Legislation Details (With Text)

File #:	Res 1431-2020	**Version:**	*	**Name:**	Biometric Privacy (S.1203/A.1911)
Type:	Resolution			**Status:**	Filed (End of Session)
				In control:	Committee on Technology
On agenda:	9/23/2020				
Enactment date:				**Enactment #:**	
Title:	Resolution calling upon the New York State Legislature to pass and the Governor to sign S.1203/A.1911, an act to amend the general business law, in relation to biometric privacy.				
Sponsors:	Robert E. Cornegy, Jr., Helen K. Rosenthal				
Indexes:					
Attachments:	1. Res. No. 1431, 2. September 23, 2020 - Stated Meeting Agenda with Links to Files, 3. Hearing Transcript - Stated Meeting 9-23-20, 4. Minutes of the Stated Meeting - September 23, 2020				

Date	Ver.	Action By	Action	Result
9/23/2020	*	City Council	Introduced by Council	
9/23/2020	*	City Council	Referred to Comm by Council	
12/31/2021	*	City Council	Filed (End of Session)	

Res. No. 1431

Resolution calling upon the New York State Legislature to pass and the Governor to sign S.1203/A.1911, an act to amend the general business law, in relation to biometric privacy.

By Council Members Cornegy and Rosenthal

Whereas, According to the Biometrics Institute, biometrics are biological and behavioral characteristics including but not limited to fingerprint recognition, facial recognition, retinal scans, and voice recognition; and

Whereas, Biometric information is becoming more widespread for security and identity verification across society, such as in banks, government facilities, airports, and businesses; and

Whereas, According to security experts, biometric information is useful for biometric security because it is always with a user, cannot be lost or forgotten, and is highly difficult to impersonate; and

Whereas, Biometric information is valuable precisely due to its unique and unchanging nature, and cannot be modified or changed like a password or PIN can, which makes it a target for hackers and cybercriminals; and

Whereas, Biometric information cannot be changed like a normal password as it is based on biological features and characteristics, meaning biometric information that has been compromised through a security breach, remains compromised; and

Whereas, Biometric information data repositories have experienced breaches, with notable security incidents reported in the media, such as the theft of 5.6 million fingerprint records and additional security clearance data from the United States (U.S.) Department of Defense in 2015, and researchers discovering in August of 2019 that a security company stored fingerprints, facial recognition data, and other security information of more than 1 million people on an unsecured and unencrypted database; and

Whereas, The same researchers who discovered that 2019 compromised security database found that the problem of unsecure biometric databases is "very common," with the researchers reportedly contacting three to four companies per week with similar issues; and

Whereas, According to studies released by the Massachusetts Institute of Technology and Stanford University in 2018, the use of biometric information like facial recognition as a surveillance tool is still highly unregulated and is uniquely biased against minority groups, particularly darker-skinned individuals; and

Whereas, Biometric information also presents privacy and security concerns for people wary of government surveillance, with notable examples including reports of China's expansive biometric database and social credit scores, the New York City Police Department's use of facial recognition technology, and the U.S. Immigration and Customs Enforcement's ("ICE") reported use of facial recognition technology to locate undocumented individuals in Maryland; and

Whereas, Illinois, Texas, Washington, and California have their own biometric information privacy laws in place; and

Whereas, New Yorkers currently have no method of knowing whether their biometric information is compromised, and no recourse should their biometric information be compromised; and

Whereas, S.1203/A.1911 would require any entity in possession of biometric information or identifiers

to develop a publicly available written policy, and would prohibit the collection, capture, purchase, or trade of the biometrics of a person without informing that person in writing and require their express written legal consent for such transactions; and

Whereas, This bill would require entities to create a plan to destroy biometric information when it is no longer in use, as well as forbid any entity possessing biometric information from either selling or profiting from this information; now, therefore, be it

Resolved, That the Council of the City of New York calls upon the New York State Legislature to pass and the Governor to sign S.1203/A.1911, an act to amend the general business law, in relation to biometric privacy.

CCK
LS # 12579
8/27/2020