DATA FOR
BLACK LIVES

WRITTEN STATEMENT
Data for Black Lives
Before the
Maryland State House Economic Matters Committee
February 2, 2022

Good afternoon and thank you to the House Economic Matters Committee for having this hearing today. [anything else to recognize about the space we're in]

My name is Robb King and I am the National Organizing Director at Data for Black Lives (D4BL). I am testifying today in order to call for No More Data Weapons. House Bill 259, Biometric Identifiers Privacy Bill, is an important step towards that call.

D4BL is a movement of activists, organizers, and mathematicians committed to the mission of using data science to create concrete and measurable change in the lives of Black people. We see the two powerful sides of data and technology – they have the power to promote progress and the power to stifle progress.

Since the advent of computing, big data and algorithms have penetrated virtually every aspect of our social and economic lives. These new data systems have tremendous potential to empower communities. Tools like statistical modeling, data visualization, and crowd-sourcing, in the right hands, are powerful instruments for fighting bias, building progressive movements, and promoting civic engagement. But history also tells the story of how often these tools too often were wielded as an instrument of oppression, reinforcing inequality and perpetuating injustice. Redlining was a data-driven enterprise that resulted in the systematic exclusion of Black communities from key financial services. More recent trends like predictive policing, risk-based sentencing, and predatory lending are troubling variations on the same theme. Today, discrimination is a high-tech enterprise.

We at D4BL know that technology is not neutral. Without intentional intervention, design, and policy, data systems risk replicating and exacerbating the inequalities that hold us all back. House Bill 259, Biometric Identifies Privacy Bill, attempts to make such an intentional intervention.

By requiring private companies to get a person's consent before they collect biometric identifiers, disclose what identifiers they collect and why, and to delete biometric identifiers by default, this bill moves us closer towards tech transparency and towards our commitment to

Consentful Tech. “Good digital consent,” according to the Consentful Tech Project, requires that consent be freely given, reversible, informed, enthusiastic, and specific. Consentful Tech Project’s definition of consent is built on the definition of sexual consent from Planned Parenthood.[1] Biometric identifiers are a top example of the conflation of the physical and data body, and a consent framework built from consent in the physical world for consent in the digital one is incredibly appropriate for addressing consent with biometric identifiers. We often hear that reversible consent is one of the hardest components in the framework to address and we applaud that House Bill 259, Biometric Identifiers Privacy Bill, specifically states that if an individual requests that their biometric identifier data be deleted, that the private entity must delete that data within 30 days. The provisions in this bill are an important step in the right direction to build a culture of consent with our data bodies.

By requiring private entities to keep biometric data secure, this bill builds on our commitments to communal and individual privacy. Like the Consentful Tech Curriculum notes, “when safety and consent are absent, those who are more marginalized experience greater harm,” so too when a data breach happens, those who are more marginalized experience greater harm. According to the RAND Corporation’s 2016 report “Consumer Attitudes Toward Data Breach Notifications and Loss of Personal Information,” when asked “If you could place a dollar value on the amount of displeasure and inconvenience that you experienced as a result of this data loss/theft, what would it be?” Black people, on the median, said $1000, compared to $500 from people who identified as Latino, $862 from people who identified as other, and a mere $250 from people who identified as white.[2]

By prohibiting private entities from selling, trading, or otherwise profiting off our biometric identifiers, and prohibiting private entities from service or price discrimination against those who don’t want to share their biometric identifiers, this bill builds on our commitment to end data capitalism. Private companies profiting off of our data is the pinnacle of data capitalism, an emerging economic model built on the extraction and commodification of data and the use of big data and algorithms as tools to concentrate and consolidate power in ways that increase economic and racial inequality.[3] Private companies using pricing discrimination to charge certain people more for services if they fail to give their biometric data sounds eerily familiar to the millions of Black people who have lived or currently live in a neighborhood that’s been

[1] The Consentful Tech Project website, https://consentfultech.io, describes the FRIES consent framework and provides greater detail.
[2] Lillian Ablon, Paul Heaton, Diana Catherine Lavery, Sasha Romanosky, “Consumer Attitudes Toward Data Breach Notifications and Loss of Personal Information.” (RAND Corporation, 2016)
[3] This definition is from the 2021 report “Data Capitalism + Algorithmic Racism” by Yeshimabeit Milner and Amy Traub. An accompanying microsite is available for further information and to download the full report at https://datacapitalism.d4bl.org.

redlined and see that their house loans, car insurance loans, and access to other services is drastically different than those outside of the redlined borders.

And, even with these positive aspects of the bill, there is still more to do. While we appreciate it as a starting point, focusing on only private entities misses the impact of surveillance and collection of biometric identifiers from academic institutions and government agencies.

The history of the immortal cells of Henrietta Lax, also known as HeLa cells, shows us how academic institutions can be some of the worst offenders in collecting and profiting off of our biometric and biological data without our consent. Henrietta Lax went for urgent medical treatment at John Hopkins Hospital, a non-profit teaching hospital, where doctors extracted her cells from her body without her consent. That biological data was then used for decades for the advancement of many interests, but without the knowledge, compensation or consent of her or her family.

The current examples of police departments using facial recognition technology also show how government agencies can be some of the worst offenders in collecting our biometric data. For example, since 2007 Atlanta has spent over $4.5 million to increase its surveillance camera network through a project called Operation Shield. Atlanta went from 20 cameras in 2007 to over 11,000 surveillance cameras today. While we don't know the exact amount of data points and faceprints that have been captured by this technology, we do know that the automated license plate readers of Atlanta have captured over 406 million license plate scans in 2019 alone, and that a single vehicle might be captured on camera as often as 17 times in a single day as it travels around the city.[4] [5] [6] Imagine that now with faces, not license plates.

It is clear to us that private, public, and governmental collection of biometric identifiers has historically been used as a data weapon, a technological tool used to surveil, police and criminalize Black and Brown communities. We are excited to see state laws that add guardrails to the collection of biometric identifiers by private entities, like HB 259, the Biometric Identifiers Privacy Bill. These bills are a first step to acknowledge the history of biometric identifiers as a data weapon, and create an intentional intervention that brings us one step closer to no more data weapons. And, we know that even with what we hope will be the passage of this bill, it is not enough and the work must continue.

[4] Josh Wade and Aaron Diamant, "Eyes on the Road." (Atlanta Journal Constitution, 2018)
[5] Dave Maas, "2020 Vigilant Data Sharing Information - Automated License Plate Reader (ALPR) (Atlanta Police Department)." (Georgia Open Records Act request, posted on Muckrock, 2020)
[6] "Follow the Trail of a License Plate." (Knight Lab, 2018)