Written commentary for July, 24th 2019 meeting of the LCC Subcommittee on Data Practices

My name is Richard Neumeister. Since the late 1970's I've been involved with privacy and open government issues on the local, state, and federal level. I have worked with and helped Minnesota legislators develop public policy on various issues and topics.

Drone regulation

The Minnesota Legislature has been grappling with drone legislation for the last five years. I lobbied on the proposals in the first year or two, but since 2016 I've been on the sidelines.

It is my intention to generally lay out my concerns today in written commentary on the suggested draft. SC 5562 can be characterized as an opaque and anemic idea or a robust and accountable suggestion to protect Minnesotans privacy and to keep law enforcement in check in using drones (UAVs).

I believe it tends to be towards the opaque and anemic.

It is important that policymakers and residents get this legislation right to protect Minnesotans privacy and civil liberties.

Search warrant important

It is essential that we not allow this new technology - with enhancements such as thermal imaging, zoom lenses, sensitive microphones, and other tech add-ons to be used without a search warrant.

The draft bill does not make clear whether the proposal updates decades-old Fourth Amendment case law as it applies in aerial surveillance. Law enforcement has argued there is no Fourth Amendment protections when hovers a UAV over an individual's property with a camera. They base that on old court decisions by the US and Minnesota Supreme Courts.

As with the tracking warrant legislation which I was involved with in 2014, the main objective was to overturn old case law and statutory language and to give robust Fourth Amendment protections for Minnesotans with their location data as they used their 'personal devices' (cell phones, etc) in their daily lives.

Does this proposal do that? Does it overturn decades-old case law and allow Minnesotans to have 21st century privacy protections when drones with enhanced technology are used? There needs to be clarity on this point. For example, in *Ciraolo*, a case decided by the US Supreme Court, the court ruled that a person does not have a right to privacy from warrantless aerial surveillance from a plane flying 1000 feet over one's home and curtilage. Law enforcement has argued the same with the use of UAVs.

In the bill language, a "law enforcement agency" is defined basically as either a police or sheriff agency. But there are other government entities that enforce rules, regulations, and law. UAVs can be easily used by those other entities as well, but it appears that the definition excludes them. For example, licensing, residential, or zoning agencies could use drones for enforcement purposes. Do not the residents of Minnesota have Fourth Amendment protections in those kind of situations?

Change to Subdivision 2

In subdivision 2, I believe that the word 'may' should be changed to 'shall'. To be made clear, the term 'probable cause' should also be added.

Problems with Subdivision 3

Do some of the subdivision 3 exceptions swallow the search warrant protection created in subdivision 2? Very possibly.

Paragraph (a) is a recognized exception to the Fourth Amendment.

The degree of privacy intrusion under paragraph (b) may turn on the enhanced software that a drone mau use in the surveillance and monitoring of a public event.

What is most troubling is paragraph (f), which allows a drone to be 'borrowed' by any government agency that wishes to use it.

Let's say a City wants to see how people are complying with certain rules of what homeowners can have in their backyards. The local agency requests the use of a drone to hover over backyards (1000 feet up) with enhanced technology to 'see' what's there. Should not the Fourth Amendment protect the homeowner in this situation? I believe so.

Subdivision 3 exceptions of (b), (d), (e), and (f) and when data is collected to where it may show a violation of law that evidence should not be used against the subject. I do not think subdivision 6 does that with the subdivision 3 exceptions.

When reviews subdivision 3 exceptions, one will note that there are different documentation standards among the paragraphs, or none at all.. It is important for the public to know when a UAV is used. This needs to be reviewed to insure responsibility and answerability to the public.

Subdivision 4

There should be some discussion about subdivision 4. I have some ideas for additional language for accountability and transparency,

I recommend that language in paragraph (d) should be changed from 'may' to 'shall'. I also recommend that language be added to cover 'enhance' technology, so that the latter part of the sentence may read 'with facial recognition or other bio-metric-matching, and enhanced technologies unless……' This change would provide Minnesotans with robust 21st century privacy protections.

Subdivision 5

I need to review subdivision 5 closely over the next month or so. It needs to be clear on what is public and what is not. I am interested to see what currently would be public and what would not become available to the public if this language was passed.

Subdivisions 9

I am concerned about subdivision 9. The language in subdivision 9 mirrors language from the tracking warrant statute.

The concerns I have with paragraphs (c) and (d) in particular: Paragraph (c) allows a prosecutor to request that data not be filed. In paragraph (d), it is specific that only upon the commencement of a criminal proceeding, the warrant application and supporting material must be filed. But what if there is no commencement of any criminal proceeding? How in that situation does the warrant and supporting data ever become public? I believe this is happening with a number of tracking warrants. What is the trigger to make sure that in these circumstances the search warrant data is eventually public?

Final comment

Minnesotan's should be able to live in security and freedom from surveillance that is not justified. The proposed bill does not provide robust protection against surveillance techniques enhanced by technology. Abstruse advances enable law enforcement and government to go beyond our expectations without many times public and policymakers making the rules with which they should abide by.

Over my four decades of involvement with privacy matters, it has been law enforcement that is the institution that wishes to make their own rules, have the least accountability, and be hush-hush on what they may be doing that compromises our privacy. There is a balance that needs to happen. I will continue to strive for that and I have done so in the past.

Please contact me if there are any questions with what I have shared with you or want specific ideas to ensure that the drone proposal is one that manners the respect of our civil liberties.