gov/public/attachments/DOC-362754A1.pdf.

[20] Joseph Cox, *I Gave a Bounty Hunter $300. Then He Located Our Phone*, Motherboard (Jan. 8, 2019), https://www.vice.com/en/article/nepxbz/i-gave-a-bounty-hunter-300-dollars-located-phone-microbilt-zumigo-tmobile.

one anti-abortion group used location data to serve ads to women seeking abortions and people at methadone clinics.[21]

Companies are working hard to develop biometric and artificial intelligence systems based on biometric data, and they are doing it with essentially no safeguards.[22] Without reasonable limits, biometric technologies threaten to enable companies (and by extension, law enforcement) to pervasively track people's movements and activities in public and private spaces and risk exposing people to forms of identity theft that are particularly hard to remedy. MIPA places reasonable limits on the processing of biometric and location information.

MIPA prohibits the use of deceptive interface designs used to obtain consent. MIPA prohibits companies from obtaining consent through the use of a variety of interface designs that often confuse or mislead people into consenting to particular data practices. For instance, the bill prevents obtaining consent in ways that ask questions or provide information in ways that people cannot reasonably understand, increase the work for the person to consent or not consent, or hide desired content or interface elements. MIPA would also create a new information privacy commission and require it to develop a recognizable and uniform logo or button to promote short-form privacy notices.

Companies have increasingly been employing deceptive design interfaces (also known as "dark patterns") to influence individual choice online and MIPA would provide safeguards for consumer autonomy. Access Now defines dark patterns as a "user interface design choice in a product or service that attempts to influence a person's decision, often toward a decision that is against the person's best interests and in favor of the provider's interest."[23] Dark patterns are a serious concern, as they can cause extensive harm to people, particularly vulnerable people. These deceptive interface designs are especially effective against those without a college education and the elderly because these populations may lack the skills, knowledge, or ability to understand how these practices work.[24] Dark patterns can lead people to over-share personal information, potentially leading to harms like data breaches. For example, 'Privacy Zuckering,' named after Facebook's CEO, is when an online platform tricks someone into publicly sharing more information about themselves than intended.[25]

Given the pervasive use of dark patterns by major online companies, MIPA's limitations on these harmful practices are necessary to protect people from the harm that stems from them. By prohibiting

---

[21] Sharona Coutts*, Anti-Choice Groups Use Smartphone Surveillance to Target 'Abortion-Minded Women' During Clinic Visits,* Rewire News Group (May 25, 2016), https://rewirenewsgroup.com/article/2016/05/25/anti-choice-groups-deploy-smartphone-surveillance-target-abortion-minded-women-clinic-visits/.

[22] For this and other reasons, the UN human rights chief recently called for a ban and moratorium on certain uses of AI. *Urgent Action Needed over Artificial Intelligence Risks to Human Rights*, United Nations (Sept. 15, 2021), https://news.un.org/en/story/2021/09/1099972.

[23] Eric Null and Willmary Escoto, *Comments to the Federal Trade Commission Re: Topics to be Discussed at Dark Patterns Workshop (Docket ID: FTC-2021-0019-0001)*, Access Now (May 28, 2021), https://www.accessnow.org/cms/assets/uploads/2021/06/Access-Now-Dark-Patterns-Comments-Final-May-28-2021.pdf, at 1.

[24] *Id*. at 5-6.

[25] *See id.* at 3-4; *see also* Privacy Zuckering, DarkPatterns.Org, https://www.darkpatterns.org/types-of-dark-pattern/privacy-zuckering.

the use of deceptive design interfaces, and requiring a uniform logo button to promote short-form privacy notices, MIPA protects consumers and ensures individual autonomy by limiting the use of design tricks that coerce customers into wasting time, money, or sharing private information. If companies do not follow those rules, MIPA would hold those companies to account.

MIPA ensures robust enforcement with a private right of action. MIPA creates a private right of action that will allow aggrieved people to hold the violator directly accountable in state court. A privacy law is only as effective as its enforcement, and allowing individuals to bring lawsuits will help ensure companies comply with the law.

Other private rights of action have been successful. For example, Illinois's biometric privacy law allows users whose biometric data is illegally collected or handled to sue the companies responsible.[26] The private right has been used to take action against Clearview AI for scraping the facial data of millions of people online.[27] It has also been used to take action against Facebook's practice of tagging people in pictures with facial recognition software without consent.[28] Without a private right of action, individuals have to rely on federal or state enforcers, like the FTC, to protect their privacy. However, "[m]arginalized communities historically have not been able to rely upon the government to protect their interests, so individuals need to be able to vindicate their own rights."[29] Thus, MIPA should include a private right of action.

MIPA is a positive framework for privacy protection and will place the burden of protecting against harmful practices on the companies that collect and use the data rather than the people, and will help users take back control of their personal information. For these reasons and others, Access Now supports MIPA and hopes the legislature will act on it.

Access Now Supports IFA

Access Now also supports S.48, the "Internet Freedom Act." Much like privacy, the federal government has not imposed strong net neutrality protections. States should move forward with legislation protecting against harmful and anticompetitive internet service provider (ISP) practices like paid prioritization, interconnection issues, zero-rating, and data caps.[30] The IFA appears to be modeled

---

[26] 740 Ill. Comp. Stat. Ann. 14/20, https://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=3004.
[27] *Illinois Court Rejects Clearview's Attempt to Halt Lawsuit against Privacy-Destroying Surveillance*, ACLU-IL (Aug. 27, 2021), https://www.aclu-il.org/en/press-releases/illinois-court-rejects-clearviews-attempt-halt-lawsuit-against-privacy-destroying.
[28] 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/.
[29] Letter to Roger Wicker *et al*., from Access Now *et al*., Apr. 19, 2019, https://newamericadotorg.s3.amazonaws.com/documents/Letter_to_Congress_on_Civil_Rights_and_Privacy_4-19-19.pdf, at 3.
[30] The FCC passed strong net neutrality protections in 2015. Protecting and Promoting the Open Internet, Dkt. No. 14-28, Report and Order on Remand, Declaratory Ruling, and Order, 30 FCC Rcd 5601 (Mar. 12, 2015), However, under the new administration, the agency repealed those rules in late 2017. Restoring Internet Freedom, Dkt. No. 17-108, Declaratory Ruling, Report and Order, and Order, 33 FCC Rcd 311 (2017). The FCC has not yet reinstated new rules as it has not been at full capacity.

primarily on the California net neutrality law, SB 822.[31] That law is the gold standard for net neutrality protections, and Massachusetts should take steps to make it the law here as well.

It is critically important as a policy matter to protect net neutrality. As explained in an amicus brief Access Now and other civil society organizations filed in the California litigation over SB 822, ISPs have a history of undermining net neutrality and have long imposed zero-rating schemes.[32] Furthermore, competition in the ISP market is bleak, making disclosure-related solutions like Rep. Rogers' H.134 insufficient.[33] And while ISPs often argue that their response to the COVID pandemic and resulting increases in traffic were handled smoothly and better than in other regions, those arguments are misleading and rely on national average figures, which gloss over evidence of people hit particularly hard by poor connections. In reality, the data does not clearly favor either side as the telecom industry claims.[34]

The IFA's provisions govern a wide variety of practices that should not be allowed. It covers the most harmful, including blocking or throttling content and engaging in paid priority. Paid priority bans are necessary because ISPs play a gatekeeper role over their subscribers' internet access, and an ISP should not be allowed to exploit that role and demand payments from online services to allow them to connect to that ISP's subscribers.

The Act also disallows circumventing the rules through interconnection practices. This issue was prevalent in the 2015 Open Internet proceeding at the Federal Communications Commission, as there was evidence in the record that ISPs were, rather than outright throttling services, allowing congestion to occur at their interconnection points, resulting in months-long service degradation.[35] This is just as harmful as outright throttling services, and the IFA rightly prevents it.

Zero-rating is another harmful practice that should be curtailed or prevented. Essentially, an ISP may "zero rate" a service by exempting it from a data cap or allowance. This potentially anticompetitive practice harms people by nudging them to use services the ISP has chosen to make more easily accessible to the subscriber—usually an affiliated service, or potentially one that has paid for the zero rating. For instance, if AT&T zero-rates its own HBO over its network, subscribers are much more likely to use that service than a competitor like Netflix or Hulu that is not similarly zero-rated.[36] Such zero rating harms Netflix, Hulu, other competitors, and the person using the device because they are less likely to use their preferred service and instead use the one that does not count toward a cap. Under IFA, if an ISP would like to zero-rate certain services, it may do so, but the ISP cannot accept compensation to do it, and must zero-rate an entire category of services like "entertainment" or

---

[31] California Senate Bill 822, https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201720180SB822.
[32] Amicus Brief of Access Now *et al*., ACA Connects v. Rob Bonta, 9th Circuit Court of Appeals, No. 21-15430, https://www.accessnow.org/cms/assets/uploads/2021/05/Amicus-Brief-Access-Now-et-al-ACA-v-Bonta.pdf at 9.
[33] *Id*. at 20.
[34] *Id*. at 30-31.
[35] *Beyond Frustrated: The Sweeping Consumer Harms as a Result of ISP Disputes*, Open Technology Institute (Nov. 2014), https://ecfsapi.fcc.gov/file/10221539522488/OTI%20Beyond%20Frustrated%20Interconnection%20Report.pdf.
[36] Ernesto Falcon & Katherine Trendacosta, *AT&T's HBO Max Deal Was Never Free*, Electronic Frontier Foundation (Mar. 18, 2021), https://www.eff.org/deeplinks/2021/03/atts-hbo-max-deal-was-never-free.

"video" services, which would mean HBO and Netflix, Hulu, and other competitors would gain the same benefit.

Access Now also supports the COVID-19 emergency provisions that prevent increasing prices or shutting off connections for pandemic-related hardship. Access to the internet can save lives, particularly during public health crises. Limiting or shutting off access to the internet has apparent problems. When governments shut down or slow access to the internet, or block or restrict access to social media platforms, websites, and other sources, it harms people and interferes with their human rights. This has led the United Nations to condemn internet shutdowns during the COVID-19 pandemic.[37] In a recent report, Access Now recommended, among other things, that governments make it easier for people to access the internet during the pandemic and ensure broadband was affordable.[38] Specifically, it suggested that governments "should require telcos not to disconnect anyone [from the internet] for pandemic-related reasons."[39] Massachusetts should be commended for attempting to do precisely that.

Conclusion

Access Now supports both MIPA and IFA, and the legislature should move both bills forward. Thank you for your time and attention to these important issues. I look forward to continuing to work with you.

[37] Michelle Bachelet, *COVID Is "a Colossal Test of Leadership" Requiring Coordinated Action, High Commissioner Tells Human Rights Council*, United Nations Human Rights Office of the High Commissioner (April 9, 2020), https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=25785&LangID=E ("I also urge an end to any blanket Internet and telecommunication shutdowns and denials of service."). *See also* Eric Null, *Expanding Connectivity to Fight Covid-19: Recommendations For Governments And Telcos*, Access Now (April 2020), https://www.accessnow.org/cms/assets/uploads/2020/04/Expanding-connectivity-to-fight-COVID19-Recommendations-for-govs-and-telcos.pdf at 9.

[38] Eric Null, *Expanding Connectivity to Fight Covid-19: Recommendations For Governments And Telcos*, Access Now (April 2020), https://www.accessnow.org/cms/assets/uploads/2020/04/Expanding-connectivity-to-fight-COVID19-Recommendations-for-govs-and-telcos.pdf at 14.

[39] *Id*.