RESTORE THE FOURTH MINNESOTA
Testimony for the Subcommittee on Data Practices
Jan 30, 2020

Mister chairmen and members of the committee, I would like to start by expressing my gratitude for this committees work on the issues of data privacy and surveillance. These topics are becoming more complex and more important as technology integrates into government and society at large.

My Name Is Cass, and I am speaking as part of the Minnesota chapter of the Restore the Fourth movement, a national campaign dedicated to renewing the protections of the fourth amendment in the modern era.

Regarding the bill being discussed today, I would like to start off by saying that our chapter views this bill as a positive step towards regulating facial recognition technology. We have been ardent supporters of the idea that law enforcement should not be able to outsource surveillance and data collection to third parties, and we are particularly happy to see a section in this bill which limits their ability to do exactly that.

This rule is sorely needed as more “Big Data” companies seek to partner with law enforcement. These private entities are not subject to the same public scrutiny or oversight that government agencies are, and frequently engage in shady practices designed to maximize profit at the expense of data security, privacy, and often basic human dignity.

But I would be remiss if I did not express the concern that our chapter has over several omissions that we see in this bill, and attempt to give the committee a technologists perspective on the risks associated with these omissions. For example, the bill takes pains to clarify that its perfectly acceptability for law enforcement to enter into agreements with other government agencies. This is concerning to us as many of these agencies have a history of engaging in practices that are just as bad if not worse then those done by private entities. This exemption is compounded by the fact that the bill applies only to law enforcement agencies, and places no restrictions or requirements on other Government entities that might use facial recognition.

But the biggest omission is the failure to address other biometric surveillance tools. Facial recognition has been a popular news topic recently, and many jurisdictions have already either banned the technology or enacted rules limiting its use. But it would be a mistake to limit oversight to facial recognition. There are other technologies that exist

right now that can be used to identify and track people from a distance, and technology is always improving.

And even though this bill deals specifically with facial recognition, outside of the reporting requirements it does not impose any meaningful limits on how law enforcement can use technology. It requires the creation and publication of written policies, but then leaves the shape and scope of those policies entirely in the hands of law enforcement.

So while this bill does make meaningful progress towards regulating Facial Recognition Technology and for providing some transparency surrounding its use, in many ways it also maintains the status quo. Right now law enforcement has a blank check to write its own rules on Facial Recognition, and this bill does not change that.

We would highly encourage this body to consider enacting more comprehensive oversight. It would be better to take a proactive approach and broadly limit the use of surveillance technology, rather then trying to play legislative wack-a-mole every time the engineers at Google or DARPA come up with a new way of spying on us.

Thank you for your time, I would be happy to answer any questions you might have.