SUPREME COURT OF FLAVELLE

ON APPEAL FROM

THE COURT OF APPEAL FOR FALCONER

BETWEEN:

FLAVELLE PRIVACY ADVOCACY CENTRE

Appellant

– and –

HER MAJESTY THE QUEEN

Respondent

An appeal concerning whether s.400 of the Flavellian *Criminal Code*

violates the *Charter of Rights and Freedoms*

FACTUM OF THE RESPONDENT

TABLE OF CONTENTS

PART I - OVERVIEW

1. Section 400 of the Flavellian *Criminal Code* represents Parliament's responsible and measured response to the evolution of modern criminality. It allows police to use sophisticated and innovative investigative techniques to apprehend dangerous criminals who use modern communications technology to facilitate and perpetrate crimes. Further, it does so while respecting the s. 8 privacy interests of Flavellians. S.400 allows law enforcement to collect and analyze anonymous metadata. To do so, they must prove to a judge that there are "reasonable grounds to suspect" that an offence has been or will be committed, and that the metadata to be collected will assist in the investigation of the offence.
2. The Appellant in this case, the Flavelle Privacy Advocacy Centre ("FPAC"), should not have been granted standing to challenge s.400. As a general research and advocacy group, it does not have the necessary direct connection to the broad constituencies that it seeks to represent in this case. Moreover, other groups with a more direct link to the subject matter of this litigation could easily launch a similar challenge. FPAC's proposed action is neither a reasonable nor an effective means of challenging s.400.
3. The Court of Appeal was correct in finding that s. 400 does not violate s.8 of the *Charter*. There is no reasonable expectation of privacy in the sort of innocuous metadata that s.400 production orders reveal. Furthermore, even if the metadata itself could potentially reveal intimate details about an individual's "biographical core", the anonymous nature of metadata vitiates any privacy concerns. "Reasonable suspicion" is a constitutionally compliant standard for an order authorizing the bulk collection and analysis of metadata

because it strikes a balance between the legitimate needs of law enforcement and the privacy interests of Flavellians.

4. The Court of Appeal was also correct in finding that any breach of s.8 could nevertheless be justified under s.1 of the *Charter*. S.400 is a proportionate and reasonable measure that contributes significantly to the pressing objective of combatting sophisticated, modern criminality. If s.400 infringes of s.8 of the *Charter* at all, it does so minimally and in a manner narrowly tailored to achieve its objectives. Any deleterious consequences of s.400 are remote and *de minimis*, and therefore can be justified in a free and democratic society.

PART II – STATEMENT OF FACTS

A. Factual Background

5. The "Carnegie" criminal organization, led by Victorius, smuggled vast quantities of illegal firearms into Flavellian communities throughout the summer of 2013. This smuggling precipitated a rapid and unprecedented increase in gun crime. Despite the best efforts of law enforcement, the flow of weapons continued unabated; it was impossible to shut down the organization without apprehending its leader. Traditional investigative techniques proved insufficient to apprehend Victorius, who used modern communications technology and a complex travel schedule to evade detection. Victorius could maintain control of a modular and decentralized criminal organization in a way that would not have been possible in the past.

   Official Grand Moot Problem, paras 3-4 [*Problem*].

6. The Flavelle National Policing Authority (FNPA) worked diligently to tackle the root cause of the violence: the "Carnegie" organization. During their investigation, they discovered evidence of the ringleader Victorius' travel patterns. Specifically, s/he was at the Austin airport on August 15, 2013 and travelled on a rigid weekly rotation between three cities.

   Problem, *supra* para 5 at paras 6-7.

7. Based on their knowledge of Victorius' travel schedule, the FNPA developed a strategy for apprehending Victorius using novel investigative techniques. FNPA requested and received an order from the court pursuant to s.400 of the Flavellian *Criminal Code*. The order required Hammerstein Inc (the national cell phone service provider) to produce

three months of historical tracking data for the phone numbers captured by the Austin airport cell phone tower on August 15, 2013. Tracking data is defined as data that relates to the *location* of a transaction, individual or thing. It is collected every time a device passes near a cell phone tower and thus updates frequently. Tracking data can place a device within a 50 meter radius. The contract between Hammerstein and its customers allowed the provider to collect this data from subscribers.

Problem, *supra* para 5 at paras 12, 14-15.

8. The tracking data produced by the order was to be analyzed by a computer system. This system would filter out any mobile phone numbers that did not follow Victorius's travel schedule. Although the order produced over 20,000 unique phone numbers, it is likely that the overwhelming majority of those numbers would not match Victorius' precise schedule and thus be viewed by an FNPA officer.

Problem, *supra* para 5 at paras 15-16.

9. Before the FNPA had a chance to conduct this analysis, information about the use of tracking data became public. Without any charges having yet been laid, Flavelle Privacy Advocacy Centre (FPAC) brought an application before the courts to declare s. 400 of the *Criminal Code* unconstitutional. In response to public concern over what an anonymous leaker described as "bulky surveillance" at Austin Airport, FNPA issued a statement. In that statement, the FNPA clarified the meaning of tracking data and reminded citizens that to obtain any subscriber information associated with tracking data collected under s.400, the FNPA would have to obtain judicial authorization based on "reasonable and probable grounds".

Problem, *supra* para 5 at para 19.

10. FPAC is an advocacy and research group that has indicated an interest in issues relating to "mass surveillance". Though it has acted as an intervener in two prior s. 8 cases, FPAC has never before been a party to public interest litigation.

Problem, *supra* para 5 at paras 20-21.

B. Trial Judgment

11. At trial, Justice Bessemer granted FPAC standing. She found a reasonable expectation of privacy in metadata on the basis that tracking data allows the viewer to determine an individual's location. The judgment raised a number of theoretical concerns, as Justice Bessemer held that "[m]etadata *may* give insight to an individual's medical status, political inclinations, personal and family relationships and professional ambitions" (emphasis added). Justice Bessemer found that the requirement for prior judicial authorization in s.400 did not prevent the section from being unconstitutional, as the standard used to obtain an order under s. 400 is "reasonable grounds to suspect" rather than "reasonable and probable grounds". Further, Justice Bessemer found that the scope of s. 400 was unreasonable, both in the time frame of the data that may be collected and the number of people who might have their data collected. Justice Bessemer recognized the importance of law enforcement having the tools to respond to crime using modern technology but refused to save s. 400 under s. 1 of the *Charter*. She did so on the basis that the provisions were insufficiently specific about the sorts of situations in which metadata might be collected and because there was significant potential for the provisions to be abused.

Problem, *supra* para 5 at paras 23-26.

C. Court of Appeal Judgment

12. The Court of Appeal unanimously overruled the trial judgment and the majority upheld s. 400 as constitutional. Justice Keith, writing for the majority, found that there was no reasonable expectation of privacy in tracking data and therefore that there had been no search. She found that tracking data does not provide private information that touches on an individual's "biographical core" for several reasons. First, she noted that tracking data is anonymous. Second, she analogized this information to the sort that police can obtain lawfully from physical surveillance. Third, pointed out that tracking data only relates to a device, not the individual using it – hence providing no details about the identity or activities of the phone's user at a given time or place.

    Problem, *supra* para 5 at paras 27-30.

13. Although she was not required to do so, Justice Keith also addressed s. 1 of the *Charter*. She found that the law had a pressing and substantial objective – namely, to equip police and prosecutors with the necessary means to investigate offenses in the modern, "high tech," environment. Further, she held that s. 400 was proportionate to its objective. Requiring a more onerous standard, such as reasonable and probable grounds, would render the section ineffective in allowing police to stop crimes before they occur.

    Problem, *supra* para 5 at para 31.

14. In a concurring judgment, Justice Neil held that FPAC did not have standing to bring a claim as they did not have a real and continuing interest in the matter. Justice Neil held that those with a direct interest in the matter, such as frequent flyers or airline employees,

were well placed to bring the claim and should be given priority in the allocation of judicial resources.

Problem, *supra* para 5 at paras 32-33.

PART III – STATEMENT OF POINTS IN ISSUE

15. There are four issues on appeal:

Issue 1 **Does FPAC have standing to challenge the constitutionality of s. 400 of the Flavellian *Criminal Code*?**

The Respondent's position is that FPAC's action does not meet the requirements for public interest standing and therefore should not have gone forward.

Issue 2 **Is there a reasonable expectation of privacy in tracking data pursuant to s. 8 of the *Charter*?**

The Respondent's position is that there is not reasonable expectation of privacy in metadata and, alternatively, that any such expectation is *de minimis*.

Issue 3 **If the answer to issue 2 is "yes", are the powers created by s. 400 "reasonable" and was the search itself "reasonable"?**

The Respondent's position is that s. 400 is a reasonable law, that the search in this case complied with s. 400, and that the search was conducted reasonably.

Issue 4 **If a breach of s. 8 is found, can s. 400 be upheld under s. 1 of the Charter?**

The Respondent's position is that s. 400 can be justified under s.1 as a reasonable limit prescribed by law.

PART IV – ARGUMENT

Issue 1: FPAC does not have standing to challenge the constitutionality of s. 400 of the Flavellian Criminal Code

16. Flavelle has many well-meaning groups. However, in the words of Justice Cory in *Canadian Council of Churches v Canada (Minister of Employment and Immigration)*, to allow each to "[pursue] their own particular cases certain in the knowledge that their cause is all important" would be disastrous.

> *Canadian Council of Churches v Canada (Minister of Employment and Immigration)*, [1992] 1 SCR 236, 88 DLR (4th) 193.

17. Most *Charter* litigation is conducted by individuals who are personally affected by the alleged *Charter* breach. Directly affected parties provide a "[c]oncrete adverseness [which] sharpens the the debate of the issues." The parties' personal investment in the outcome "helps ensure that the arguments are presented thoroughly and diligently." From time to time, however, courts may exercise their discretion to grant "public interest standing" to groups that are not directly affected by legislation or government action. FPAC seeks such standing here.

> *Canada (Attorney General) v Downtown Eastside Sex Workers United Against Violence Society,* 2012 SCC 45, [2012] 2 SCR 524 citing in part *Baker v Carr*

18. In deciding whether to grant public interest standing, courts must be mindful of the reasons for limiting standing. Those reasons have been clearly elucidated by the courts.

In *Canada (Attorney General) v Downtown Eastside Sex Workers United Against Violence,* Justice Cromwell stated that:

> Limitations on standing are necessary in order to ensure that courts do not become hopelessly overburdened with marginal or redundant cases, to screen out the mere "busybody" litigant, to ensure that courts have the benefit of contending points of view of those most directly affected and to ensure that courts play their proper role within our democratic system of government.
>
> *SWUAV, supra* para 17 at para 1.

19. Courts look to three factors to determine whether an organization may bring a case based on public interest standing:

> a) whether the case raises a serious justiciable issue;
>
> b) whether the party bringing the case has a real stake in the proceedings or is engaged with the issues that it raises; and
>
> c) whether the proposed suit is, in all of the circumstances and in light of a number of considerations, a reasonable and effective means to bring the case to court.
>
> *SWUAV*, *supra* para 16 at para 2.

20. There is no disagreement that the case raises a serious justiciable issue. However, the parties differ as to whether FPAC is an appropriate group to bring the claim. The Respondent submits they are not.

A. FPAC was not directly affected and does not have a genuine interest in the validity of the legislation or the public action

21. FPAC's claim to have a genuine interest in the constitutionality of s. 400 is tenuous and insufficient to grant public interest standing. FPAC is a general privacy advocacy, research and awareness organization with no special relationship to any directly affected parties or the issues before the court. Public interest standing requires a substantial

connection with the claim, such as in *SWUAV*, where the group seeking public interest standing was composed of directly or formerly directly affected members of the community it sought to represent. The community in that case was a substantially more homogenous group. Here, FPAC seeks to represent *all* of the affected individuals, who have in common only their location on a specific day and their use of mobile devices.

SWUAV, *supra* para 17 at para 5.

22. Metadata, by its very definition, covers a vast population whose only unifying feature is their use of mobile phones, which in today's society is almost ubiquitous. Unlike *SWUAV*, we have no guarantee that the appellants here will be able to provide the court with an understanding of the impact of any alleged privacy violation on individuals across Flavelle. FPAC's engagement so far has been largely academic. There is a significant difference between the expertise necessary to provide legislative testimony or to act as an intervener and the deep knowledge and factual context given by directly affected litigants.

23. This case is different from past cases in which public interest standing has been used to empower directly affected groups. *SWUAV* allowed standing for a group that had a deep connection with a small community and long term continuing interest in the outcome of the case. In *Chaoulli v Quebec (Attorney General)*, a doctor and patient were granted public interest standing based on their personal experiences with the public health care system, which gave them a genuine interest in the claim. FPAC has not been affected by the alleged search in the same manner.

SWUAV, *supra* para 16 at para 5.

2005 SCC 35, [2005] 1 SCR 791 at para 35 [*Chaoulli*].

B. FPAC's proposed suit is not a reasonable or effective way to bring the issue before the courts

24. Almost as soon as information about "bulky surveillance" by the FNPA was leaked to the public, FPAC brought a claim as to the constitutionality of s. 400. This claim comes to the court with a sparse factual record and the court does not have the benefit of the result of the investigation. The court cannot make *Charter* decisions in a "factual vacuum" or "based upon the unsupported hypothesis of enthusiastic counsel."

> *Mackay v Manitoba,* [1989] SCR 357, 61 DLR (4th) 385 at para 8.

25. Courts must take a "flexible, discretionary approach" to determining whether a proposed claim is a reasonable or effective way to bring a claim forward. In doing so, they must look to:

> a) whether the proposed action is an economical use of judicial resources;
>
> b) whether the issues are presented in a context suitable for judicial determination in an adversarial setting; and
>
> c) whether permitting the proposed action to go forward will serve the purpose of upholding the principle of legality.
>
> *SWUAV, supra* para 16 at para 1, 50.

26. Though the applicant is not *required* to show that the measure will not be subject to attack by a private litigant, "[a]ll of the other relevant considerations being equal, a party with standing as of right will generally be preferred." Some groups, such as airline employees, business travellers and airport staff, regularly attend the Austin Airport – some, on a daily basis – and could reasonably have known that their data had been captured by the alleged search. These directly impacted groups have not yet brought a

challenge but face no practical impediment to doing so. Duplicative challenges are not economical uses of judicial resources.

SWUAV, supra para 16 at para 37.

27. There is no barrier preventing these groups from bringing a claim. In fact, Justice Neil in the Court of Appeal noted that they are well placed to bring a claim. In contrast, the affected populations in *SWUAV* or *Chaoulli* were incredibly vulnerable and practically unable to bring a claim. In *Chaoulli,* Binnie and Lebel JJ wrote that it would be "unreasonable to expect a seriously ailing person to bring a systematic challenge".

SWUAV, supra para 16 at para 71.
Chaoulli, supra 20 at para 189.

28. Granting FPAC public interest standing fulfills none of the purposes of standing. The provisions are not immune from challenge without FPAC's claim. Further, the claim FPAC is bringing is not different from the claim a directly affected individual or group would bring. It does not have a "distinctive and important interest different from" more directly affected groups. It does not seek, as in *SWUAV,* to challenge "nearly the entire legislative scheme" while a directly affected party would only challenge parts. A directly affected party bringing the challenge would make the same claims that FPAC makes.

SWUAV, supra para 16 at para 64, 68.

Issue 2: There is no reasonable expectation of privacy over tracking data

29. The rise of the Internet age forced our society, and hence the courts, to confront new and pressing issues regarding privacy. Yet the fundamental principles that ground the protection of an individual's privacy have not changed. As affirmed recently in *R v Spencer*, "the protection of privacy is a prerequisite to individual security, self-fulfillment and autonomy as well as to the maintenance of a thriving democratic society."

> *R v Spencer*, 2014 SCC 43, [2014] SCJ No 43 at para 15 [*Spencer*].

30. There is no reasonable expectation of privacy over historical tracking data. A reasonable expectation of privacy depends on a number of factors summarized in *Spencer*, namely:

> a) the subject matter of the alleged search;
>
> b) the claimant's interest in the subject matter;
>
> c) the claimant's subjective expectation of privacy in the subject matter; and
>
> d) whether this subjective expectation of privacy was objectively reasonable, having regard to the totality of the circumstances
>
> *Spencer*, *supra* para 26 at para 18.

31. The requested tracking information does not touch on the biographical core of personal information, both because it is anonymous and because, even if it were not, it does not provide any significant details about the individual. A citizen's interest in the tracking data is minimal: it provides information about a cellular device's location, not an individual's. Individuals' subjective expectation of privacy over this information is minimal: the public can glean more detailed information by choosing to track a publicly

available IP address. Further, individuals are unlikely to have an expectation of privacy over information that is only "viewed" by machine.

A. The subject matter of tracking data does not touch on the "biographical core" of personal information

i. The threshold of privacy has not been crossed

32. The privacy interest protected by s. 8 is based on "the assumption that all information about a person is in a fundamental way his own, for him to communicate or retain… as he sees fit." The "search" in this case did not provide information "about a person" because the information was anonymous and the vast majority of the information was never reviewed by a conscious being.

> *R v Tessling*, 2004 SCC 67, [2004] 3 SCR 432 at para 23 quoting A.F. Westin, *Privacy and Freedom* (1970), [*Tessling*].

33. The subject matter of the alleged search is tracking data that does not identify the person producing it. To match an individual as the owner of the cell phone number produced by Hammerstein, the police would have to obtain an additional production order on reasonable and probable grounds. The metadata collected cannot "include information which tends to reveal intimate details of the lifestyle and personal choices of the individual" when by its very nature it is anonymous. A person's interest in their online privacy is fundamentally linked to the state being able to "link particular kinds of information to identifiable individuals".

> *R v Plant*, [1993] 3 SCR 281, [1993] WWR 287 [*Plant*].
>
> *Spencer, supra* para 26 at para 47.

ii. The tracking data does not touch on the "biographical core"

34. Even if anonymity did not prevent this information from touching on the "biographical core," the information is so general and non-descript that it cannot provide intimate details of an individual's life. Tracking data may provide details about the device's location, but, as Justice Keith found, it does not provide any information regarding who was in possession of the cell phone at that time or what they were doing at a particular location. Similar to cases involving electricity consumption, the tracking data provided does not give access to the user's personal information. It is not certain who is using the cell phone at the time the tracking data is collected or even the device's exact location. Though many people have personal cell phones that are not shared, many organizations have cell phones that are shared amongst employees. Families may share cell phones between family members. Other individuals may use multiple cell phones throughout the course of a day. A cell phone number may be changed and a new person may be associated with that tracking data. Police cannot know whether the tracking data associated with any particular device provides an accurate map of a specific individual's movements. That device may be shared or it may not be the only device an individual uses.

    R v Gomboc, 2010 SCC 55, [2010] 3 SCR 211 at para 43 [*Gomboc*].

    Plant, supra para 30.

35. The trial judge wrote that "[m]etadata may give insight to an individual's medical status, political inclinations, personal and family relationships and professional ambitions." However, it is difficult to see how these details could be gleaned from the high level information contained in tracking data. Tracking data does not provide the intimate,

nuanced details about a person that comes, for instance, from an IP address. An IP address provides detailed information about an individual's preferences and engagement with the Internet, including internet search history. Anonymous IP address information is thus far more detailed than tracking data. Despite this, IP address activity is publically viewable. For example, any member of the public can view IP addresses associated with file sharing on services such as Limewire. By contrast, tracking data is only specific to a radius of 50 meters. In many cases, a radius that wide would not allow the police to conclude in which house, business or building the device was located.

Spencer, *supra* para 26 at para 8.

B. There is no significant interest over metadata

36. An individual's informational privacy interest is not engaged by the collection of tracking data. The information cannot give rise to a "strong, immediate and direct inference" about an individual. Tracking data only provides information about the movements of a device – making it much less conclusive than the reading from a DRA or a search by a sniffer dog, both of which provide almost conclusive evidence of criminal activity. There are many steps needed to turn the raw data into anything resembling an inference. First, one would need to identify the coordinates provided by the metadata and transfer them to real world maps to identify landmarks within that 50 meter radius. GPS coordinates 43 N and 79 W could be a strip club or it could be a fast food shop – with only that data, it is impossible to know. From there it would be necessary to run searches to evaluate patterns over time – searches which may exclude the vast majority of data. Then, to match the tracking data to an individual, law enforcement would require further judicial authorization on reasonable and probable groups, pursuant to *R v Spencer*.

Gomboc, supra para 32 at para 8.

Plant, supra para 30.

R v Kang-Brown, 2008 SCC 18, [2008] 1 SCR 456 at para 38 [*Kang-Brown*].

37. The fact that information is *collected* digitally does not fundamentally alter its character. Metadata is in the same class of information as police can gain from surveillance, as found by Justice Keith. In effect, tracking data is merely an online version of the "situational landscape" that Justice La Forest describes in *R v Wise*. It is a digitized version of public space, where police can observe anonymous individuals and filter out those who pose a threat to public safety. There is no significant interest over this kind of information.

> *R v Wise*, [1992] 1 SCR 527, [1992] SCJ No 16, quoting M. Gitterman, "A Formulation of the Value and Means Models of the Fourth Amendment in the Age of Technologically Enhanced Surveillance" (1988), 39 *Syacuse L. Rev*. 647 [*Wise*].

C. Any subjective expectation of privacy is not objectively reasonable

38. Though some individuals may assert a subjective expectation of privacy over tracking data, that expectation is not objectively reasonable or widespread in the Flavellian population. The typical behavior of internet users and cell phone users demonstrates that they are not concerned about the information that can be attached to a unique identification number.

39. The information gathered was not viewed by any law enforcement personnel, or, indeed, any person *at all*. Much like the countless machines and programs that review this information as it is transmitted via the Internet, the FNPA's computer did not have any distinct awareness of the information. Privacy is important to protect individuals from

other conscious beings, not from a computer program that reviews the data in terms of 0's and 1's, only flagging information within its prescribed set of conditions. Insofar as no human was ever to review the vast majority of this information, the alleged search is not nearly as broad as FPAC claims. Indeed, metadata analysis is arguably not a search at all if conducted solely by a machine.

40. Defining what has actually been "searched" is very different for digital rather than physical spaces. An individual's s. 8 rights are not violated when an inanimate object "reads" private information. It is only when data is exposed to *human* observation that privacy concerns take on an air of reality. Orin S. Kerr provides an apt illustration of this principle: "a text query that searches only for the word "assassination" anywhere on a hard drive may be broad at a physical level – the entire hard drive must be scanned – but its invasion of privacy is fairly slight. In contrast, obtaining a copy of a target's diary from a known position on the hard drive may be narrow at a physical level but amounts to a tremendous invasion of privacy." The alleged "search" on these facts may have not provided *any* results. In that case, no police officer would ever have viewed the data. FPAC's premature claim deprives the court of the factual record to decide this issue.

> Kerr, Orin S. "Searches and Seizures in a Digital World" (2005) 119 Harv L Rev 531.

41. These sort of identifiers are shared by individuals through their IP addresses, cookies and various other methods, leaving a trail of personal information "breadcrumbs" around the internet for any member of the public to view. Police can already view internet searches, websites visited, and downloads by a specific IP address without a warrant. That power does not prevent individuals from using the internet, just as the knowledge that they *may*

be observed in public does not ordinarily deter individuals from leaving their homes. Tracking data is much the same. The information gleaned about an individual is insufficient to significantly impact their day-to-day lives. Individuals do not have an expectation of privacy over this information.

42. Finally, the contract with Hammerstein clearly lays out that Hammerstein can collect information. Terms in contracts are "highly significant" in determining an individual's reasonable expectation of privacy. Though disclosure to the police may not have been explicitly communicated, the information was already shared with the company – diminishing any expectation of privacy.

Gomboc, supra para 32 at para 31.

Issue 3: If there was a reasonable expectation of privacy, any search was reasonable and therefore compliant with s. 8 of the Charter

43. If there was a reasonable expectation of privacy in the metadata at issue, the search was reasonable and therefore compliant with s. 8 of the *Charter*.

44. Per *Collins*, a search is reasonable if:

a) it is authorized by law

b) the law itself is reasonable; and

c) the search was conducted in a reasonable manner.

R v Collins, [1987] 1 SCR 265, 38 DLR (4th) 508 at para 23 [*Collins*].

45. The Appellant submits that s. 400 is unreasonable because it authorizes metadata collection based on a standard of "reasonable suspicion" instead of "reasonable and

probable grounds". The Appellant also submits, in the alternative, that the search in this case was not authorized by s. 400. The Respondent disagrees on both points and submits that the decision of the Court of Appeal ought to be upheld.

A. S. 400 of the *Criminal Code* is a Reasonable Authorizing Law

i. The "Reasonable Suspicion" Standard in s. 400 is Appropriate.

46. First, the law itself is reasonable because the standard of reasonable suspicion is a constitutionally acceptable standard for an order authorizing bulk metadata collection. *Hunter v Southam* set out reasonable and probable grounds as the *default* standard on which searches and seizures ought to be authorized. However, the Court has held less stringent standards – including reasonable suspicion – to be constitutionally compliant in some circumstances.

> *Hunter v Southam,* [1984] 2 SCR 145, 11 DLR (4th) 641 at para 43.

47. This case is analogous to past cases in which the reasonable suspicion standard was held to comply with s. 8. In *Kang-Brown*, the Court held that police sniffer dog searches could be conducted based on reasonable suspicion without prior judicial authorization. Binnie J took a nuanced and pragmatic approach, holding that the standard had to be calibrated to the nature of the technique. Requiring reasonable and probable grounds would render sniffer dogs, as an investigative tool, "superfluous and unnecessary". Reasonable suspicion could strike an appropriate balance between the "legitimate needs of law enforcement" and the privacy interests of citizens. In the case of sniffer dogs, this balance was achieved because the technique was "minimally intrusive, narrowly targeted and [highly accurate]".

> *Kang-Brown, supra* para 34 at paras 21, 24, 60.

48. The Court struck a similar balance in permitting a lower standard of justification at border crossings in *Simmons*, for "bedpan vigils" in *Monney*, and for searches by school officials in *M(M.R.)*. In these cases, the Court emphasized that a diminished expectation of privacy, coupled with the exigencies of law enforcement and public safety, could justify a lower but still constitutionally compliant standard of reasonable suspicion. In this case, if there is an expectation of privacy in metadata, it is a lesser expectation than in the *content* of communications. By contrast, there are significant, exigent challenges posed to law enforcement by criminals using modern communications technology.

R v Simmons, [1988] 2 SCR 495, 55 DLR (4th) 673 at para 52.
R v Monney, [1999] 1 SCR 652, 171 DLR (4th) 1 at para 48.
R v M(M.R.), [1998] 3 SCR 393, 166 DLR (4th) 261 at para 47, 48.

49. As new investigative techniques have become available, and as technology has advanced, the Court has shown willingness to adapt the s. 8 analysis to new realities. *Hunter v Southam* was decided 30 years ago, at a time when the bulk analysis of anonymous metadata by computers could not have been within the contemplation of the Court. S. 400 represents Parliament's attempt to harness this new and innovative investigative technique to apprehend dangerous criminals while still respecting the autonomy and dignity interests of Flavellians.

50. An order for bulk collection of metadata based on reasonable suspicion allows the police to use computer technology to discern patterns from otherwise decontextualized information. These patterns can then be used to establish reasonable and probable grounds for an order to obtain subscriber information. This is analogous to a case where reasonable suspicion authorizes a sniffer dog search, and a positive match by the sniffer

dog then enables the police to arrest and search the suspect. In both cases, reasonable suspicion is a permissible standard because the information gleaned from the search is inherently limited, and only upon reasonable and probable grounds can that information be contextualized through a more invasive search. However, it should be noted that in contrast to this case, the Court in *Kang-Brown* permitted a lower standard of suspicion in the absence of prior judicial authorization.

Kang-Brown, supra para 34 at para 22.

51. As in *Kang-Brown*, requiring reasonable and probable grounds to obtain anonymous metadata would make this technique functionally useless in many circumstances. At the point where the police have reasonable and probable grounds for a search of any particular individual, they would have no need for metadata. They could simply apply for a warrant consistent with *Spencer* for the production of subscriber information, or indeed for the *content* of their communications.

ii. The Prior Judicial Authorization Requirement of s. 400 is an Adequate Safeguard

52. The Appellant relies on the concern articulated by the trial judge that s. 400 permits collecting the metadata of potentially thousands of individuals. The Crown does not dispute this. Per *R v Chehil,* difference between reasonable suspicion and reasonable and probable grounds is the difference between *possibility* and *probability*. Here, the Crown need only establish the possibility, not the probability, that each search will assist the investigation. However, any concern regarding the search of unnecessary numbers of people is remedied by the fact that s. 400 requires prior judicial authorization. As in the case at bar, the police must justify the scope of their request for metadata to a judicial

officer. The text of s. 400 states that the justice "may" – as opposed to "shall" –authorize the request if he or she is satisfied that the police have met the standards set out in the provision. Therefore, it is open to the authorizing justice to either reject an overbroad request or to craft a more narrow production order consistent with the scope of reasonable suspicion supported by the evidence. Our criminal justice system relies heavily on, and places great trust in, the diligence and professionalism of trial judges in restraining police conduct.

R v Chehil, 2013 SCC 49, [2013] 3 SCR 220 at para 27 [*Chehil*].

53. The prior judicial authorization requirement in s. 400 safeguards the public interest and helps guarantee that intrusions into privacy are proportionate. In the words of Cromwell J in *R v Vu*, "[t]he prior authorization requirement ensures that, before a search is conducted, a judicial officer is satisfied that the public's interest in being left alone by government must give way to the government's interest in intruding on the individual's privacy in order to advance the goals of law enforcement".

R v Vu, 2013 SCC 60, [2013] 3 SCR 657 at para 22 [*Vu*].

54. Direct notice to affected individuals is not a necessary safeguard in all cases. The Appellant relies on the Supreme Court's decision in *R v Tse* for the proposition that the absence of an "after the fact" notification requirement in the text of s. 400 is fatal to its constitutionality. However, that case dealt with an emergency intercept provision of the *Criminal Code* that *did not* require prior judicial authorization. The Court in *Tse* was concerned about the lack of *any* appropriate safeguards or checks on police conduct. However, the Court explicitly did not hold that after-the-fact notice was a constitutional necessity. In the words of Moldaver and Karakatsanis JJ, "After-the-fact notice … is one

way of correcting [accountability concerns]; it may not be the only one. Other effective means are no doubt open to Parliament." In this case, Parliament has opted for the more direct form of accountability offered by prior judicial authorization.

R v Tse, 2012 SCC 16, [2012] 1 SCR 531 at para 86.

B. The Search Was Authorized By s.400

55. The Appellant submits that the search was unreasonable because the evidence in this case did not provide a sufficient basis for the scope of the production order. As a result, they argue that the trial judge erred in authorizing the production order. In the Appellant's view, the authorities did not meet the standard of reasonable suspicion required by s. 400. They argue that because thousands of individuals' data was captured by the order, there cannot have been adequate basis for reasonable suspicion on all of them. However, the Appellant's submissions misapprehend the standard of reasonable suspicion. The Court has emphasized that such standards are flexible and context-dependent. The Appellant is correct that, in the words of Karakatsanis J in *Chehil,* **"**the objective facts must be indicative of the possibility of criminal behaviour". But the facts need not support the *probability* that each individual whose data is collected will be involved in criminality, only the *possibility*. Further, the Court in *Chehil* explicitly rejected the notion that "the evidence must itself consist of unlawful behaviour, or must necessarily be evidence of a specific known criminal act."

Chehil, supra para 49 at para 35.

C. The Search Was Conducted Reasonably

56. In this case, the search was authorized by a prior judicial order and the police complied with the scope of the order. Therefore, the onus is on the claimants to demonstrate unreasonableness.

57. Although the Appellants appear to have abandoned this argument in this court, the trial judge held that the search was overly-broad. The Respondent agrees with the Court of Appeal's decision to overturn that holding. In this case, the authorities identified one time and one place Victorious was known to have been. They used this as the suspicion basis for obtaining an order to collect metadata. The order was limited in scope. It only covered people who travelled through one location (Austin Airport) on one day (August 15, 2013). Access to the metadata was heavily limited by the approach taken by the police. The data was not to be analysed by a human being until after a computer sorted it. At no point would the substance, meaning or content of any communications be collected.

58. The search was also limited to metadata about past communications; it was not a warrant for ongoing wiretapping or production. Unlike in *R v Telus Communications*, the state was not engaging in ongoing surveillance directed at an undefined number of people. The parameters of the search, although characterized by the Appellant as wide, were temporally limited and precisely defined.

R v Telus Communications, 2013 SCC 16, [2013] 2 SCR 3 at para 13.

59. In sum, the police crafted the narrowest request possible to achieve their objective of apprehending Victorius. They waited until they had judicial endorsement of that request. Once the metadata was in their possession, they proceeded to handle it in a responsible

way. They minimized the degree to which any private information might be examined or analysed by human beings, winnowing the scope of the information down through computer analysis. It is notable that the claimants in this case have provided no credible example of a way in which the police could have narrowed their approach without abandoning this line of investigation entirely. The appellants base their submissions entirely on hypothetical examples that have no relation to the facts of this case. The Supreme Court has repeatedly made clear that *Charter* issues must not be evaluated in a "factual vacuum".

MacKay v Manitoba, *supra* para 24 at para 8.

Issue 4: If there was a breach of s. 8, s. 400 of the Criminal Code can nevertheless be upheld pursuant to s.1 of the Charter

60. If this Court finds that s. 400 infringes s. 8 of the *Charter,* the provisions can be saved under s. 1 of the *Charter*. The law is rationally connected to the pressing and substantial objective of providing law enforcement with the necessary tools to meet the realities of crime in the internet age. The law is proportionate to any alleged limitation on s. 8 rights. But before conducting a full *Oakes* analysis, it is necessary to make several comments regarding the proper analytical approach to s. 1 analysis in the s. 8 context.

A. The Proper Analytical Approach to s. 1 in the s. 8 Context

61. At first glance, it might appear that an "unreasonable" law for the purposes of s. 8 cannot be considered a "reasonable limit prescribed by law" for the purposes of s. 1. In order for s. 1 to come in to play, a court would already have to have found that a search or seizure was unreasonable. In particular, a court would have to have found either that (a) the

search was not authorized by law or (b) the law authorizing the search was unreasonable. However, both the facts of this case and recent Supreme Court jurisprudence suggest that any violation of section 8 found in this case can be justified under section 1.

62. However, the Supreme Court's decision in *Bedford* suggests that s.1 remains available to justify limitations on *all* rights enumerated in the *Charter.* The mere fact that rights such as those guaranteed by ss.7 and 8 have internal limitations does not preclude the possibility of s.1 justification. In *Bedford,* the Court clarified that the proportionality analysis undertaken in determining whether there has been a breach of s.7 is crucially different from the proportionality analysis conducted under *Oakes*. In general terms, "[t]he question of justification on the basis of an overarching public goal is at the heart of s. 1 , but it plays no part in the s. 7 analysis, which is concerned with the narrower question of whether the impugned law infringes individual rights."

> *Canada (Attorney General) v Bedford*, 2013 SCC 72, [2013] 3 SCR 1101 at para 125 [*Bedford*].

63. More specifically, in determining whether there has been a s. 7 infringement, the Court pronounced that the internal limitations analysis functions differently from the *Oakes* proportionality test:

> "[U]nder s. 7 …[t]he inquiry into the purpose of the law focuses on the nature of the object, not on its efficacy. The inquiry into the impact on life, liberty or security of the person is not quantitative — for example, how many people are negatively impacted — but qualitative. An arbitrary, overbroad, or grossly disproportionate impact on one person suffices to establish a breach of s. 7"
>
> *Bedford, supra* para 62 at para 127.

64. The same principle is readily applicable to s. 8. A search might be "unreasonable" with respect to the privacy interests of one individual and one particular investigation, but the authorizing law might nevertheless be proportionate to a broader public goal of pressing and substantial importance. A law might be unreasonable under a "qualitative" s.8 analysis, but nevertheless be justified under a "quantitative" *Oakes* analysis. In concrete terms, this means that under an s.1 analysis, the Court can give greater weight to the empirical significance of the state's objective. It also means that the Court is more capable of weighing the salutary effects of the law against its deleterious consequences. The case at bar is one where any s. 8 violation can be saved under this type of s. 1 analysis. This will also be one of the first opportunities for this Court to fully apply the s. 1 analysis to an s.8 infringement, given that the overwhelming majority of such infringements are handled under s. 24(2).

B. Application of *Oakes*

65. Per *Oakes*, an otherwise *Charter* infringing law can be considered a reasonable limit under s. 1 where the state establishes:

> (i) a pressing and substantial objective;
>
> (ii) a rational connection between the objective and the impugned law; and
>
> (iii) proportionality, both in the sense that the law minimally impairs *Charter* rights in achieving its objectives and in the sense that the salutary effects of the law outweigh its deleterious consequences
>
> *R v Oakes,* [1986] 1 SCR 103, 26 DLR (4th) 200 at para 70.

i. The Objective of the Law is Pressing and Substantial

66. The objective of the law is clearly pressing and substantial. The Courts below were in unanimous agreement on this subject. As held by the Court of Appeal, the state has a

pressing and substantial interest in adopting new investigative techniques that adapt to modern criminality within a "high-tech environment". It has become increasingly necessary to use sophisticated techniques such as metadata analysis to combat equally sophisticated and organized criminals.

67. Indeed, the investigation that precipitated the present *Charter* challenge provides a compelling example of this reality. The public was put in significant danger by the "Carnegie" firearms smuggling operations. Traditional investigative techniques failed to suffice in apprehending Victorius. S/he ran a modular and decentralized criminal organization by taking advantage of modern technology. An innovative, technologically sophisticated response was required.

ii. The Law is Rationally Connected to its Objective

68. There is a clear rational connection between this objective and s. 400 of the *Criminal Code*. By allowing a judge to authorize the bulk collection of metadata based on reasonable suspicion, s. 400 permits the authorities to use novel and targeted investigative techniques, such as bulk computer metadata analysis, to apprehend dangerous criminals such as Victorius.

69. The main point of disagreement in this case is whether the alleged infringement of s. 8 is proportionate to the objective of the legislation. Before engaging in the proportionality analysis, it is important to note that attaining the right balance between security and privacy in the internet age is challenging and complex. Parliament is called upon to balance competing interests. On the one hand, Parliament must respect the clear interest that Flavellians have in protecting informational privacy as greater portions of their lives

are lived online. On the other hand, Parliament must also tackle the ever-increasing harm that can be done to citizens by crimes perpetrated through, or facilitated by, the use of modern communications technology. Parliament must do this despite the fact that such crimes are becoming increasingly difficult to investigate or even detect. Given the complexity of achieving such a balance, the Court ought not overturn the considered decisions of democratically elected representatives lightly. As Chief Justice McLachlin wrote in *Alberta v Hutterian Bretheren*, "[t]he bar of constitutionality must not be set so high that responsible, creative solutions to difficult problems would be threatened. A degree of deference is therefore appropriate".

> *Alberta v Hutterian Brethren of Wilson Colony,* 2009 SCC 37, [2009] 2 SCR 567 at para 37.

iii. The Law is Minimally Impairing

70. The majority in the Court of Appeal correctly found that s. 400 was proportionate to the legislative objective. A warrant based on "reasonable suspicion" strikes the right balance between facilitating police investigation of crimes on the one hand and the need to have checks and balances on police conduct on the other.

71. The majority in the Court of Appeal also correctly held that "a more onerous standard would not allow the police to take preventive measures to stop crimes before they occur." The case at bar provides, once again, a clear example of this principle. If reasonable and probable grounds were necessary, the police would never have been able to the conduct anonymous bulk metadata analysis necessary to find Victorius' telephone number. Without such an analysis, they would never have had enough evidence to apply for a warrant on reasonable and probable grounds to obtain her/his subscriber information.

Unable to capture the leader of the organization, the police would be limited to investigating the smuggling of illegal weapons into the country after the fact, coping reactively with the violent crimes such weapons facilitate instead of addressing the root cause.

72. In contrast to the well-reasoned decision of the Court of Appeal, the trial judge committed a number of errors in reasoning when she held that the law was disproportionate to its objective. Her primary concerns related to the potential for abuse and a lack of clarity about the circumstances in which these powers might be used.

73. The trial judge articulated these concerns despite the applicants being unable to point to any actual case of abuse. There is no evidence on the record of any improper police conduct whatsoever. Moreover, the trial judge failed to consider the fact that s. 400 requires the authorities to receive prior judicial authorization in order to collect metadata. Therefore, her concern that s. 400 could be used "in a manner that is wholly unrelated to any clear objective" is unfounded. Where the objective of the police in obtaining metadata is improper, the justice hearing the application is obligated to reject it.

74. In any event, the mere *potential* for abusive and improper application of a legislative enactment is not, on its own, grounds for invalidating legislation. As Binnie J held in *Little Sisters,* 'Parliament is entitled to proceed on the basis that its enactments "will be applied constitutionally" by the public service.' It is not enough for the applicants in this case merely to raise the unsubstantiated spectre of improper police conduct to prove that the legislation fails the proportionality stage of the *Oakes* test.

> *Little Sisters Book and Art Emporium v Canada (Minister of Justice),* 2000 SCC 69, [2000] 2 SCR 1120 at para 71.

75. In fact, the law is narrowly tailored. If the law does infringe the s. 8 rights of Flavellians, it does so as little as possible while still achieving the objective of allowing the new technique of metadata analysis to be used effectively to combat crime. s. 400 does not allow the police to access the *content* of communications. It does not allow police to obtain subscriber information without a warrant on reasonable probable grounds. It does not allow the police to obtain any data whatsoever without a judicial authorization. At the same time, a more stringent standard, such as reasonable and probable grounds, would make the technique of metadata analysis functionally useless in many situations, just as a such a requirement would have made the sniffer dog searches in *Chehil* and *Kang-Brown* redundant.

iv. The Salutary Effects of the Law Outweigh Any Deleterious Consequences

76. Finally, the salutary effects of the law clearly outweigh any deleterious consequences. The law allows the police to use innovative techniques to protect the physical safety of Canadians by putting dangerous criminals, like Victorius, behind bars. At the same time, any privacy infringements are minimal. Most, if not all, metadata is innocuous and reveals little about the individual's "biographical core". Where any genuinely private information is collected, it is anonymous and not connected to a name or address. Given the "bulk" nature of such data analysis, any information collected is also unlikely to ever be viewed by a human being. As such, any harm to citizens' privacy interests is remote and *de minimis*.

> *Dagenais v Canadian Broadcasting Corp.,* [1994] 3 SCR 835, 120 DLR (4th) 12 at para 88.

PART V – ORDER SOUGHT

77. The Respondent seeks an order that the appeal be denied and the costs be awarded against the Appellant in this Court and in both courts below.

ALL OF WHICH IS RESPECTFULLY SUBMITTED

Signed this 18th day of September 2014.

_____

Counsel for the Respondent

SCHEDULE A – TABLE OF AUTHORITIES

i. Case Law

Case Law	Paragraph
Alberta v Hutterian Brethren of Wilson Colony, 2009 SCC 37, [2009] 2 SCR 567	**69**
Canadian Council of Churches v Canada (Minister of Employment and Immigration), [1992] 1 SCR 236, 88 DLR (4th) 193.	**16**
Canada (Attorney General) v Bedford, 2013 SCC 72, [2013] 3 SCR 1101.	**62, 63**
Canada (Attorney General) v Downtown Eastside Sex Workers United Against Violence Society, 2012 SCC 45, [2012] 2 SCR 524.	**17, 18, 19, 20, 23, 25, 26, 27, 28**
Chaoulli v Quebec (Attorney General), 2005 SCC 35, [2005] 1 SCR 791.	**23, 27**
Dagenais v Canadian Broadcasting Corp, [1994] 3 SCR 835, 120 DLR (4th) 12.	**76**
Hunter et al v Southam Inc, [1984] 2 SCR 145, 11 DLR (4th) 641.	**46**
Little Sisters Book and Art Emporium v Canada (Minister of Justice), 2000 SCC 69, [2000] 2 SCR 1120.	**74**
Mackay v Manitoba, [1989] SCR 357, 61 DLR (4th) 385.	**24, 59**
R v Chehil, 2013 SCC 39, [2013] 3 SCR 220.	**52, 55, 74**
R v Collins, [1987] 1 SCR 265, 38 DLR (4th) 508.	**44**

Case Law	**Paragraph**
R v Gomboc, 2010 SCC 55, [2010] 3 SCR 211.	**34, 36, 42**
R v Kang-Brown, 2008 SCC 18, [2008] 1 SCR 456.	**36, 47, 50**
R v M. (MR), [1998] 3 SCR 393, 166 DLR (4th) 261.	**48**
R v Monney, [1999] 1 SCR 652, 171 DLR (4th) 1.	**48**
R v Oakes, [1986] 1 SCR 103, 26 DLR (4th) 200.	**65**
R v Plant, [1993] 3 SCR 281, [1993] WWR 287.	**33, 34, 36,**
R v Simmons, [1988] 2 SCR 495, 55 DLR (4th) 673.	**48, 57**
R v Spencer, 2014 SCC 43, [2014] SCJ No 43.	**29, 30, 33, 35,**
R v Telus Communications, 2013 SCC 16, [2013] 2 SCR 3.	**58**
*R v Tessling***,** 2004 SCC 67, [2004] 3 SCR 432.	**32**
R v Tse, 2012 SCC 16, [2012] 1 SCR 531.	**54**
R v Vu, 2013 SCC 60, [2013] 3 SCR 657.	**54**
R v Wise, [1992] 1 SCR 527, [1992] SCJ No 16.	**37**

ii. Secondary Sources

Secondary Sources	Paragraph
Kerr, Orin S. "Searches and Seizures in a Digital World" (2005) 119 Harv L Rev 531.	**40**

SCHEDULE B – STATUTES

***Canadian Charter of Rights and Freedoms*, Part I of the Constitution Act, 1982, being Schedule B to the Canada Act 1982 (UK), 1982, c 11.**

Rights and freedoms in Canada

1. The *Canadian Charter of Rights and Freedoms* guarantees the rights and freedoms set out in it subject only to such reasonable limits prescribed by law as can be demonstrably justified in a free and democratic society.

Search or seizure

8. Everyone has the right to be secure against unreasonable search or seizure

Flavelle *Criminal Code*

400 (1) On ex parte application made by a peace officer or public officer, a justice or judge may order a person to prepare and produce a document containing tracking data that is in their possession or control when they receive the order.

400 (2) Before making the order, the justice or judge must be satisfied by information on oath that there are reasonable grounds to suspect that

a. An offence has been or will be committed under this or any other Act of Parliament; and
b. The tracking data is in the person's possession or control and will assist in the investigation of the offence.