Testimony of Willmary Escoto, U.S. Policy Analyst at Access Now to the Maryland Senate Finance Committee In Support of SB335 (Biometric Identifiers Privacy Act)
February 7, 2022

Dear Chair Kelley, and Members of the Committee:

Thank you for holding this week's hearing on bills related to consumer protection. I am writing on behalf of Access Now in support of SB 335, An Act establishing the Biometric Identifiers Privacy Act Information Privacy Act, which provides 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 SB 335

SB 335 provides strong privacy protections 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 SB 335 that empower online autonomy and choice, and increase overall privacy protection.

Privacy Is a Fundamental Right and Is Important to People in Maryland

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

[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/.

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]

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 year, 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 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

---

[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.

[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*.

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 reporting agency Experian got hacked, compromising the private credit reports of millions of people.[12] 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]

Maryland residents cannot control their own digital identity without a modern data protection law. SB 335 can help lead the way and set an example for other states to follow.

SB 335 Includes Several Provisions that Empower Choice and Protect Privacy

Maryland should enact strong data protection legislation for its people to remedy the shortcomings in U.S. law. SB 335 provides a comprehensive privacy framework that would significantly change the privacy landscape in the state, particularly on protections for biometric data, consumer rights, and civil remedies. Below, I focus on three important provisions in SB 335 that should be retained.

SB 335 gives users more power over their data. SB 335 gives people the right to know, access 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. SB 335 would at least give people more control over the data companies collect about them, allowing them to better control their online identities. Specifically, SB 335 would allow people to access the biometric data a company has collected about them, and if that person wants that data deleted, they are entitled to take those actions. SB 335 requires businesses to delete Marylanders' biometric identifiers after a fixed length of time and specifies how consumers' data will be collected, stored, and used. These provisions offer important rights that are often missing, or difficult to take advantage of, online.

[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/.
[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.

SB 335 heightens protections for biometric data. SB 335 would require covered entities to inform in writing and obtain handwritten consent by individuals when collecting and processing biometric data.
Covered entities would also be required to establish a retention schedule and guidelines for permanently destroying biometric data, and the bill places limits on the data's monetization. Covered entities would be banned from collecting, trading, or selling a person's biometric identifiers without affirmative consent.

The collection and use of biometric data, particularly face data, poses significant risks to individuals.[14] 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."[15]

Companies are working hard to develop biometric and artificial intelligence systems based on biometric data, and they are doing it with essentially no safeguards.[16] 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. SB 335 places reasonable limits on the processing of biometric information.

SB 335 *ensures robust enforcement with a private right of action.* SB 335 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.[17] The private right has been used to take action against Clearview AI for scraping the facial data of millions of people online.[18] It has also been used to take action against Facebook's practice of tagging people in pictures with facial recognition software without

[14] 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/.
[15] 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.
[16] 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.
[17] 740 Ill. Comp. Stat. Ann. 14/20, https://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=3004.
[18] *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.

consent.[19] 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."[20] Thus, SB 335 should include a private right of action.

SB 335 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 SB 335 and hopes the legislature will act on it.

Conclusion

Access Now supports SB 335 and the legislature should move the bill forward. Maryland will protect its residents and be a leader in biometric privacy and racial justice by enacting SB 335. Thank you for your time and attention to these important issues. I look forward to continuing to work with you.

[19] 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/.
[20] 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.