ACLU CALIFORNIA ACTION
CFA
CONSUMER FEDERATION OF CALIFORNIA CFC
ELECTRONIC FRONTIER FOUNDATION EFF
MEDIA ALLIANCE
OAKLAND PRIVACY
PRC Privacy Rights Clearinghouse
SECURE JUSTICE

June 23, 2021

The Honorable Jacqui Irwin
California State Capitol, Room 5119
Sacramento, California 95814

Re: AB 751 – as revised 4/20/2021
OPPOSE

Dear Assemblymember Irwin:

Our organizations are dedicated to protecting Californians' privacy rights. We regret that we must respectfully oppose your AB 751, which would remove the sunset date on the current pilot program authorizing the State Registrar to accept an electronic request for a certified copy of vital records if the request is accompanied by an electronic verification of identity rather than a notarized affidavit of identity. Despite your good intentions, AB 751 unfortunately threatens to place the privacy and personal information of Californians in jeopardy. Privacy is protected by the California Constitution and should not be set aside in an attempt to ease the issuance of vital records. More than ever, it is critical that California adopt appropriate measures to protect Californians from invasive and discriminatory corporate and government surveillance.

AB 751 would be the first explicit authorization in statute for the use of face surveillance technology by a state entity. The legislature has previously restricted the state's use of face surveillance technology due to its unique risks, including prohibiting its use in conjunction with police body cameras and prohibiting the DMV from purchasing or using face surveillance technology without express authorization from the legislature.[1]

The goal of AB 751 is to make it easier to access vital records, but authorizing use of face surveillance technology will not achieve that goal. To access vital records online, AB 751 requires an individual to provide a real-time image of themselves. Face surveillance technology then compares that image to a submitted driver's license or passport photo. Because real-time images have different lighting and resolution than official government photos, face surveillance technology frequently fails to identify individuals correctly.[2] Implementing such an error-prone procedure would only decrease government efficiency. This technology has also been shown to be inaccurate, particularly with respect to people of color and others, as discussed further below. At the same time, operation costs would increase, as records offices would need to transmit and store driver's licenses and passports in a secure, encrypted manner, as well as train staff in new software

[1] AB 1215 (Ting, 2019) and AB 1 (Evans, 2009), respectively.

[2] National Institute of Standards and Technology, *Face Recognition Vendor Test, Part 2: Identification*, September 11, 2019, https://pages.nist.gov/frvt/reports/1N/frvt_1N_report.pdf.

and troubleshooting procedures. We have also seen repeatedly that no system is truly secure from hacking.

While vendors may promise theoretical benefits, the reality is that face surveillance systems are already being used to harm. ICE is taking advantage of state and private face surveillance systems to target immigrants, police have used it to target people of color, and governments are using it to oppress religious minorities and discourage free expression.[3] The threat of more harms has grown as companies like Clearview AI secretly build massive face recognition databases and provide them to businesses, police, and ICE to assist its aggressive targeting of immigrants. California should not be spending taxpayer money on bolstering this exploitative surveillance technology.

AB 751's explicit embrace of face surveillance systems would be a step backward for Californians and would create a dangerous precedent. The implementation and maintenance of face surveillance systems will expose already vulnerable populations to further harm. By authorizing face surveillance technology, AB 751 opens up the path to government misuse of such technology.

Further, face surveillance systems are well-documented to be inaccurate and biased on the basis of race, gender, age, and disability status. Face surveillance has been repeatedly demonstrated to be less accurate when used against Black people, people of Asian descent, and women.[4] The use of face surveillance systems to verify California Bar exam takers, for example, repeatedly failed to recognize test takers of color.[5] Members of the California legislature and the California Congressional delegation have experienced this disproportionate error rate firsthand in tests comparing them against mug-shot databases. Many systems also misgender transgender and gender nonconforming people, and some even purport to identify a person's sexual orientation, relying on and perpetuating harmful stereotypes about physical appearance,[6] while others claim to discern political affiliation.[7] The use of biased face surveillance will have serious ramifications for Californians, including failing to correctly identify many of them.

AB 751 also infringes on Californians' privacy rights and expectations by authorizing the use of data brokers to verify a person's identity. By sanctioning identity verification through credit reporting agencies and similar databases, AB 751 will allow third-party data companies to profit

[3] Catie Edmundson, ICE Used Facial Recognition to Mine State Driver's License Databases, New York Times, July 7, 2019, https://www.nytimes.com/2019/07/07/us/politics/ice-drivers-licenses-facial-recognition.html; Russell Brandom, *Facebook, Twitter, and Instagram surveillance tool was used to arrest Baltimore protestors*, Verge, Oct. 11, 2016, https://www.theverge.com/2016/10/11/13243890/facebook-twitter-instagram-police-surveillance-geofeedia-api; Paul Mozur, *One Month, 500,000 Face Scans: How China Is Using A.I. to Profile a Minority*, New York Times, Apr. 11, 2019, https://www.nytimes.com/2019/04/14/technology/china-surveillance-artificial-intelligence-racial-profiling.html.

[4] The National Institute of Standards and Technology released results for a comprehensive study of face surveillance systems finding that African American and Asian people were up to 100 more times likely to be misidentified than white men, depending on the algorithm and use case. Drew Harwell, *Federal study confirms racial bias of many facial-recognition systems, casts doubt on their expanding use*, Washington Post, Dec. 19, 2019, https://www.washingtonpost.com/technology/2019/12/19/federal-study-confirms-racial-bias-many-facial-recognition-systems-casts-doubt-their-expanding-use/.

[5] Chase DiFeliciantonio, California bar exam takers say facial recognition software rejected them, San Francisco Chronicle, October 8, 2020, https://www.sfchronicle.com/business/article/California-bar-exam-takers-say-facial-recognition-15629617.php.

[6] Devin Coldewey, AI that can determine a person's sexuality from photos shows the dark side of the data age, TechCrunch, September 7, 2017, https://techcrunch.com/2017/09/07/ai-that-can-determine-a-persons-sexuality-from-photos-shows-the-dark-side-of-the-data-age/.

[7] Facial Recognition Reveals Political Party in Troubling New Research, Jan. 13, 2021, https://techcrunch.com/2021/01/13/facial-recognition-reveals-political-party-in-troubling-new-research/

off the personal data of Californians. Some data brokers, such as Acxiom and Intelius, collect personal details about consumers' behavior online, their income, and addresses, which are used to create a detailed profile about them. This information is then sold and resold, and often used for marketing and potentially for other purposes, including lending decisions.

Apart from the dangers of collecting and storing all this data, detailed—and often erroneous—consumer profiles can lead to race or income-based discrimination. For example, when consumers are categorized into data segments, if a person is categorized as "low income," they may be subject to ads for subprime credit or receiving different levels of service from companies.[8] And, because this data collection occurs largely without the consumer's knowledge or affirmative consent, consumers are unable to properly protect themselves. In a study conducted at the University of Illinois at Urbana-Champaign, 89% of participants indicated that they did not think marketing and advertising companies should be permitted to "track consumers' online activity without asking for permission."[9] By authorizing the use of these data brokers for identity verification purposes, AB 751 both props up this problematic industry and risks locking people out from verifying their identity due to errors in data brokers' databases.

AB 751's methods for identity verification present troubling privacy implications for all Californians. There are far too many inherent risks in verifying someone's identity with biometrics such as face surveillance technology or with third-party data brokers; these methods are also ripe for further misuse by government entities and private companies. For example, at least three California government agencies have reported using Clearview AI's database,[10] even though they were not authorized to use face surveillance technology.

Moreover, neither AB 751 nor the pilot program the bill would make permanent are necessary to ensure people can safely get certified copies of vital records during the COVID-19 pandemic. People can still request vital records online by submitting a scan of a notarized affidavit of their identity. With mobile notaries and socially distanced notarization, the notarized affidavit of identity remains a safe and viable option for everyone. Straying from this proven, reliable method for identity verification threatens increased harm, identity theft, and serious privacy intrusions for all Californians.

For these reasons, we must respectfully oppose AB 751.

Sincerely,

Becca Cramer-Mowder
Legislative Coordinator & Advocate, ACLU California Action

[8] Brittany A. Martin, *The Unregulated Underground Market for Your Data: Providing Adequate Protections for Consumer Privacy in the Modern Era*, 105 Iowa L. Rev. 865, 888 (2020).

[9] Jay P. Kesan et al., *A Comprehensive Empirical Study of Data Privacy, Trust and Consumer Autonomy*, 91 Ind. L.J. 267, 297 & tbl.1 (2016).

[10] A confidential source provided BuzzFeed News with a table revealing entities that had accessed Clearview AI's database. Spokespersons from California Department of Correction and Rehabilitation, California Department of Health Care Services, and California State University, Long Beach Police have confirmed their employees used Clearview AI's database. Ryan Mac, Brianna Sacks, Caroline Haskins, and Logan McDonald. *Your Local Police Department Might Have Used This Facial Recognition Tool to Surveil You. Find Out Here*, BuzzFeed News, April 9, 2021, https://www.buzzfeednews.com/article/ryanmac/facial-recognition-local-police-clearview-ai-table.

Tracy Rosenberg
Advocacy Director, Oakland Privacy
Executive Director, Media Alliance

Susan Grant
Director of Consumer Protection and Privacy, Consumer Federation of America

Emory Roane
Policy Counsel, Privacy Rights Clearinghouse

Lee Tien
Legislative Director & Adams Chair for Internet Rights, Electronic Frontier Foundation

Robert Herrell
Executive Director, Consumer Federation of California

Brian Hofer,
Executive Director, Secure Justice

cc: Members and Committee Staff, Senate Judiciary Committee