Written testimon for today's facial recognition hearing

Mo Lotman <mo@thetechnoskeptic.com>
Fri 7/30/2021 1:27 PM

To: Manning, Jacqueline O. (HOU) <Jacqueline.O.Manning@mahouse.gov>

Dear commissioners,
Please find below the written testimony that I provided in today's hearing.

Best wishes,
Mo Lotman
49 Myrtle St. #2
Somerville, MA 02145
617-616-5580

Thank you to Senator Eldridge and Representative Day and the commission for conducting this hearing.
My name is Mo Lotman. I publish a magazine called the Technoskeptic which takes a critical look at the impact of technology on society, and I'm a resident of Somerville.

It has long been recognized, in our national constitution under the fourth amendment, and in the Universal Declaration of Human Rights, among many other places, that there is a fundamental right to privacy. This right exists to protect citizens from harassment, profiling, intimidation, public shaming, social control, and the horrors of violent discrimination.
      Facial recognition software is a mortal threat to the right of privacy. Period. This conversation often gets bogged down in details about algorithms and technology and codes of ethics, but ultimately those just help enshrine facial recognition by implying there might be a just way to deploy it. But there is no ethical use of facial recognition software, because in order for it to work, it must first create a biometric dossier of every citizen, collected without consent, and then constantly put all citizens under surveillance and run all citizens through a virtual line-up, also without consent. Corporations and Law enforcement are incentivized to surveil as much as possible in order to provide the most comprehensive databases with the highest likelihood of accurate returns. This mass surveillance is the precise opposite of privacy, and its capabilities, thanks to technologies of automation and artificial intelligence, allow law enforcement, governments, and even private citizens to do things that have never before been possible in human history. Namely, it creates the possibility of being able to track, follow, accumulate, and instantly search permanent records of innocent people's whereabouts, activities, and associations at all times, even potentially in real time, without limit.
      There is no way to reasonably compare this behavior to any low-tech surveillance of the past, because it is utterly asymmetrical, it is indiscriminate, it is automated, it acts at scale, and it is impossible to erase. We cannot use prior metrics like "reasonable expectation of privacy" to determine the settings for these systems, A) because we have been told through the last decade of hi-tech surveillance that there can be no privacy anywhere. And B) because a police officer standing on a corner watching people walk by on a sidewalk has nothing in common with a video camera with infinite memory, infinite pattern recognition, and infinite searchability scanning faces from above.

Once data is gathered, there is no way to confidently control its use, in part because future uses that we can not even yet imagine will create new opportunities to abuse it. Panels like this one in the future can decide to simply change the rules about what the data may be used for. And to give a very local relevant example, the data gathered by the Mass Pike cameras and transponders, which is prohibited by state law (Part I, Title II, chapter 6C, section 13) to be used for anything other than toll administration, are in fact made available for real-time public safety alerts, to gather statistics on highway usage, and for searches by law enforcement and via subpoenas for court cases like divorce proceedings.

Surveilling people used to cost resources: time, personnel, equipment, and money. These limits were natural boundaries which held power in check. To use resources efficiently, it made no sense to surveil everybody. But when technology drives policy, the logic of surveillance triumphs over the state's ability to administer justice.

This commission is meant to evaluate government use of facial recognition technology. Item 8 under this commission's proposed duties in Section 105 of Chapter 253 of the Acts of 2020 is to "examine whether, and under what circumstances, it is appropriate for law enforcement agencies to perform facial recognition searches without a warrant,"

The fact that there is a question as to whether a warrant is required for a search—something that is guaranteed by the fourth amendment of the United States Constitution—demonstrates the problem inherent in this entire line of inquiry. The fact of the matter is that technologies of automation, AI, and surveillance have combined to drive policy, rather than justice or the rule of law.

Unfortunately there is no "good" or "ethical" facial recognition system because there is no good or ethical mass surveillance. What the CEO of Clearview AI testified about earlier—a google for photos that hijacks, without consent, innocent people's snapshots and web posts in order to create a universal surveillance database which he is proud to say specifically includes children—describes an Orwellian dystopia. It is not a mystery that mass surveillance can lower civilian crime—any repressive, authoritarian government can do that.

Whatever individualized harms facial recognition may prevent are greatly outweighed by the general harms it creates all the time for all citizens, in perpetuity. If you feel the need to conjure anxiety in order to act, rather than imagine unsolved crimes or acts of terrorism, I ask you to instead consider the implications of these technologies in the hands of a president, governor, or police chief who is driven by authoritarianism, a lust for power, or the ability to punish political enemies. By enabling systems of automated mass surveillance, you are creating a turn-key totalitarian state, one that may ultimately prove impossible to resist. I like to believe that that is not what Massachusetts is about. I urge you to reject not just facial recognition schemes but the logic of mass surveillance in its entirety.

Thank you.