Published on *The National Law Review* https://natlawreview.com

States Gear Up to Limit Use of Biometrics and Biological Data

Article By:

Theodore F. Claypoole

This may be the year when limitation of biometric capture goes national. Right now, company's using biometrics are driven by one state law, but others could soon join.

As limits on biometrics cascade forth from Illinois in private cases based on the state's Biometric Information Protection Act (BIPA), other state legislatures have decided to place limits on capture and use of biometric information. The private right of action and statutory damages offered by BIPA have made Illinois the experimental lab where U.S. companies learn what counts as a biometric program and what their limits on that program may be. Illinois may soon have company.

New York's legislature is considering restrictions of consumer biometrics this term, and the proposed act looks like Illinois' BIPA, requiring written notice of taking a biometric identifier, notice of how the identifier will be used and disposed of, and written permission from the subject to do so. It also contains a broadly worded "thou shalt not profit from anyone's biometric identifier" that could eviscerate the entire biometric technology industry if it is interpreted in an expansive fashion. The disclosure prohibitions are also surprisingly broad and could lead to liability for simply using a biometric tech processor. The legislation also contains a private right of action and statutory damages that seem lifted straight from BIPA.

New York has also proposed a less comprehensive bill that would restrict companies from using biometric information in marketing. I don't understand the driver for this particular bill, if the legislature is more concerned about a company only marketing to people grouped by biometric data, so selling to people with brown eyes or with single whorls in their thumbprints, or whether it is concerned with the manipulation of serving ads using your own voice or earlobes to sell material. However, there must be a concern because someone wrote an Act to consider.

Legislation proposed in Maryland regulates biometric identifiers and requires companies capturing such information to publish a written retention policy that will establish "guidelines for permanently destroying biometric identifiers and biometric information on the earlier of" three years or when the initial purpose for obtaining the biometric identifiers was satisfied. The Maryland act, like New York and Illinois, includes the same private right of action and statutory damages clauses.

Virginia has proposed a bill directed primarily at employers who chose to use biometric tools with

their employees. The bill requires written informed consent from an employee before the capturing and storing of the biometric data. The bill would also restrict employers from profiting from the biometric data of their workers.

South Carolina's entry into this race is a consumer protection act with very broad definitions of personal information and biometric information. This bill is almost a "CCPA for biometrics" which addresses consumer rights to prevent sale of biometric data, protections for children, and prohibition on discrimination against consumers for protecting their biometric data. This act seems to anticipate a future world where companies are using biometric data in more expansive ways than much of what I have seen, which is primarily biometric use for identification, authentication or other security purposes. There is some voice stress analysis in use, but it seems the target of this bill is anticipatory, rather than reactionary.

California's legislature passed one of the most thoughtful and constructive biometric laws last year, but it was vetoed by Governor Gavin Newsom. A similar law was introduced into this year's legislative session. The Genetic Information Privacy Act (GIPA) placed limits on what companies could do with DNA information gathered from California residents, addressing a major privacy loophole that affects the DNA entertainment industry.

In the U.S., HIPAA protects biological information that person would give to a doctor, hospital or pharmacist to assist in medical treatment, so DNA provided for this purpose would be covered under federal privacy protections. However, millions of people have decided to swab themselves and hand this DNA data – the core information describing a person's physical being – to unregulated private companies who reserve the rights to use your DNA information for all kinds of purposes. Some of these recreational DNA mills provide your data to law enforcement and some to the pharma industry, and at least one has been recently bought by big private equity firms looking to expand the range of what can be done with volunteered DNA. So this is a significant privacy problem, in part because most people who swab themselves for the benefit of these private companies are unaware of the risks and likely exposure of their biological information.

The newly introduced California law, like GIPA, would require direct-to-consumer genetic testing companies to honor a consumer's revocation of consent to use the DNA sample and to destroy the biological sample within 30 days of revoking consent. It would also provide consumers access to their genetic data. The law would not provide a provide right of action, but could be enforced by state or local officials. It may be written to overcome Gov. Newsom's objects, which he claimed were related to restricting COVID-fighting efforts.

These legislative actions may or may not be passed into law. In any case it is clear that use of biometrics by businesses for consumers, marketing and employees have sparked the imagination of state legislatures, and we are only likely to see more action in biometrics for years to come.

National Law Review, Volume XI, Number 33