CANADIAN CIVIL LIBERTIES ASSOCIATION | ASSOCIATION CANADIENNE DES LIBERTES CIVILES

Oral Submission to the Standing Committee on Access to Information, Privacy and Ethics (ETHI) for the Study of Device Investigation Tools Used by the Royal Canadian Mounted Police

44th Parliament, 1st Session, August 9, 2022

Brenda McPhail, Ph.D.

Director, Privacy, Technology & Surveillance Program, Canadian Civil Liberties Association

Thank you for inviting the Canadian Civil Liberties Association to appear before you today. I am grateful to the Committee for commencing a study of the RCMP use of on-device investigative technology, an issue of national concern that is also a symptom of a larger problem of inadequate oversight and accountability when police acquire and use advanced surveillance technology.

The revelations about ODIT are just the latest in a series of similar media-led reveals regarding invasive techniques from social media monitoring to cell site simulators to illegal Clearview AI facial recognition. This isn't a one-off problem, it's a pattern pointing to a crisis of accountability. Operational secrecy is a legitimate need in specific investigations; secrecy around policies that apply to categories of dangerous surveillance technologies is not legitimate in a democracy. We must not allow law enforcement bodies to conflate one with the other to avoid accountability.

Why are these technologies dangerous from a civil society perspective? You are aware of the basic risks to privacy rights. So I'll focus on three other reasons. First, our government agencies are encouraging an industry known for prioritizing profits over human rights and feeding the worst impulses of authoritarian governments. I work with a network of global civil liberties organisations, where many of my colleagues see Canada as a role model on issues of law enforcement and due process. This kind of revelation diminishes our international reputation not just at the level of governments but on the ground.

Second, using these tools encourages law enforcement to exploit vulnerabilities in the technologies we all depend on rather than help get them fixed. We've known for some time that the CSE has dueling accountabilities in relation to their active cyber mandate

and their responsibility to protect our cyber infrastructure; now we know the RCMP have a similar conflict. This is making us all a bit less safe daily in the name of public safety.

And finally, there is the question of due process. Your witnesses yesterday noted that an agreement detailing the ways the technology has to be protected is a condition of its use. What impact does that agreement have on court disclosures? Are cases ever not taken forward because to do so would reveal details of the technology? How does operational secrecy compromise the pursuit of justice?

Those are some of the problems. What are the potential solutions?

First of all, we need a moratorium. This study is just the beginning of an important public conversation we must have. If it's true that this tech is a "last resort" option it can't be that much of a risk to public safety to pause its use, certainly not when weighed against the privacy and due process rights at stake, but also the social and diplomatic impacts of the Canadian government condoning the sale and use of spyware.

Then we need to go back to basics. And the basic question isn't "how do we make sure the RCMP or any other body uses these tools lawfully?", rather it must be, "is the use of such tools necessary, proportionate and in keeping with Canadian values?" It probably won't surprise you that I think it is not. I think, like Europe and the US, we should include the potential for a ban on state purchase of this kind of spyware technology in our conversations. But if it is democratically debated and determined that it is fit for a narrow purpose, the second question we then need to turn to is how to make the concept of "lawful use" more meaningful by updating our laws to appropriately govern the decisions to purchase and use such technologies, and to provide transparency and accountability sufficient to engender public trust.

For laws to be good enough, we first would need stringent, effectively enforced, import and export controls and limits.

We would need a system where decisions about using controversial and potentially rights-infringing technologies can no longer happen behind the scenes. For that we need not just mandatory PIAs, but should consider the creation of a truly independent advisory body working with appropriate transparency specifically to evaluate and set national standards for the procurement and use of surveillance technologies. Not a body internal to the RCMP, but rather a body along the lines of the New York State Task Force on the Regulation of Biometric Surveillance which includes police, government, civil society and legal and regulatory stakeholders with relevant expertise.

We would also need public reporting obligations on the use of ODITs. The annual report on the use of electronic surveillance repeatedly mentioned as an accountability

measure is insufficient; the tools used matter, that's why we're having this conversation, yet that report simply gives statistics for any audio or video surveillance.

Which leads to a final point. Only 1 warrant application of the 331 in that report was refused between 2016 and 2020. That suggests we need a public interest amicus to provide a counterpoint to the police position during warrant applications.

There are more problems and more solutions. But for that, I look forward to your questions.