Testimony in Support of HB 218/SB 16

"Commercial Law – Consumer Protection – Biometric Identifiers and Biometric Information Privacy"

January 25, 2021

Margaret Hu, Professor of Law and International Affairs, Penn State Law and School of International Affairs, Institute for Computational and Data Sciences, The Pennsylvania State University-University Park

Professor Hu has written multiple works on biometric surveillance, including: *Biometric ID Cybersurveillance* (2013); *Biometric Cyberintelligence and the Posse Comitatus Act* (2016); and *Algorithmic Jim Crow* (2017)

Failing to regulate biometric data is dangerous.

- Biometric data – fingerprints, iris scans, digital photos for facial recognition technology, DNA database screening, keystroke analysis, voice and gait analysis, and other identifiers - can be easily stolen and hacked if privacy and security requirements are not imposed under the law.
- A private right of action incentivizes preemptive security, including deletion of biometric data in a timely manner and storing biometric data with responsible cybersecurity measures.
- Corporations often suggest biometric data collection is necessary for consumer analysis, cybersecurity, authentication, software applications, training and assessment, research and development, client identification, etc.
- Governmental entities, especially law enforcement, are increasingly seeking and utilizing corporate biometric data in order to conduct criminal and national security assessments.
- Because biometric data collection methods, biometric databases, biometric data algorithms used for identification and security are not regulated, they can be inaccurate or use outdated technology.
- Algorithms/AI used to analyze biometric data has been found to have a disparate impact and result in discriminatory results (e.g., higher false positives for certain minority communities).

Biometric data poses unique data privacy risks.

- Biometric data is particularly sensitive in that it relies upon identification markers of the human body in order to serve various objectives, such as identity verification (are you who you say you are?); identity determination (who are you?); and identity inference (are you a risk?).
- Biometric data, in addition to being particularly sensitive, is also ubiquitous and difficult to safeguard for data privacy and data protection purposes (digital images of one's face can be captured publicly and over the internet through the posting of digital images by others).
- In addition, the ability to integrate biometric databases with public and private databases allows for an aggregation of highly personal data. The predictive analytics capacity made possible through AI increases exponentially as the data that is analyzed becomes more personalized and linked to individuals' identities.

Biometric data anchors the expansion of cybersurveillance.

- Biometric data surveillance should be understood as the embrace of a dramatic expansion of mass surveillance in both the private and public sectors.
- Newly developed big data cybersurveillance tools fuse biometric data with biographic data and internet and social media profiling.

- Biometric data collection and analysis technologies should be considered within a broader context of cybersurveillance capacities and dataveillance trends in governance norms and by private corporations in the digital economy.

Biometric data is susceptible to abuse and misuse.

- "Identity management" is often defined as a method for granting, restricting, or denying access and privileges on the basis of one's identity.
- The intersection between biometric data and identity management is critical to understanding how biometric data can facilitate identity theft, appropriation/misappropriation of identity through impersonating/spoofing digital identity, and other cybercrimes.
- Technological innovation is embracing biometric data as the gold standard for identity management, at the same time, there is a failure of law and regulation to properly safeguard this valuable and sensitive information.
- The rapid expansion of identity management opens the possibility for the misuse and abuse of biometric data if the collection, retention, and use of biometric data is not closely regulated.
- Once biometric databases are breached, biometric data cannot be reissued (e.g., can reissue a new password if a password is compromised, however, cannot reissue new fingerprints, DNA, etc. if biometric databases are hacked and biometric security systems are breached).