

Citizen Surveillance, Street Checks and the Right to Privacy

At the core of police street checks is citizens' personal information. After all, street checks are an intelligence tool meant to gather information that might be useful in future investigations. They are state-sponsored citizen surveillance. Information is gathered and recorded through observation and through stopping and requesting information from citizens. Who are you? Do you live around here? Where are you going? Why are you here? Who is your friend?

The right to privacy is based on the fundamental right of individuals to define themselves, to be free from arbitrary surveillance and from the judgement and values of others. Privacy is essential for the well-being of individuals. For this reason alone, it is worthy of protection, but it also has profound significance for public order. The restraints imposed on government to pry into the lives of citizens go to the essence of a democratic state.¹

The connection between privacy and human rights has never been more obvious than it is in a review of the use of street checks. Both are concerned with protecting human dignity and both support the ability of citizens to engage in public life without fear of or interference from police.

Privacy laws provide protections that restrain government's collection, use and disclosure of our personal information. Police in Nova Scotia are subject to those privacy laws.

As we review and consider the way forward on this challenging issue, a few essential privacy rules can help guide the way:

1. Demonstrate that street checks are legally necessary and authorized: Police may only collect personal information if they are legally authorized to do so. Having a clear analysis of when and if street checks are authorized is an essential first step. Randomly or arbitrarily collecting and recording identifying information to create a database for general intelligence purposes should be explicitly prohibited. Police officers must be trained so that they clearly understand the limited and specific circumstances, if any, in which street checks may be authorized and must be required to identify their authority in advance of any collection of personal information.

2. Keep personal information secure: Any personal information collected must be properly secured and must only be used for the limited and specific purposes allowed by law. Having clear rules about who and when the street check data may be accessed will help to protect the information. But equally important is the need to have an electronic audit trail so that there is a record of who accessed the data and when.

3. Build public trust through transparency: Finally, a meaningful right to privacy also includes citizens' right to know who is collecting the information, what the authority for the collection is, why it is being collected and how it will be used. Further, like our right to know who accesses our personal health information, citizens should be provided with the means to know who, when and why any individual has accessed street check data.

¹ Alan F. Westin, *Privacy and Freedom* (1970), pp. 349-50.

One very fundamental shortcoming in Nova Scotia's privacy law is that while municipal police are subject to privacy rules, they are not subject to any independent oversight. This means that if police violate Nova Scotia's privacy law, there is no legal right for citizens to complain to my office about that violation. Part of the solution therefore lies in ensuring that police are subject to meaningful independent oversight of their compliance with Nova Scotia's privacy rules.

Modern privacy protections support human rights protection and strengthen our democracy by restraining the power of police to pry into the private lives of citizens.

Catherine Tully is Nova Scotia's Information and Privacy Commissioner.