

**Inquiry under Part 5 of the Freedom of Information and Protection of Privacy Act ("FOIPPA") between:**

**An Applicant**

**and**

**the Vancouver Police Department ("VPD")**

**and**

**BC Association of Chiefs of Police (intervenor) and BC Association of Municipal Chiefs of Police (intervenor) and BC Civil Liberties Association (intervenor) and BC Freedom of Information and Privacy Association (intervenor) and Open Media (intervenor) and Canada Research Chair of Ethics, Law and Technology, University of Ottawa (intervenor)**

**Submission of:** the British Columbia Civil Liberties Association and Canada Research Chair of Ethics, Law and Technology, University of Ottawa

**INTRODUCTION**

1. The Vancouver Police Department ("VPD") has withheld from the Applicant records ("the Records") relating to the use of cell site simulators, or IMSI catchers (commonly referred to as Stingrays) and refused to confirm or deny the existence of the Records under s. 8(2)(a) and s. 15(1)(c) of the *Freedom of Information and Protection of Privacy Act*, RSBC 1996, c 165 ("FOIPPA"):

8(2) Despite subsection (1) (c) (i), the head of a public body may refuse in a response to confirm or deny the existence of

(a) a record containing information described in section 15 (information harmful to law enforcement)

...

15(1) The head of a public body may refuse to disclose information to an applicant if the disclosure could reasonably be expected to

...

(c) harm the effectiveness of investigative techniques and procedures currently used, or likely to be used, in law enforcement

2. IMSI catchers are surveillance devices that intercept cell phones' and other wireless communication devices' connections to legitimate communication towers in order to collect data from the devices. Data collected by IMSI catchers may include geo-location, traffic and communications content data (Cavoukian, Ann, "Then and Now: Securing Privacy in Public Spaces", Information and Privacy Commissioner, Ontario, June 2013 [Reference Material for the Submissions of the British Columbia Civil Liberties Association and Canada Research Chair of Ethics, Law and Technology, University of Ottawa ("RM") Tab 1], available at <https://www.ipc.on.ca/images/Resources/pbd-surveillance.pdf>).

3. IMSI catchers collect data from devices that are within a given geographical range and thus, necessarily capture the data of vast numbers of the people who are not the targets of the surveillance. Some IMSI catchers are "able to intercept up to 60000 communications per hour" (see go2INTERCEPT, *GSM Interception – IMSI Catcher and Voice Interception*, go2SIGNALS, 2013 [RM Tab 6], available at <https://s3.amazonaws.com/s3.documentcloud.org/documents/1217047/1362-plat-product-list-product-description.pdf> at p. 3).

4. The British Columbia Civil Liberties Association and the Canada Research Chair of Ethics, Law and Technology, University of Ottawa (the "Intervenors") submit that the VPD has impermissibly refused to confirm or deny the existence of the Records, that the disclosure of all information contained in the Records could not reasonably be expected to harm the effectiveness of investigative techniques and procedures, and that the Records must be disclosed in the public interest.

## THE TEST FOR EXERCISING LAW ENFORCEMENT PRIVILEGE UNDER ACCESS TO INFORMATION LEGISLATION

5. Sections 8(2) and 15(1)(c) of *FOIPPA* allow for a discretionary exercise of law enforcement privilege in the context of access to information legislation. In *Ontario (Public Safety and Security) v. Criminal Lawyers' Association*, 2010 SCC 23 ("*CLA*"), the Supreme Court of Canada ("SCC") clarified that the exercise of discretionary law enforcement privilege ("may refuse") under access to information requires a consideration of factors both for and against disclosure, including a weighing of the public interest in disclosure (*CLA* at para. 46).

6. Thus, the assessment is a two-part test. The first step assesses whether the criteria for the privilege is met. If so, the second step addresses whether the disclosure should be made or refused. A primary factor in the second step is assessing the public interest in disclosure:

... these determinations [in the second step] necessarily involve consideration of the public interest in open government, public debate and the proper functioning of government institutions. A finding at the first stage that disclosure may interfere with law enforcement is implicitly a finding that the public interest in law enforcement may trump public and private interests in disclosure. At the second stage, the head must weigh the public and private interests in disclosure and non-disclosure, and exercise his or her discretion accordingly.

*CLA*, para. 48

7. The Intervenors submit that the VPD's claim that the Records are subject to law enforcement privilege fails at both stages of the two-part test.

**DISCLOSURE OF THE RECORDS CANNOT REASONABLY BE EXPECTED TO HARM THE EFFECTIVENESS OF INVESTIGATIVE TECHNIQUES AND PROCEDURES**

8. The VPD has the burden of proof in demonstrating that the Applicant has no right of access to the Records (*FOIPPA*, s. 57).

9. Part one of the assessment requires the VPD to demonstrate that it has met the criteria for the specific type of discretionary privilege that is allowable under the relevant sections of *FOIPPA*. The criteria is that disclosure could reasonably be expected to harm the effectiveness of investigative techniques and procedures ("ITPs") currently used, or likely to be used, in law enforcement.

10. The discretionary exception from disclosure to protect ITPs is clearly harms-based. The VPD must adduce sufficient evidence to demonstrate harm. The requirements are summarized in OIPC BC Order 00-01 *Inquiry Regarding Langley Township Bylaw Enforcement Records* at p. 5:

To summarize what I said about the reasonable expectation test in Order No. 323-1999, a public body must adduce sufficient evidence to show that a specific harm is likelier than not to flow from disclosure of the requested information. There must be evidence of a connection between disclosure of the information and the anticipated harm. The connection must be rational or logical. The harm feared from disclosure must not be fanciful, imaginary or contrived.

11. Further, this harms-based test involves harms that are probable harms and "well beyond" merely possible. The language used in s. 15(1)(c) of *FOIPPA* is that harm to the effectiveness of ITPs "could reasonably be expected". The "could reasonably be expected" standard has been interpreted by the SCC in *Ontario (Community Safety and Correctional Services) v. Ontario (Information and Privacy Commissioner)*, 2014 SCC 31, at para. 54:

This Court in *Merck Frosst [Merck Frosst Canada Ltd. v. Canada (Health)]*, 2012 SCC 3] adopted the "reasonable expectation of probable harm" formulation and it should be used wherever the "could reasonably be expected to" language is used in access to information statutes. As the Court in *Merck Frosst* emphasized, the statute tries to mark out a middle ground between that which is probable and that which is merely possible. An institution must provide evidence "well beyond" or "considerably above" a mere possibility of harm in order to reach that middle ground: paras. 197 and 199.

*IMSI catchers are not secret - they are well-publicized*

12. It is no secret that Canadian police may be using or planning to use IMSI catchers. There has been a vibrant public discourse about the possible use of IMSI catchers by police in Canada, with a vast array of media outlets reporting on this matter, including the *Globe and Mail*, *CBC News*, *CTV News*, the *Vancouver Sun*, *Winnipeg Free Press*, *Radio-Canada*, *Global News*, the *Province*, the *Vancouver Courier*, the *Tyee*, *Huffington Post*, the *Toronto Star* and others. Most recently the *Globe and Mail* reported on a criminal case in which the RCMP acknowledged the use of a "mobile device identifier" during an investigation that took place from 2010 to 2012. Defence counsel is seeking confirmation that the device(s) acknowledged are IMSI catchers (see Freeze, Colin et al., "RCMP fight to keep lid on high-tech investigation tool", the *Globe and Mail*, Mar. 13, 2016 [RM Tab 5], available at <http://www.theglobeandmail.com/news/national/rcmp-trying-to-keep-lid-on-high-tech-methods-used-to-fight-mafia/article29204759/>).

13. Extensive use of IMSI catchers by police and intelligence agents in other jurisdictions has been reported in the media. Jeremy Scahill and Margot Williams in "Stingrays: A Secret Catalogue of Government Gear for Spying on Your Cellphone" cite "nearly 60 law enforcement agencies in 23 [U.S.] states [that] are known to possess a Stingray or some form of cell-site simulator, though experts believe that number likely underrepresents the real total." (Scahill, Jeremy and Williams, Margot, "Stingrays – A Secret Catalogue of Government Gear for Spying on Your Cellphone", *The Intercept*, Dec. 17, 2015 [RM Tab 8], available at <https://theintercept.com/2015/12/17/a-secret-catalogue-of-government-gear-for-spying-on-your-cellphone>).

14. Police use of IMSI catchers is the subject of investigative journalism in Europe (see Volynsky, Masha, "Spy games turn real as eavesdropping technology spreads", *Radio Prague*, Aug. 16, 2012 [RM Tab 10], available at <http://www.radio.cz/en/section/curraffrs/spy-games-turn-real-as-eavesdropping-technology-spreads>; Foss, Andreas et al., "Secret surveillance of Norway's leaders detected", *Aftenposten*, Dec. 16, 2014 [RM Tab 4], available at <http://www.aftenposten.no/nyheter/iriks/Secret-surveillance-of-Norways-leaders-detected-7825278.html>).

*IMSI catchers are not secret – they are properly subject to legislation in other jurisdictions*

15. Growing awareness of IMSI catchers and controversy regarding the serious risk of improper use and violation of citizens' privacy rights has resulted in several jurisdictions bringing in laws with respect to police use of IMSI catchers. The *New York Times* reports that laws with respect to IMSI catchers by law enforcement authorities have been introduced and/or approved in Washington, Utah, Virginia, California, Texas and in U.S. Congress (see Williams,

Timothy, "Covert Electronic Surveillance Prompts Calls for Transparency", *The New York Times*, Sep. 28, 2015 [RM Tab 11], available at

[http://www.nytimes.com/2015/09/29/us/stingray-covert-electronic-surveillance-prompts-calls-for-transparency.html?\\_r=0](http://www.nytimes.com/2015/09/29/us/stingray-covert-electronic-surveillance-prompts-calls-for-transparency.html?_r=0)).

16. In Germany the use of IMSI catchers by law enforcement agencies is authorized by statute, which also mandates statistical reports on their usage. Information about German law enforcement's use of IMSI catchers is published by the Parliament at regular intervals and there have been several formal parliamentary questions submitted regarding the use of IMSI catchers, as well as a decision from the German Constitutional Court regarding their use (see Directorate-General for Internal Policies, Policy Department C – Citizens Rights' and Constitutional Affairs, Civil Liberties, Justice and Home Affairs, *Parliamentary Oversight of Security and Intelligence Agencies in the European Union –Study*, European Parliament, 2011 [RM Tab 3], available at

<http://www.europarl.europa.eu/document/activities/cont/201109/20110927ATT27674/20110927ATT27674EN.pdf> ; Soghoian, Christopher et al., *Written Remarks for the German Parliament Committee of Inquiry*, Speech, Privacy & Technology Project, The American Civil Liberties Union, Jun. 26, 2014 [RM Tab 9], available at <http://files.cloudprivacy.net/bundestag-testimony-csoghoian-june-26-final.pdf>).

17. Not only have some jurisdictions legislated with respect to IMSI catchers, some acknowledge a benefit in being transparent with respect to their use and policies. This can be seen in the United States Department of Justice press release announcing "a new policy for its use of cell-site simulators that will enhance transparency and accountability..." (see Department of Justice, Office of Public Affairs, *Justice Department Announces Enhance Policy for Use of*

*Cell-Site Simulators*, The United States Department of Justice, Sep. 3, 2015 [RM Tab 2], available at <https://www.justice.gov/opa/pr/justice-department-announces-enhanced-policy-use-cell-site-simulators>), and, in the case of Germany, mandated regular reporting on the use of IMSI catchers.

*Disclosure of well publicized ITPs cannot reasonably be expected to cause probable harm to their effectiveness*

18. The VPD claims that even the acknowledgement that it does or does not possess information about IMSI catchers could reasonably be expected to be harmful to the effectiveness of their use of IMSI catchers, now or in the future. It is not possible to logically support this claim in light of growing public awareness of IMSI catchers, the well-publicized fact that Canadian police may be using IMSI catchers, and the number of other jurisdictions that have acknowledged and legislated with respect to their police use of IMSI catchers.

19. The OIPC has previously addressed the importance of publicity as a factor in the law enforcement privilege analysis. In considering the scope of s. 15(1)(c) of *FOIPPA*, OIPC BC Order No. 50-1995 in *Inquiry Re: A decision by the Ministry of Finance and Corporate Relations to refuse access to records from an internal audit concerning a conflict of interest investigation* adopted the reasoning of Ontario Information and Privacy Commissioner Order 170 in Appeal 880222 dated May 25 1990, in which sufficient publicity of the impugned ITPs was generally found to preclude the possibility that their effectiveness could be impaired by disclosure:

In order to constitute an "investigative technique or procedure" in the requisite sense, it must be the case that disclosure of the technique or procedure to the public would hinder or compromise its effective utilization. The fact that the particular technique or procedure is generally known to the public would



normally lead to the conclusion that such compromise would not be effected [sic] by disclosure and according [sic] that the technique in question is not within the scope of the protection afforded by section 14(1)(c) [of the Ontario *Freedom of Information and Protection of Privacy Act*] (pp. 30-31). [emphasis added]

20. The logic that prevents generally known ITPs from being subject to non-disclosure rules extends beyond the context of access to information requests. In a different context (publication bans) the SCC analysed how disclosure of certain well-publicized aspects of undercover operations affect the efficacy of the operations.

... the danger to the efficacy of the operation is not significantly increased by republication of the details of similar operations that have already been well-publicized in the past. It is the incremental effect of the proposed ban, viewed in light of what has already been published before, that must be evaluated in this appeal.

*R. v. Mentuck*, 2001 SCC 76, para. 45 ["*Mentuck*"]

21. The VPD takes the position that any information it discloses, including acknowledging that there is or is not information *to* disclose, could reasonably be expected to reduce the effectiveness of the technique. But information about IMSI catchers, like the "Mr. Big" techniques that were at issue in *Mentuck*, is already widely available. That IMSI catchers exist, that many police forces use them, and that many police forces, including Canadian police, are resisting efforts to access information about police use of IMSI catchers, are public facts well reported in the media. Thus, even if the test were one of hypothetical risk and not one dependent on evidence, the theoretical possibility of a reduction in effectiveness caused by acknowledging the existence or nonexistence of the Records could only have a vanishingly small, incremental effect on the effectiveness of the technique given the context of the current publicity.

22. Further, we note that after a ruling that upheld the Toronto Police Service's Board's decision to neither confirm nor deny information about IMSI catchers, the Toronto Police casually waived the privilege. "I have made some inquiries and we do not use the Stingray

technology and do not have one of the units", Craig Brister, Toronto Police spokesperson, is reported as having written to the *Toronto Star*. As such, despite submissions on their behalf to the Ontario OIPC to the contrary, the Toronto Police have most recently demonstrated no concern that harm could reasonably be expected from the release of such basic information to the public (see King, Robin Levinson, "The cellphone spyware the police don't want to acknowledge", *Toronto Star*, Dec. 15, 2015 [RM Tab 7], available at <http://www.thestar.com/news/canada/2015/12/15/the-cellphone-spyware-the-police-dont-want-to-acknowledge.html>).

23. Consequently, the VPD cannot reasonably assert that harm is probable, which it must be able to demonstrate to meet the requisite standard. Any anticipated harms from disclosure are speculative, marginal and without logical connection. The evidentiary burden in the first part of the test is not met, which is determinative of the question.

### **DISCLOSURE OF THE INFORMATION SHOULD BE MADE IN THE PUBLIC INTEREST**

24. Although the VPD cannot demonstrate probable harm resulting from general disclosure, an analysis of the second part of the test is instructive. The second part of the test asks whether, having regard to the significance of any risk of harm to effectiveness, disclosure should be made in the public interest. This part of the test necessarily involves "consideration of the public interest in open government, public debate and the proper functioning of government institutions" (*CLA*, para. 48).

25. We will address the public interest in disclosure of the Records under three headings: 1) police accountability; 2) protection of individuals' constitutional rights; and 3) the scale of the privacy rights concern.

26. We incorporate the values of the *Canadian Charter of Rights and Freedoms*, Part I of the *Constitution Act, 1982*, being Schedule B to the *Canada Act 1982 (U.K.), 1982, c. 11* (the "*Charter*") into our analysis. Legislative provisions are to be interpreted so as to conform to the *Charter* in so far as possible and only if they cannot be so interpreted are they invalid (*R. v. Tse*, 2012 SCC 16, para. 20 ["*Tse*"]). The disclosure or non-disclosure of the Records necessarily involves *Charter* values, in particular with respect to section 8 of the *Charter*, which provides "not just freedom from unreasonable search and seizure, but also the ability to identify and challenge such invasions" (*Tse*, para. 83 quoting the intervener Criminal Lawyers' Association (Ontario)'s factum at para. 31, emphasis added) and section 2(b) of the *Charter*, under which denial of access to information may be a violation of the right to freedom of expression in certain circumstances.

*The public interest in ensuring the proper functioning of government - Police Accountability*

27. Underlying the request for the Records is a pressing concern about police accountability.

As the SCC stated in *Mentuck* at paras. 50 and 51:

... A fundamental belief pervades our political and legal system that the police should remain under civilian control and supervision by our democratically elected officials; our country is not a police state. The tactics used by police, along with other aspects of their operations, is a matter that is presumptively of public concern.

....

...[t]here has always been and will continue to be a concern about the limits of acceptable police action. The improper use of bans regarding police conduct, so

as to insulate that conduct from public scrutiny, seriously deprives the Canadian public of its ability to know of and be able to respond to police practice that, left unchecked, could erode the fabric of Canadian society and democracy.

28. The information that is being sought in this matter goes to the very heart of an important police accountability issue. The use of IMSI catchers in other jurisdictions has generated legislative and policy reforms with respect to police use of these controversial surveillance devices. The critical examination that should be underway in Canada on this topic is currently confined to academic discussions and public discussion in the media. There is no meaningful legal or policy response to current or anticipated use of IMSI catchers. Refusal to confirm or deny police use or anticipated use of IMSI catchers is retarding or even preventing a meaningful legal and policy engagement with the issue. As such, the values underlying s. 2(b) of the *Charter* are engaged. Access to information is a derivative right under s. 2(b) "which may arise where it is a necessary precondition of meaningful expression on the functioning of government" (*CLA*, para. 30).

*The public interest in ensuring the protection of individuals' constitutional rights*

29. Even more so, the values underlying s. 8 of the *Charter* are central to this assessment. There is a reasonable expectation of privacy in cell phone activity (*R. v. Mahmood*, 2011 ONCA 693). Section 8 protects against intrusion of the state on an individual's privacy. As the SCC stated in *Hunter et al. v. Southam Inc.*, 1984 2 S.C.R. 145, s. 8 "requires a means of preventing unjustified searches before they happen" (at p. 160, emphasis in the original). Typically, this has meant prior judicial authorization, the importance of which "is even greater for covert interceptions of private communications" (*Tse*, para. 17). In exceptional cases in which prior authorization is not mandated, subsequent oversight must be available. The essential principle is that the State must in all instances demonstrate that intrusions on individuals' privacy are

reasonable. Only on this basis can s. 8 serve its function as "a shield against unjustified state intrusion on personal privacy" (*R. v. Kang-Brown*, 2008 SCC 18, para. 8).

30. The principle that the State must justify its intrusions on individuals' privacy interests has important implications for its disclosure obligations. In *Tse* the SCC found that the absence of an after-the-fact notice requirement in a *Criminal Code* provision permitting wiretapping without prior approval was a "fatal defect":

The jurisprudence is clear that an important objective of the prior authorization requirement is to prevent unreasonable searches. In those exceptional cases in which prior authorization is not essential to a reasonable search, additional safeguards may be necessary, in order to help ensure that the extraordinary power is not being abused. Challenges to the authorizations at trial provide some safeguards, but are not adequate as they will only address instances in which charges are laid and pursued to trial. Thus, the notice requirement, which is practical in these circumstances, provides some additional transparency and serves as a further check that the extraordinary power is not being abused.

*Tse*, para. 84

31. As the provisions of *FOIPPA* must comply with s. 8, the access to information exceptions cannot shield from disclosure all information with respect to ITPs that intrude on a reasonable expectation of privacy. Such intrusion engages the protection of s. 8 and requires the police to establish that the intrusion is reasonable. Without such basic disclosure, individuals, who are entitled to challenge state interference of their privacy, are simply precluded from being able to exercise that right.

32. Section 15(1)(c) of *FOIPPA*, particularly in light of s. 8(2)(a) (the additional 'neither confirm or deny') cannot be read as allowing the withholding of any and all information with respect to IMSI catchers, which clearly are ITPs with the ability to intrude on a reasonable expectation of privacy. Such a reading is not only counter to s. 8 of the *Charter*, it effectively provides a means of undermining the protections of s. 8. We submit that, in order to be

interpreted to comply with s. 8, the relevant sections of *FOIPPA* cannot apply to ITPs that intrude on a reasonable expectation of privacy. And as such, that the VPD cannot refuse to respond to the request for Records.

*The public interest in addressing privacy rights concerns on a scale that likely affects many thousands of people*

33. The scale of the privacy rights concern is a factor that should be considered in weighing the public interest in disclosure of the Records. The nature of the surveillance that takes place with IMSI catchers is akin to that of "tower dumps". In Canada, police can obtain a production order for all records of cellular phone traffic through a particular cell tower over a specific period of time. These are known as tower dump production orders. Tower dumps share with IMCI catchers the feature of gathering the personal information of a great many people who are not the targets of the police surveillance.

34. Recently in *R. v. Rogers Communications*, 2016 ONSC 70 ("*Rogers Communications*"), the Court found the tower dump production orders at issue to have authorized unreasonable searches in violation of the rights of the Rogers and Telus subscribers whose information was captured in the production orders. The Court went on to give guidance on how to tailor production orders to conform to the *Charter* by respecting the principles of incrementalism and minimal intrusion.

35. The evidence in *Rogers Communications* showed that the scale and scope of unconstitutional searches through overly broad tower dump production orders was potentially staggering. In affidavit evidence, Telus testified that had it dealt with thousands of court orders requiring cell records since 2004, and in 2013 responded to approximately 2,500 production

orders and general warrants. Rogers had records of many thousands of court orders requiring the production of cell records dating back decades, and in 2013 alone "produced 13,800 'files' in response to production orders and search warrants" (para. 10). Any one of the thousands of orders could require the production of records of thousands of people. One of the specific production orders at issue in the case was so overbroad that it required production of personal information pertaining to over 40,000 subscribers when information of only a few individuals was actively sought by the police (para. 42).

36. The many thousands of people whose information had been unjustifiably collected through insufficiently tailored tower dump production orders would have no means of defending their privacy except through their service providers. One of the issues in this case was whether Rogers and Telus had standing to defend their subscribers' privacy. The Court found that they did have standing to assert the privacy interests of their customers and were contractually obliged to do so. The importance of the standing question was highlighted by the Court:

The choice is stark. There is an issue concerning the privacy rights of hundreds of thousands of Canadians. If Rogers and Telus are correct, this legal issue can and will be addressed with opposing points of view put forward by counsel. A decision on point can provide guidance to the police and issuing justices. If the Respondent is correct, this legal issue will never be addressed and some justices of the peace will continue to grant similar production orders which, as I will later explain, are overly broad and unconstitutional

*Rogers Communications*, para. 37

37. Police use of IMSI catchers raises the same concern about how to protect the privacy rights of unknown numbers of individuals who are not the target of police surveillance. Only with IMSI catchers, there are no telecommunications service providers able and obliged to defend their subscribers' privacy interests. Thus, the choice is even starker than in *Rogers Communications*. Acknowledgement of the use or anticipated future use of IMSI catchers is the

first step to providing guidance to the police and issuing justices, and protecting the privacy rights of thousands of individuals. Failure to disclose the information allows for the use of IMSI catchers without proper authorization or with authorizations that are overly broad and unconstitutional in the same way tower dumps had been operating prior to *Rogers Communications*.

38. Finally, as noted in *Rogers Communications*, there is no legislation that "addresses the retention of tower dump records nor other more invasive collections of personal information such as wiretap evidence" (para. 60). As another component of the need for disclosure of the Records in the public interest, IMSI catchers clearly should be part of the considerations for any future legislative reforms in post-seizure data retention periods and safeguards.

#### **THE CHARTER OF RIGHTS AND FREEDOMS**

39. The nature of the question in this inquiry is the exercise of discretion for a claim of law enforcement privilege under access to information legislation. We are confident that the legislative provisions can and will be interpreted to conform to the *Charter*. Were this to prove not to be the case, we would argue that the provisions themselves were a violation of ss. 2(b) and 8 of the *Charter*, on the basis of the arguments above describing the nature of the applicable *Charter* values. We would further argue that such a violation could not be justified under section 1 of the *Charter*.

#### **NOT ADDRESSING SECTION 25 OF FOIPPA**

40. We are choosing not to address s. 25 of *FOIPPA* (disclosures in the public interest) as our reading of the applicable test, as per *CLA*, already incorporates a public interest analysis.



41. That said, we submit that any of our public interest arguments would be equally applicable to an analysis under s. 25. The authority for that proposition is *CLA* at para. 43, in which the Court finds the law enforcement privilege analysis incorporating a public interest assessment and the assessment that would be done under the public interest override provision in the access to information legislation in that case are essentially the same analysis.

## **CONCLUSION**

42. In summary, we say that the VPD cannot demonstrate on the basis of evidence and logic that any and all information contained in the Records, including the mere fact of whether the Records exist or not, should be withheld on the grounds that it would cause probable harm to the effectiveness of the ITPs to disclose the information.

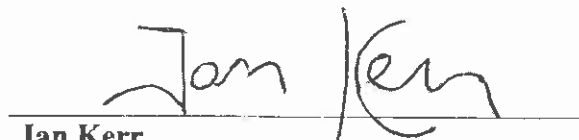
43. Even if the VPD were to demonstrate on the basis of evidence and logic that all information contained in the Records, including the mere fact of whether the Records exist or not, must be withheld to prevent probable harm to the effectiveness of the ITPs, the Records should nevertheless be disclosed in the public interest. The harms that could flow from acknowledging already well-publicized ITPs cannot override the overwhelming public interest in ensuring the proper functioning of government with respect to police accountability and the protection of individuals' constitutional rights. We say this is particularly so with respect to the issue of police use of IMSI catchers which, like tower dumps, inherently have the potential to

violate vast numbers of individuals' rights, with virtually no means of redress if the use of the IMSI catchers remain secret.

Respectfully submitted this 23rd day of March, 2016.

A handwritten signature in cursive script, appearing to read "M. Vonn" with a horizontal line extending to the right.

**Micheal Vonn and Michael Elliot**  
British Columbia Civil Liberties  
Association

A handwritten signature in cursive script, appearing to read "Ian Kerr" with a horizontal line extending to the right.

**Ian Kerr**  
Canada Research Chair of Ethics, Law  
and Technology, University of Ottawa

## **LIST OF AUTHORITIES**

*Hunter et al. v. Southam Inc.*, 1984 2 S.C.R. 145

*Inquiry Re: A decision by the Ministry of Finance and Corporate Relations to refuse access to records from an internal audit concerning a conflict of interest investigation*, OIPC BC Order No. 50-1995

*Inquiry Regarding Langley Township Bylaw Enforcement Records*, OIPC BC Order 00-01

*Ontario (Public Safety and Security) v. Criminal Lawyers' Association*, 2010 SCC 23

Order 170, Appeal 880222, Information and Privacy Commissioner of Ontario

*R. v. Kang-Brown*, 2008 SCC 18

*R. v. Mahmood*, 2011 ONCA 693

*R. v. Mentuck*, 2001 SCC 76

*R. v. Rogers Communications*, 2016 ONSC 70

*R. v. Tse*, 2012 SCC 16

## **LEGISLATION**

*Canadian Charter of Rights and Freedoms*, ss. 1, 2(b), 8Part I of the *Constitution Act, 1982*, being Schedule B to the *Canada Act 1982* (U.K.), 1982, c. 11

*Freedom of Information and Protection of Privacy Act*, RSBC 1996, c 165, ss. 8(2), 15(1)(c), 25, and 57