2019-2020 Legislative Memorandum

Subject: An act to amend the executive law, in relation to prohibiting the use of biometric surveillance technology by law enforcement; establishing the biometric surveillance regulation task force; and providing for the repeal of certain provisions upon expiration thereof

S. 7572 (Hoylman)/ A.9767 (Glick)

Position: SUPPORT

I write today on behalf of the Electronic Frontier Foundation (EFF), a San Francisco-based, non-profit organization that works to protect civil liberties in the digital age. EFF represents more than 30,000 active donors and members, including thousands of supporters in New York. We support S.7572 (Hoylman) / A. 9767 (Glick) and urge the legislature to pass it.

This critical legislation would create a moratorium on an urgent threat to personal privacy, free speech, and racial justice: government use of biometric surveillance technology. The bill stops the government's use of these technologies, such as facial recognition, and allows for lawmakers and communities to have much-needed conversations about the privacy, speech, and other risks their use poses to New Yorkers—particularly the disparate impact of their use on historically underserved communities.

EFF objects to government use of face surveillance technology for several reasons.[1] First, face surveillance is a growing threat to personal privacy. Surveillance cameras in public spaces are proliferating, operated by myriad government and private entities. These cameras are increasingly networked into unified systems. Face surveillance technologies are also growing increasingly powerful. In combination, these technologies can track everyone who lives and works in public spaces by means of a unique identifying marker that is difficult to change or hide—our own faces. We must not build an infrastructure that empowers government to easily track where everyone is going, what they are doing, and who they are with. Once government builds this infrastructure, there is the inherent risk that thieves will steal this sensitive data, employees will misuse it, and policy makers will redeploy it in new unforeseen manners.

Second, government use of face surveillance technology in public places will chill people from engaging in protests. Courts have long recognized that government surveillance of First Amendment activity has a "deterrent effect." *See, e.g., Lamont v. Postmaster*, 381 U.S. 301 (1965). Empirical research confirms this problem. *See, e.g.,* Stoycheff, "Facebook's spiral of silence effects in the wake of NSA Internet monitoring" (2016); Penney, "Online surveillance and Wikipedia use" (2016).[2]

[1] *See generally* https://www.eff.org/pages/face-recognition; https://www.eff.org/wp/law-enforcement-use-face-recognition.

[2] https://journals.sagepub.com/doi/pdf/10.1177/1077699016630255; https://scholarship.law.berkeley.edu/btlj/vol31/iss1/5/.

Third, surveillance technologies have an unfair disparate impact on people of color, immigrants, and other vulnerable populations. Governments use them to spy on advocates for racial justice. For example, police have used phony accounts and powerful automated tools to spy on the social media advocacy of Black Lives Matter.[3] Surveillance technologies often criminalize entire neighborhoods. For example, watch lists are often over-inclusive and error-riddled, and cameras often are over-deployed in minority areas.[4] And these spying tools increasingly are being used in conjunction with powerful mathematical algorithms, which often amplify bias.[5]

Notably, studies show that face surveillance technologies have higher error rates when used with minorities, women, and young people. *See, e.g.,* "Facial recognition is accurate, if you're a white guy," N.Y. Times (Feb. 9, 2018) (reporting on a study by Joy Buolamwini of the M.I.T. Media Lab); "Amazon is pushing facial technology that a study says could be biased," N.Y. Times (Jan. 24, 2019) (reporting on another study by Buolamwini).[6]

Finally, S.7572 (Hoylman) / A. 9767 (Glick) would remedy violations of the moratorium by allowing individuals to seek injunctive and declaratory relief against a police agency or officer that violates this rule. Such private rights of action are crucial to ensuring that privacy laws have teeth, and provide consumers with the enforcement they deserve.

Government use of face surveillance technology is a threat to privacy, free speech, and racial justice. We thank you for addressing this important issue with the strong legislation that New Yorkers need. We urge the legislature to pass it. If you have further questions or would like to discuss anything I have said in more detail, please contact me at hayleyt@eff.org or 415-436-9333 x161.

Sincerely,

Hayley Tsukayama
Legislative Activist
Electronic Frontier Foundation
(415) 436-9333 x 161

[3] https://www.theguardian.com/technology/2016/oct/11/aclu-geofeedia-facebook-twitter-instagram-black-lives-matter; https://www.washingtonpost.com/news/morning-mix/wp/2018/08/23/memphis-police-used-fake-facebook-account-to-monitor-black-lives-matter-trial-reveals/?utm_term=.13db56fe4bb8.

[4] https://www.eff.org/deeplinks/2017/04/next-steps-toward-reforming-californias-unfair-gang-databases; https://www.eff.org/deeplinks/2015/01/what-we-learned-oakland-raw-alpr-data.

[5] https://www.newscientist.com/article/2166207-discriminating-algorithms-5-times-ai-showed-prejudice/.

[6] https://www.nytimes.com/2019/01/24/technology/amazon-facial-technology-study.html; https://www.nytimes.com/2018/02/09/technology/facial-recognition-race-artificial-intelligence.html.