

Thank you Mr. Chairman. My name is Matt Ehling. I am here today on behalf of the Minnesota Coalition on Government Information. I appreciate the opportunity to appear, and I also appreciate this committee's attention to the LPR issue over the past several weeks. I am here to testify in favor of HF 155, and will provide a two-part analysis that outlines why this bill provides the best resolution to the issue of license plate reader regulation.

1. The first part of the analysis involves looking closely at what LPR technology provides. It is our organization's belief that policy that guides the use of government technology - especially technology that collects data on individuals - should be narrowly tailored to meet a specific purpose.

As you've heard, LPR allows the automation of a formerly manual process of checking vehicle plates against existing police databases for open warrants, stolen vehicles, and the like. Industry literature speaks to this capability, as does the testimony that you've heard in recent weeks. It is clear that using LPR to generate "hit" data that correlates plate images to existing law enforcement leads provides a public safety benefit. This use of LPR - for a specific and limited purpose - should be supported. HF 155 enables this specific purpose, and would convert hit data to a "private" or "nonpublic" status for subsequent use by law enforcement.

As this committee has also heard previously, LPR generates a data by-product --- "non-hit" data -- data that does not correlate to information in police databases. This data contains the locations of vehicles - and thus, individuals - that are not related to existing law enforcement operations. This "non-hit" data accounts for the vast majority of LPR data, and its existence triggers the second part of our analysis.

2. Non-hit LPR data has generated the bulk of the discussion and controversy in this debate so far. We believe that the answer to regulating this sort of data is found by looking to our nation's history and tradition.

The American legal system has a long-standing tradition of limiting the collection and maintenance of data about individuals, unless that data has an identifiable law enforcement purpose - as opposed to merely a possible or speculative purpose.

We see this in the Fourth Amendment's calls for specificity in warrants, as opposed to the open and general warrants of the British crown. In the 1960s - when the first federal wiretap laws were written - "minimization" procedures were put in place, so that non-pertinent telephone conversations heard through wiretaps

were not collected or archived. Likewise, in the 1970s, the U.S. attorney general instituted procedures under which the FBI could only open investigations and gather data if a criminal predicate was first met - expressly limiting the FBI's ability to gather data and maintain data that was not relevant to a criminal investigation.

The advent of mass collection technologies - whether LPR or other techniques - have begun to place strains on this long-standing premise. Such technologies allow larger and larger data sets to be gathered on the public in general, for *possible* and *speculative* purposes, rather than focusing specifically on suspected or known lawbreakers. This has caused a rift to develop between our history and tradition, and our technological capabilities. Today, we would urge this committee to cast its vote on the side of tradition.

Since this debate started three years ago, we've supported the idea that non-hit data should be kept only as long as necessary to technically separate the hit data, from the non-hit data. This bill accomplishes that purpose by keeping hit data, and then discarding the non-hit data thereafter.

Finally and most importantly, it is worth noting that the debate over non-hit LPR data is bigger than just this single technology. With LPR, the Minnesota legislature will be establishing - for the first time - how it will treat data from mass surveillance technologies, including drones, facial recognition, and more. What is decided this session will have long-range consequences, and will set the baseline for the future relationship between the government, and its citizens in the realm of technological surveillance. We believe that this bill sets the correct and appropriate precedent for these consequential matters, and we urge you to support it. Thank you.