Comment on facial recognition for LCC Subcommittee on Data Practices
Rich Neumeister

To: Members of the LCC Subcommittee on Data Practices, January 30, 2020

Good morning,

Let me start with three examples of the use or possible use of facial recognition which has been in the news locally. The issues and concerns raised in the illustrations highlight decisions that you may need to make with this overwhelming and powerful technology.

Last week I testified before the Met Council on their one million dollar plus new camera surveillance system which they will be purchasing and implementing on the light rail system. The contractor providing the cameras and built-in microphones will be Hitachi Vantara Corporation.

This contractor sells with their surveillance systems facial recognition capabilities and software. A piece of this capacity and software allows for the analysis of live video to "**automate facial recognition** of registered individuals and ensures proactive security for operational purposes."

Second illustration, the St Paul Police Department per Pioneer Press recently purchased a computer analysis system called BriefCam. The technology helps the department sort through thousands of hours of surveillance cameras which are from public and private sources.

The provider has infrastructure which it sells with "face recognition capabilities provide(s) best-in-class face matching as seamlessly integrated component of its extensible Video Contents Analytics platform."

Final example, a criminal complaint was filed recently against a suspect by the Minneapolis Police Department. In the complaint so stated: "Facial recognition software was employed and led to identifying defendant as the subject."(Tony Webster reported)

The complaint was filed on November 8, 2019. Several days earlier at a community meeting on privacy, a police captain of the Minneapolis Police Department.....stated "Other departments use facial recognition ... we don't have any current plans to employ that technology." (Tony Webster reported)

The exemplifications show questions and policy decisions that the legislature needs to make.

The working draft (SC5873-1) presented for discussion highlights some, but not all of those questions and decisions.

Will the legislature take an approach to have a comprehensive policy or have de-centralized process where the local political subdivision makes the decisions and sets the policies?

This is the central point of subdivision 4. My suggestion have a broad policy with specific guard rails, accountability, and transparency. Similar as to what was done with license plate readers and body cameras.

Another question, what photo databases are being or could be used to compare images when facial recognition is done, booking and arrest photos, how about drivers license photos, ie? My understanding is that drivers license photo cannot currently be used. Is that correct?

Where does the definition of 'facial recognition technology' originate from? I spoke with a privacy expert who indicated to me that the definition "opens the ability to do real-time face analytics on streaming video, which Amazon's Rekognition (facial recognition software and program) currently sells. It was suggested for a substitute the definition used by the City of Oakland, California in their local ordinance. There are other ideas for definitions from many sources.

There should be included in your packet a paper copy of recommendations from the Georgetown Law Center on Privacy and Technology on policy and legislation from their comprehensive report on facial recognition. The report was done in 2016, they may have done an update.

The list of recommendations helps you as policymakers decide questions and issues that need to be addressed in legislation regarding facial recognition.

As I stated in written testimony last November:

"Facial recognition technology challenges First and Fourth Amendment principles to their core. Nothing new as Minnesota policymakers have discovered with avalanche of new technology such as Stingray, license plate readers, for example. There are no restrictions or regulations in Minnesota with use and deployment of this particular technology."

This is the second time that a body of the Minnesota Legislature is taking up the topic of facial recognition on it's own without being intertwined with other initiatives. Today's meeting is one of starting the discussion of specifically what the law to be, but the continuation of discussion with the public as to what the law should be must also continue!

The legislature needs to enact comprehensive law on facial recognition. There needs to be guardrails, standards, and curtailing policies so that the use and rules are not developed by law enforcement agencies in secret. There needs to be legislative approval and transparent discussion for the public. Our privacy and civil liberties can be diminished if this onerous and powerful technology is not kept in check.