TESTIMONY OF SHENNA BELLOWS

LD 1561 – Ought to Pass

An Act To Regulate the Use of Traffic Surveillance Cameras

Submitted to the

JOINT STANDING COMMITTEE ON TRANSPORTATION

February 5, 2010

Senator Damon, Representative Mazurek and members of the Joint Standing Committee on Transportation, my name is Shenna Bellows, and I am the Executive Director for the Maine Civil Liberties Union, a state-wide organization committed to defending and advancing civil liberties and civil rights in Maine. On behalf of our over 3300 members, I urge you to pass LD 1561, An Act to Regulate the Use of Traffic Surveillance Cameras, to safeguard the liberty and security of ordinary Mainer who have broken no law going about their daily lives.

Automatic License Plate-Readers (ALPR) scan and store the license plates of any car that an equipped police cruiser encounters—on the highway, in a parking lot, in a neighborhood. The scanner then checks the plate against databases, watch-lists and the identity and location of the scan is stored in a police database.

Justice Louis Brandeis wrote in 1928, "The makers of the Constitution: conferred as against the government, the right to be let alone – the most comprehensive of rights and the right most valued by civilized men." Mainers cherish our right to be left alone by the government – to think, say, and do what we want as long as we are not hurting our neighbors or breaking the law. ALPRs, like all surveillance, threaten those fundamental privacy rights.

There are three primary civil liberties problems with this technology itself – the cameras, the hot lists, and most seriously, the database.

First, surveillance cameras, in themselves, have a chilling effect on freedom of movement. People behave differently when they believe themselves to be under surveillance. This has been a theory behind prison architecture for decades, and indeed, we have come to expect cameras in situations where heightened security is at issue – at the bank or the airport. Cameras on police cars can be very effective, and indeed, the ACLU has supported them in situations that protect both police and citizens, by videotaping arrests and questioning of suspects. But there is a difference between the camera used to monitor interactions between law enforcement and the public and surveillance cameras that monitor the ordinary activity of us, the people as we go about our daily lives. In a free society, we have an expectation that we are not being monitored by law enforcement unless we are suspected of wrongdoing or involved in a situation that

requires police action. All people in America are presumed innocent and law-abiding unless the evidence indicates otherwise. The very nature of these surveillance cameras turns that presumption of innocence on its head – into a presumption that we are all guilty.

Second, the cameras rely on "hot lists," lists fed into the camera by law enforcement to generate automated matches. Even if we can't agree that surveillance cameras in themselves have a chilling effect on a free society, then perhaps we can agree on the dangers of unlimited "hot lists." The technology that many of you have seen and you will hear described in more detail functions using "hot lists" that allow law enforcement to match a photographed license plate to a license plate number on a hot list. This technology allows law enforcement to use any hot list that they like or even to construct a hot list themselves. Imagine the potential abuse of such hot lists. Law enforcement could sweep the parking lot of a No on 1 or Yes on 1 rally…or a synagogue…or a mosque…or a church to record the license plate numbers, which would then enable law enforcement to use that list of license plate numbers to monitor the actions of those participants. Think that wouldn't happen in America? Ask the Eastern Maine Peace and Justice Center or Senator John Kerry or others who have been subjected to FBI surveillance because of their political activities. We have further concerns about use of some federally compiled lists, like the so-called terrorist watch list, which numbers over one million names and includes names like those of the civil rights leader and current Congressman John Lewis as well as eight-year old Mikey Hicks. Hot list technology that creates an automated match makes this surveillance camera system even more powerful and potentially threatening to civil liberties than an ordinary camera.

Third, the most dangerous aspect of this system is the database that the camera creates and feeds. I have seen this database in my visit to South Portland to meet with law enforcement. The database contains the record of every car law enforcement has encountered with a photograph, date, time and location. This database contains a virtual map of the movements of ordinary citizens about the community. Lieutenant Frank Clark has described this in the newspaper saying, "Information is gold." He is absolutely correct. Already, other jurisdictions are sharing these databases with repo companies looking to repossess vehicles whose owners are behind on payments. The commercial and political interest in these types of databases is enormous. A journalist friend of mine said when I shared with him the details of this information, "I do want to know if the mayor is at the liquor store. That's news." The newspaper…or one's political opponents…might very well be interested in who visits the liquor store or the adult video shop or a psychiatrist or a family planning center. Commercial entities have a strong interest in who shops at their stores or their competitor's stores. You will hear from supporters of this technology that their interest is very limited, but we know from experience that inevitably mission creep expands uses of these powerful technologies from law enforcement to intelligence gathering to total information awareness, all at the expense of the privacy of ordinary citizens.

This leads me to two questions about security and liberty raised by this technology. The first question is whether or not this data is subject to Maine's Right to Know laws or the Freedom of Information Act. There are generally exceptions for "investigatory information" for law enforcement, but ordinary citizens presumably are not under investigation. As a member of the Right to Know Advisory Committee I have received numerous complaints about the Right to Know laws being used to obtain private, personal information about Maine citizens in ways never intended by the government entity collecting that information.

The second question or concern is one about the security of the database and the hotlists themselves. As our opponents and we can agree – this information is a goldmine, which makes it more vulnerable to those who would do us wrong – to hackers who might be interested in stalking the movements of a potential victim, or selling the information to a political campaign or to a private company. The federal government, the State of Maine and large companies like Hannaford and Bank of America employ full-time data security departments and yet still suffer enormous data threats and breaches. Collecting this "gold" at local levels without property security safeguards will inevitably lead to data breaches. The question is not if this data will be breached, but when and how and at what cost to your constituents.

When the government invades our privacy by collecting information about our private, personal lives, the government then has a responsibility to ensure that we are kept safe from those who would seek merely to embarrass one of us or our neighbors to those who would do us harm. We are concerned that the hasty adoption of this technology has serious and dramatic implications for both our liberty and our security.

Now, I know and respect both Lieutenant Frank Clark and Chief Ed Googins. I accepted their invitation to meet and to discuss this technology in detail and look at the database. This is not about South Portland or the integrity of the South Portland police department but rather about policy for the entire state. This technology is very new and to a large extent untested. The technology has only existed for a few years, and most of the dozens of police departments around the country have only purchased it recently. New technological developments are always exciting and glamorous, but even as technology makes our lives easier or faster, technology also creates new challenges or problems. It's easy to focus on the excitement without fully considering the full range of implications. Just as Facebook users are only now grappling with the potential embarrassments or harm to their privacy might create from over-sharing, I fear that if we hastily adopt this new technology we will find ourselves grappling with significant embarrassments and harms in the future. Just because we can do something doesn't always mean we should.

The three civil liberties problems with the technology itself include the cameras, the hot lists used to create matches, and the database. Each of those technological elements creates liberty and security vulnerabilities. The urge to use the newest, fastest technology is not surprising, but ALPR's simply place too much data mining power in the hands of the police and those who breach their systems.