HARVARD UNIVERSITY
GRADUATE SCHOOL OF BUSINESS ADMINISTRATION

GEORGE F. BAKER FOUNDATION

SHOSHANA ZUBOFF
Charles Edward Wilson Professor of Business Administration, Emerita

Soldiers Field Road
Boston, Massachusetts 02163

May 20, 2021

Senator Susan Deschambault, Chair
Representative Charlotte Warren, Chair
Maine State Legislature
Committee on Criminal Justice and Public Safety
c/o Legislative Information Office
100 State House Station
Augusta, ME 04333

RE: LD 1585: An Act to Increase Privacy and Security by Prohibiting the Use of Facial Surveillance by Certain Government Employees and Officials – Ought to Pass

Dear Chairs Deschambault and Warren and members of the Committee:

I write in support of LD 1585: An Act to Increase Privacy and Security by Prohibiting the Use of Facial Surveillance by Certain Government Employees and Officials. I appreciate your interest in face surveillance and urge you to vote ***ought to pass.***

On May 18, 2021 Amazon.com Inc. announced that it would extend indefinitely its moratorium on sales of its facial recognition software, "Rekognition," to law enforcement agencies.[1] Its moratorium was first announced in June 2020, at the height of nationwide protests triggered by the murder of George Floyd, as law enforcement agencies were seen to be abusing the powers afforded by facial recognition systems. Microsoft and IBM similarly halted sales of their powerful facial recognition software to law enforcement.[2] These corporations have called repeatedly for state and Federal laws to regulate the use of one of the most potent, invasive, and oppressive technologies of the digital age. Now executives have taken the extraordinary step of foregoing revenues rather than support the proliferation of face surveillance technologies without appropriate laws to guide their use in a democratic society.

[1] Jeffrey Dastin, "Amazon extends moratorium on police use of facial recognition software," Reuters (May 18, 2021). https://www.reuters.com/technology/exclusive-amazon-extends-moratorium-police-use-facial-recognition-software-2021-05-18/

[2] Rebecca Heilweil, *Big tech companies back away from selling facial recognition to police. That's progress.*, Vox (Jun. 11, 2020), https://www.vox.com/recode/2020/6/10/21287194/amazon-microsoft-ibm-facial-recognition-moratorium-police; Jeffrey Dastin, *Amazon extends moratorium on police use of facial recognition software*, Reuters (May 18, 2021), https://www.reuters.com/technology/exclusive-amazon-extends-moratorium-police-use-facial-recognition-software-2021-05-18/.

At this point in our nation's history, the collection, use, dissemination, and retention of biometric identifiers is an unregulated 'wild west' in which Americans have no protection from the use or abuse of facial recognition technologies. As a citizen of a democratic society, there is nothing an individual American can do to prevent the capture and mining of one's face by the government or a private company, despite the known threats that these systems pose to privacy and civil liberties. **An individual's ability to control access to his or her identity and personal information, including determining when, how, and to what purpose these are revealed, is an essential aspect of personal security and privacy guaranteed by the Bill of Rights.[3] The use of facial recognition technology erodes that ability.[4]**

Facial recognition techniques can be deployed covertly, remotely, and on a mass scale. Participation in society necessarily exposes one's images in public spaces, whether online or on a city street. Ubiquitous effortless identification by hidden software systems and devices eliminates the individual's ability to control the disclosure of their identities along with valuable 'metadata,' such as 'facial micro-expressions,' used to discern emotional states and other personal information. Face surveillance creates new opportunities for behavioral, tracking, monitoring, and prediction that pose risks to the First Amendment rights of free association and free expression — particularly to those who engage in lawful protests — as well as to Fourth Amendment rights of unlawful search and seizure.[5] Last summer a protester in New York City was identified through facial recognition, leading to a high-profile siege of his apartment.[6] Facial recognition technology simply puts too much unaccountable power in the hands of the police.

These themes are augmented by a growing body of research that shows facial recognition technologies to be racially and gender biased. Recent studies from MIT analyzing commercially available facial recognition systems found that they mis-identified women and people of color far more frequently than white men.[7] Indeed, facial recognition algorithms may mis-identify black women in up to 35% of cases.[8] A landmark 2019 study from the National Institute of Science and Technology confirmed these findings.[9] The most prominent commercial facial recognition system, Clearview AI, has not even been tested for racial bias.

[3] William O. Douglas, "Dissenting Statement of Justice Douglas, Regarding Warden v. Hayden, 387 U.S. 294" (US Supreme Court, April 12, 1967), https://www.law.cornell.edu/supremecourt/text/387/294; Nita A. Farahany, "Searching Secrets," University of Pennsylvania Law Review 160, no. 5 (2012): 1271.

[4] Shoshana Zuboff, *The Age of Surveillance Capitalism*, Public Affairs: New York, 2019.

[5] *See* Ian Kerr & Jennifer Barrigar, *Privacy, Identity and Anonymity* (Apr. 1, 2012), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3396076. See also, Carpenter v. United States, 138 S.Ct. 2206, 2217 (2018).

[6] George Joseph and Jake Offenhartz, *NYPD Used Facial Recognition Technology In Siege Of Black Lives Matter Activist's Apartment*, Gothamist (Aug. 14, 2020), https://gothamist.com/news/nypd-used-facial-recognition-unit-in-siege-of-black-lives-matter-activists-apartment.

[7] Joy Buolamwini and Timnit Gebru, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, 81 Proceedings of Machine Learning Res. 77-91 (2018), http://proceedings.mlr.press/v81/buolamwini18a.html, *and* Inioluwa Deborah Raji and Joy Buolamwini, *Actionable Auditing: Investigating the Impact of Publicly Naming Biased Performance Results of Commercial AI Products*, AIES '19 (January, 2019), https://dl.acm.org/doi/abs/10.1145/3306618.3314244.

[8] *Id*.

[9] Patrick Grother, Mei Ngan, and Kayee Hanaoka, Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects, NIST (December 2019), https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf.

Clearview illustrates how the dangers of facial recognition do not end with racial bias, rather these systems drive the rapid expansion of the surveillance state.[10] Clearview is built on "more than three billion images scraped from Facebook, YouTube, Venmo and millions of other websites, making it larger and more invasive than any other government or private sector system." Described as "the radical destruction of privacy," the system receives any uploaded photo and instantly matches it to photos in its data set along with links to pages where the photos appear. Actively marketed to law enforcement agencies, it already boasts 600 US police departments among its clients.[11]

There is a growing recognition among leaders in the law enforcement and cybersecurity communities that the massive scale of facial recognition data sets and their highly imperfect systems of analysis have become risks to effective law enforcement, individual liberty, and national security. When Massachusetts was debating a moratorium on law enforcement use of facial recognition last session (which passed the Legislature but was vetoed by the Governor), the District Attorneys of both Suffolk and Middlesex Counties testified in support of the moratorium citing inaccuracy in 30% of cases and frequent rights' violations.[12] Cybersecurity experts note that the ubiquitous digitization of personal information, including facial recognition, was considered key to national security at the start of 'the war on terror.' In the current era, however, these same operations are making individual citizens and American society as a whole more vulnerable to cyberattacks.[13]

For these reasons and more, there is growing support in the states and in Congress for a ban or moratorium on facial recognition technology. In October 2020, Vermont became the first state to enact a statewide ban on law enforcement use of facial recognition technology.[14] In April 2021,Virginia also passed a statewide ban on law enforcement use of facial recognition technology without prior legislative approval.[15] In June 2020, Boston City Council voted to ban facial recognition for city agencies.[16] City governments in San Francisco and Oakland, CA, and Somerville, MA, have adopted similar laws.[17] And as you are aware, voters in Portland, Maine just approved a ballot measure banning the use of facial recognition by police and city agencies.[18] The trend is clear, the public does not want police departments or other public agencies to use facial

[10] Clare Garvie and Laura M. Moy, *America Under Watch: Face Surveillance in the United States*, Georgetown Law Center on Privacy & Technology (May 16, 2019), https://www.americaunderwatch.com.

[11] Kashmir Hill, "The Secretive Company That Might End Privacy as We Know It," *The New York Times,* (January 18, 2020). https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html

[12] Chris Lisinski, *Mass. lawmakers urged to pause, regulate face recognition*, State House News (Oct. 23, 2019), https://www.bizjournals.com/boston/news/2019/10/23/mass-lawmakers-urged-to-pause-regulate-face.html.

[13] See for example, Martin C. Libicki, "The Convergence of Information Warfare," Strategic Studies Quarterly, 2017: 49–65.

[14] 2020 Vt. Acts & Resolves 166.

[15] 2021 Va. Acts 537.

[16] Ally Jarmanning, *Boston Lawmakers Vote To Ban Use Of Facial Recognition Technology By The City*, NPR (Jun. 24, 2020), https://www.npr.org/sections/live-updates-protests-for-racial-justice/2020/06/24/883107627/boston-lawmakers-vote-to-ban-use-of-facial-recognition-technology-by-the-city.

[17] *See* EPIC, State Facial Recognition Policy, https://epic.org/state-policy/facialrecognition/.

[18] Russell Brandom, *Portland, Maine has voted to ban facial recognition*, The Verge (Nov. 4, 2020), https://www.theverge.com/2020/11/4/21536892/portland-maine-facial-recognition-ban-passed-surveillance.

recognition technologies in the absence of the transparency and accountability that only law and regulations can guarantee.

There is bipartisan Congressional support for halting the use of facial recognition technology by the government. Senator Edward Markey [D-MA] and Senator Mike Lee [R-UT] have called for the Department of Homeland Security to pause its use of facial recognition technology.[19] The Senators said, "DHS should pause their efforts until American travelers fully understand exactly who has access to their facial recognition data, how long their data will be held, how their information will be safeguarded, and how they can opt out of the program altogether."[20] Prior to his passing, Rep. Elijah Cummings [D-MD] and Rep. Jim Jordan [R-OH] – the Chair and Ranking Member of the House Oversight Committee – were working on legislation that would place a moratorium on funding facial recognition technology use by the federal government.[21] "It seems to me, it's time for a time out," said Ranking Member Jim Jordan at a recent hearing on facial recognition technology.[22]

Without law and regulations to protect American citizens' privacy, security, and civil rights, our society is simply not prepared to deploy facial recognition technologies. The public knows this. As has often been the case throughout American history, it is citizens and state legislators who lead the way. I urge Maine legislators to join Vermont and Virginia and ban the use of facial recognition by "certain government employees and officials" at this time. The Committee should vote *ought to pass* on LD 1585.

Sincerely,

Shoshana Zuboff,
Resident of Nobleboro, Maine
Author, *The Age of Surveillance Capitalism*
Charles Edward Wilson Professor Emerita, Harvard Business School

[19] Davey Alba, *These Senators Want Homeland Security To "Pause" Its Airport Facial Recognition Program* (Mar. 12, 2019), https://www.buzzfeednews.com/article/daveyalba/these-senators-want-homeland-security-to-pause-its-facial; Letter from Sens. Edward Markey and Mike Lee to Kirstjen Nielson, Secretary, Dept. of Homeland Security (Dec. 21, 2017), https://www.markey.senate.gov/imo/media/doc/DHS%20Biometrics%20Markey%20Lee%20letter1.pdf; Letter from Sens. Edward Markey and Mike Lee to Kirstjen Nielson, Secretary, Dept. of Homeland Security (May 11, 2018), https://www.markey.senate.gov/imo/media/doc/Biometric%20Exit%20Program%20Letter.pdf; Press Release, Sens. Edward Markey and Mike Lee, *Senators Markey and Lee Call for Transparency on DHS Use of Facial Recognition Technology* (Mar. 12, 2019), https://www.markey.senate.gov/news/press-releases/senators-markey-and-lee-call-for-transparency-on-dhs-use-of-facial-recognition-technology.

[20] Press Release, Sens. Edward Markey and Mike Lee, *Senators Markey and Lee Call for Transparency on DHS Use of Facial Recognition Technology* (Mar. 12, 2019), https://www.markey.senate.gov/news/press-releases/senators-markey-and-lee-call-for-transparency-on-dhs-use-of-facial-recognition-technology.

[21] POLITICO Morning Tech, *Lawmakers want limits on facial recognition funds* (Aug. 22, 2019), https://www.politico.com/newsletters/morning-tech/2019/08/22/lawmakers-want-limits-on-facial-recognition-funds-472395.

[22] *Facial Recognition Technology (Part 1): Its Impact on our Civil Rights and Liberties*, House Comm. on Oversight and Gov't Reform, 116th Cong. (May 22, 2019) (Sen. Jim Jordan at 1:26:08), https://oversight.house.gov/legislation/hearings/facial-recognition-technology-part-1-its-impact-on-our-civil-rights-and