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 APPELLANT

TABLE OF CONTENTS

PART I – OVERVIEW

1. Section 400 of the *Criminal Code* violates the constitutional right of Flavellians to freedom from unreasonable search and seizure. In an attempt to locate the leader of a criminal organization, three months of metadata from the cellphones of 20,000 individuals was collected and analyzed. Parliament is entitled to empower the police to use new investigative techniques, but s. 8 of the *Charter* demands that any expansion of police investigative powers meet the minimum constitutional standards for privacy protection.
2. The Court of Appeal and Trial Court were correct in establishing that the Flavelle Privacy Advocacy Centre has standing to bring this claim. Private claimants in this case were unaware that their metadata was collected and were unable to bring a claim.
3. Flavellians have a reasonable expectation that the government will not use their cellphones as tracking devices. Tracking data from cell phones provides core personal information which individuals wish to keep out of the hands of the state. Section 400 permits the police to conduct unreasonably broad searches of highly personal data on the "suspicion" that data will "assist" in the investigation. Moreover, if s. 400 is constitutionally valid, it does not allow for blanket searches of months of data from thousands of phones.
4. The infringement of s. 8 cannot be saved by s. 1 of the *Charter*. The impugned provision is an overly broad and grossly disproportionate attempt by Parliament to expand police powers to make use of consumer communications technologies. Crime-fighting in the modern era does not require nor justify significant invasions into individual privacy.

PART II – STATEMENT OF FACTS

A. Factual Background

5. Between May and August of 2013, in an effort to combat a gun smuggling ring, the Flavelle National Policing Authority ("**FNPA**") focused their investigative efforts on a character known under the pseudonym of Victorius.

    Official Grand Moot Problem, para 5 [*Problem*].

6. The FNPA knew little about Victorius. They knew that he was responsible for co-ordinating between the satellite units of a de-centralized gun smuggling ring. They knew that Victorius travelled between the cities of Stern, Austin and Stewart on a regular schedule, spending seven days in each city. The FNPA received a tip that Victorius had passed through the Austin Airport on August 15, 2013. With some creative policing, this information was all that the FNPA needed to close in on Victorius.

    Problem, *supra* para 5 at para 6.

7. The FNPA successfully obtained cell phone tracking data collected and held by the telecommunications company Hammerstein Inc. ("**Hammerstein**") by applying for an order under section 400 of the *Criminal Code*. The FNPA collected the tracking data of every cell phone subscriber in range of the Hammerstein cell phone transmission tower servicing the Austin Airport on August 15, 2013. As a result, the tracking data of over 20,000 independent phone numbers was collected by the FNPA.

    Problem, *supra* para 5 at para 8.

8. The FNPA collected the tracking data of each of those 20,000 independent phone numbers for the period spanning from May 15, 2013 to August 15, 2013. The FNPA had access to the last three months of movements for every cell phone subscriber who passed

through the Austin airport on August 15.

Problem, *supra* para 5 at para 15.

9. The tracking data was collected by Hammerstein for the purpose of improving cell phone service and coverage. Hammerstein was permitted to collect the tracking data of its cell phone subscribers under its service contract. Under the service contract, Hammerstein was not permitted to disclose that information to third parties except in accordance with the relevant privacy statutes.

Problem, *supra* para 5 at para 12.

10. The FNPA sought to look through the tracking data of every phone number collected in order to find a phone number that could be matched to Victorius' travel schedule.

i. Tracking Data

11. Cell phone tracking data can be used to approximate the location of a cell phone. The data is collected by every transmission tower within range of a cell phone's reception. Tracking data discloses the direction of the cell phone from the transmission tower and strength of a cell phone's signal which can approximate distance.

12. In urban areas where there are multiple sophisticated transmission towers, tracking data can reliably reveal that a cell phone was somewhere within a 50 metre radius by triangulating between multiple transmission towers. As technology improves and investment in cell phone infrastructure increases, tracking data increases in accuracy.

Problem, *supra* para 5 para 17.

13. Smartphones such as iPhones, Blackberries or Android phones send a signal to a transmission tower every three minutes. Older cell phones may only send a signal when a

call or text message is sent or received. Some cell phones transmit tracking data even when they are turned off.

ii. The Public Outcry

14. On September 10, 2013, Constable Herty of the FNPA received the requested tracking data from Hammerstein.
15. On September 15, before the data was analyzed, information was leaked to the Austin Daily Mail that the FNPA had undertaken a "bulky" surveillance of Flavellian metadata.
16. The leak resulted in public outcry in the Flavellian media. Flavellians were deeply concerned that their government was 'spying' on them. Concerns were expressed that the government of Flavelle would disclose information to foreign security agencies such as the National Security Agency of the United States which had recently been the subject of a similar public outcry as a result of a metadata collection scheme.

    Problem, *supra* para 5 at para 17.

17. The FNPA refused to disclose the date, purpose or means of their surveillance to the public for fear of compromising their investigation. The public was only informed that the surveillance involved the metadata of their communications.

    Problem, *supra* para 5 at para 18.

iii. The Flavelle Privacy Advocacy Centre

18. The Flavelle Privacy Advocacy Centre ("**FPAC**") is a non-profit organization with a longstanding commitment to advocacy, research and awareness of privacy issues in Flavelle. Its members are individuals who are interested in ensuring that the government

is accountable for breaches of its citizens' privacy. Members include academics, lawyers, journalists, and philanthropists.

Problem, *supra* para 5 at para 20.

19. Recently FPAC has intervened in two cases involving alleged breaches of section 8 of the *Charter*. One involved an appeal to the Supreme Court of Flavelle involving the privacy interest held in internet subscriber information. Another involved the privacy interest individuals have in cell phones seized incident to arrest. FPAC has been actively involved in the legislative process by testifying before parliamentary and legislative committees. FPAC has also made representations before public inquiries. Additionally, FPAC holds public meetings and rallies, publishes articles and holds seminars for students and professionals.

Problem, *supra* para 5 at para 21.

B. Trial Judgment

20. At trial Bessemer J. held that s. 400 of the Flavelle *Criminal Code* was unconstitutional and infringed an individual's s. 8 right to be free from unreasonable search and seizure. In her reasons, Bessmeer J. found that metadata "is far from innocuous" and "the ability of law enforcement to track the location of citizens on such a broad scale and with such ease has chilling repercussions for personal liberties". Bessemer J. held that the legal standard for obtaining metadata, due to the private nature of the information, should be reasonable and probable grounds. Furthermore, s. 400 is unreasonable in scope both temporally and in the number of people it could affect. Finally, he found that s. 400 could not be saved under s. 1 of the *Charter* for lack of proportionality.

Problem, supra para 5 at paras 29-32

C. Court of Appeal Judgment

21. The Court of Appeal reversed the trial judgment, holding that s. 400 does not infringe s. 8 of the *Charter* because there is no reasonable expectation of privacy in tracking data. Keith J. found that tracking data does not touch the "biographical core" of individuals. Further, Keith J. wrote that the FNPA would require a warrant to identify the individuals whose cell phone data has been singled out and although subscriber information attaches a reasonable expectation of privacy, it would require a warrant obtained on reasonable and probable grounds. Finally, Keith J. commented that the "reasonable grounds to suspect" standard operates proportionally to its objective by imposing checks and balances while allowing law enforcement to conduct surveillance and therefore s. 400 could be saved under s. 1.

    Problem, supra para 5 at paras 28-31.

22. Justice Neal, in his concurrence, was the only justice to find that FPAC does not have standing to bring the claim. While he noted that FPAC has engaged in "notable work", he denied FPAC standing because private plaintiffs were more suitable to bring this claim.

    Problem, supra para 5 at paras 32-33.

PART III – ISSUES

23. There are four issues on appeal:

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

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

Issue 3: If so, were the search powers created by s. 400 "reasonable" and was the search itself "reasonable"?

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

PART IV – ARGUMENT

Issue 1: FPAC has public interest standing to pursue this action

24. Both courts below were correct in holding that FPAC has public interest standing in this action. This claim raises a serious justiciable issue in which FPAC has a genuine interest. This action is a reasonable and effective way to bring the issue before the courts.

A. The Modern Approach to Standing

25. The modern approach to standing was recently re-examined by the Supreme Court of Canada in *Downtown Eastside Sex Workers United Against Violence v Canada (Attorney General)* ["***SWUAV***"]. *SWUAV* further extended the "flexible, discretionary approach to public interest standing."

> *Canada (Attorney General) v Downtown Eastside Sex Workers United Against Violence Society,* 2012 SCC 45, [2012] 2 SCR 534 at para 1 [*SWUAV*]

26. The test for public interest standing first emerged in *Borowski v Canada (Minister of Justice)* as part of the 'Thorson Trilogy'. The test was refined in *Canadian Council of Churches v R* where the Supreme Court of Canada emphasized that the "applicable principles should be interpreted in a liberal and generous manner." The court summarized the test for standing as having three aspects:

> First, is there a serious issue raised as to the invalidity of legislation in question? Second, has it been established that the plaintiff is directly affected by the legislation or if not does the plaintiff have a genuine interest in its validity? Third, is there another reasonable and effective way to bring the issue before the court?
>
> *Thorson v Canada (Attorney General)*, [1975] 1 SCR 138, [1974] SCJ No 45. [*Thorson*].

Nova Scotia Board of Censors v McNeil, [1976] 2 SCR 265, 12 NSR (2d) 85. *Minister of Justice v Borowski*, [1981] 2 SCR 575, [1981] SCJ No 103 at para 56 [*Borowski*].

Canadian Council of Churches v R, [1992] 1 SCR 236, [1992] SCJ No 5 at paras 37, 56 [*Canadian Council*].

27. Following *SWUAV*, it is no longer necessary for a party seeking public interest standing to prove that there was no other reasonable and effective means for the action to be brought. Instead, the party seeking standing need only prove that its own action was one, of potentially many, reasonable and effective means of bringing the claim. The test for public interest standing was reformulated as:

> Whether the case raises a serious justiciable issue, whether the respondents have a real stake or a genuine interest in the issue(s) and the suit is a reasonable and effective means of bringing the issues before the courts in all of the circumstances.

SWUAV supra para 25 at para 53.

28. Flexibility and discretion are essential to standing. As Laskin J. noted in *Thorson*, public interest standing "is a matter particularly appropriate for the exercise of judicial discretion, relating as it does to the effectiveness of process." Cromwell J. in *SWUAV* also highlighted the importance of discretion when he stated that “the three factors should not be viewed as items on a checklist or as technical requirements”. Instead, the factors should be seen as interrelated considerations to be weighed cumulatively, not individually, and in light of their purposes.

Thorson supra para 26 at para 37.
Finlay v Canada (Minister of Finance), [1986] 2 SCR 607, [1986] SCJ No 73 at pp 634 and 635.
Canadian Council supra para 26 at para 36.
SWUAV supra para 25 at para 36.

29. The discretion of courts to permit or deny a party public interest standing must be attentive to the purposes underlying standing law.

SWUAV supra para 25 at para 1.

30. At the root of standing law is the need to strike a balance "between ensuring access to the courts and preserving judicial resources." Public interest standing is a vital instrument to ensure the rule of law. Questions of constitutionality should not be immunized from judicial review by denying standing on the basis that no singular party is reasonably able to bring suit. On the other hand, courts should be on guard against the abuse of public interest standing to permit marginal or redundant suits. A party seeking public interest standing must have a degree of familiarity and expertise with the issues to make them a competent party to advance a suit.

Canadian Council supra para 26 at para 35.
Thorson supra para 26 at para 39.

B. Application of the Test for Public Interest Standing

31. FPAC's claim satisfies the three-part test for public interest standing as set out in *SWUAV*:

i) This action raises a justiciable issue;

ii) FPAC has a genuine interest in the issues; and

iii) This action is a reasonable and effective means of resolving the issues

i. Serious Justiciable Issue

32. There is a low bar for whether a constitutional claim raises a serious issue as to the validity of the legislation. In *Canadian Council* a "wide-sweeping and somewhat

disjointed attack" containing allegations "so hypothetical in nature that it would be impossible for any court to make determination with regard to them" was found to raise a serious justiciable issue.

Canadian Council supra para 26 at para 38.

33. This claim raises a serious justiciable issue. The constitutionality of legislation which expands law enforcement's ability to penetrate the private sphere of citizens in the course of criminal investigations is a "substantial constitutional issue" and an "important one" that is "far from frivolous." The claim is a narrow and concentrated challenge to one provision in the *Criminal Code* on the basis of s. 8 of the *Charter*.

SWUAV supra para 25 at para 54.

ii. Genuine Interest

34. The court in *SWUAV* identified the "engagement" of the organization seeking standing as the primary factor to be assessed in finding a genuine interest. Engagement is measured by looking at the plaintiff's reputation, continuing interest, and link with the claim.

SWUAV supra para 25 at para 43.
Canadian Council supra para 26 at para 39.

35. FPAC is deeply engaged in privacy issues related to state surveillance and the collection of metadata. FPAC's membership is made up of academics, journalists and philanthropists. FPAC and its members have been involved in privacy matters for decades.

36. FPAC has intervened in two similar cases at the Supreme Court of Flavelle in the past year. Both cases involved balancing police powers and s. 8 privacy interests in light of

new technologies. FPAC's most recent intervention at the Supreme Court of Flavelle involved an alleged s.8 breach arising from the collection of internet subscriber information. FPAC's second most recent intervention at the Supreme Court of Flavelle involved an alleged s.8 breach in the search of a smart phone incident to arrest.

37. FPAC is closely involved in the legislative process as it relates to privacy. FPAC has frequently been asked to testify or present materials to parliamentary committees. FPAC made representations at a public inquiry that occurred following reports that the FNPA conducted mass surveillance.

iii. Reasonable and Effective Means

38. The reasonable and effective means portion of the test is not a "strict requirement" such that the plaintiff must show that there are no other reasonable means of bringing the claim. Rather, the third factor must be applied with a view to the purposes and flexibility which underlie public interest standing as a whole.

    SWUAV supra para 25 at paras 44 and 49.

39. The court in *SWUAV* identified a non-exhaustive list of factors that may be taken into account when assessing the third factor of the test. These factors include:

    i) whether the plaintiffs have capacity to bring the claim;
    ii) whether the plaintiffs' interests transcend those of the most directly affected;
    iii) whether the plaintiff acts on behalf of marginalized persons;
    iv) whether realistic alternatives are more efficient; and
    v) whether any private litigant has a direct and personal stake in the claim.

    SWUAV supra para 25 at para 51.

40. The relevant factors point towards granting FPAC public interest standing in this case.

41. FPAC has the capacity to bring this claim. The claim has been appealed on its merits to the highest court in Flavelle. FPAC has extensive and particular expertise on the matters at the heart of this claim.

42. FPAC acts on behalf of affected individuals who had no way of knowing that their data was collected by the police. The time and manner of the surveillance was not disclosed to the public. No private affected individual could have reasonably brought this claim.

43. This claim transcends private interests. Privacy issues under s.8 are especially appropriate for public interest standing. Privacy has long been recognized to involve the expectations and trust citizens collectively place in their government. The impugned legislation potentially impacts every citizen without their knowledge. The most insidious harm in this case was not felt by any private individual, but the polity.

> *R v Patrick*, 2009 SCC 17, [2009] 1 SCR 579 at para 14 [*Patrick*].
> *R v Gomboc*, 2010 SCC 55, [2010] 3 SCR 211 at para 34 [*Gomboc*].
> *R v Ward*, 2012 ONCA 660, [2012] OJ No 4587 at paras 81-85 [*Ward*].

44. FPAC is the most efficient party that can realistically bring this claim. Affected cell phone holders do not have unique insights into how the collection of tracking data violated their privacy. More than 20,000 people were directly affected by the impugned surveillance. FPAC is in a better position than any private individual to convey and defend the variety of interests affected. Affected cell phone users may have been closer to a cell phone transmission tower, but they are no more proximate to the interests and facts underlying this claim.

C. Conclusion on Standing

45. The discretion to allow public interest standing must be exercised flexibly and purposively. The state action at issue affected a large and unknowing body of citizens, none of whom have a unique interest or special expertise in the facts and issues at hand. FPAC is a long-standing and reputable organization with the expertise to represent the wide array of privacy interests implicated in this case. In these circumstances, FPAC should be granted public interest standing to bring this action.

Issue 2: The collection of tracking data constitutes a search under s.8 of the Charter

46. Under s. 8 of the *Charter*, "[e]veryone has the right to be secure against unreasonable search or seizure." The jurisprudence has long recognized the need for a purposive approach to interpreting s.8 that emphasizes the protection of privacy as a prerequisite to individual security, self-fulfillment and autonomy as well as to the maintenance of a thriving democratic society.

> *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 s. 8.
> *Hunter et al v Southam Inc, [1984] 2 SCR 145, 11 DLR (4th) 641* at pp 156-57 [*Hunter*].
> *R v Tessling*, 2004 SCC 67, [2004] 3 SCR 432 at paras 12-16 [*Tessling*].

47. There are two distinct questions which must be answered in any s. 8 challenge. The first is whether there was a reasonable expectation of privacy in the subject matter. The second is whether the search was an unreasonable intrusion on that right to privacy.

> *R v Edwards*, [1996] 1 SCR 128, [1996] SCJ No 11 at para 33.

48. By tracking the location of 20,000 Flavellian citizens over the course of three months, the respondent breached s. 8 of the Charter.

A. What constitutes a search

49. To determine whether a search has been conducted within the meaning of s.8 the court must look at whether, in the totality of the circumstances, cell phone holders had a reasonable expectation of privacy in the information provided to the police. If there was a reasonable expectation of privacy, then obtaining that information was a search.

R v Spencer, 2014 SCC 43, [2014] SCJ No 43 at para 17 [*Spencer*].

50. The "totality of circumstances" must be assessed by looking at a wide variety and number of factors. Courts have grouped these factors into four headings:

i) the subject matter of the alleged search;

ii) the claimant's interest in the subject matter;

iii) the claimant's subjective expectation of privacy in the subject matter; and

iv) whether the expectation of privacy was objectively reasonable.

Tessling supra para 46 at para 32.
Patrick supra para 43 at para 27.
Spencer supra para 49 at para 18.

i. The Subject Matter of the Search

51. Information that tends to reveal intimate details of lifestyle and personal choices attracts the protection of s. 8. Section 8 protects "a biographical core of personal information which individuals in a free and democratic society would wish to maintain and control from dissemination to the state."

R v Plant, [1993] 3 SCR 281, [1993] SCJ No 97 at p 293 [*Plant*].
Spencer supra para 49 at para 27.
R v Cole, 2012 SCC 53, [2012] 3 SCR 34 at paras 35, 45.

52. The subject matter of the search must be characterized by looking beyond the mundane information obtained and at what it could reveal about those to whom it pertains.

> *Spencer supra* para 49 at paras 25-26.
> *R v Trapp*, 2011 SKCA 143 [2011] SJ No 728, *per* Cameron JA, at paras 33-37.
> *R v Kang-Brown*, 2008 SCC 18, [2008] 1 SCR 456 at paras 174-5, 227 [*Kang-Brown*].

53. The police obtained cell phone 'tracking data' which reveals the location of cell phones. 'Smart phones' record tracking data every three seconds. Tracking data records the direction of a cell phone in relation to a transmission tower, as well as an estimated distance from the tower. In urban areas with good transmission tower coverage tracking data can reliably pin-point an individual to within 50 metres.

54. It is possible to identify individuals from the cell phone data that the police collected. People behave in patterns. Individual identities can be discovered by comparing patterns in the metadata to facts otherwise known about a person. Even knowing a person's address and place of work may be sufficient to identify them within the data.

55. Information touching on a person's biographical core can be inferred from tracking data. Tracking data, like an IP address, bears little information when viewed in isolation. Through inferences, however, tracking data can reveal much about a person. The mere fact that a person was in a certain location can give rise to sensitive information about the person in that location. One or more visits to an abortion clinic, a marijuana dispensary, a gay club, or a religious building reveal personal information about the person in that location.

56. The collection of metadata such as tracking data can be more corrosive to privacy than conventional searches. The metadata of our communications are structured. Metadata is presented numerically and can be easily sorted and searched. Information about a single

person which may take days to find by tracking the content of their communications, may be discovered about thousands of people in a matter of minutes with metadata. This "enables 'mass' or 'wholesale' electronic surveillance", which in the United States has been found to "rais[e] greater Fourth Amendment concerns than a single electronically surveilled car trip."

> *In the Matter of an Application of the United States of America for an Order Authorizing the Release of Historical Cell-Site Information*, No 10-MC-897, United States District Court, ED New York (August 22, 2011) at para 16.
>
> Felten, Edward W., "Declaration of Professor Edward W. Felten," *American Civil Liberties Union et al v James R Clapper et al*, No 13-cv-03994 United States District Court, SD New York (August 2013).

57. The use of software to filter the data does not prevent a s. 8 breach. The subject of the search should be assessed by looking at what was collected, rather than the portions of what was collected that happened to be seen.

58. Firstly, there was no requirement in the order nor the statute that the police filter the data with computer software. The privacy of Flavellian citizens should not be left to the whims of the police in their selection of a filtering methodology.

59. Secondly, the software does not remove the potential for abuse. The only meaningful oversight over the data can occur at the point of collection. Once the information is within police hands, the police themselves are the only ones capable of ensuring that the information is not used in a way that creates a privacy breach. Aside from whistleblowers, the public has no way of knowing whether information in police hands is being handled in a way that prevents privacy violations. Unlike in *Kang-Brown,* the collection and analysis of tracking data is not done in full public view. This gives rise to

the concern LaForest J. expressed in *R v Duarte* that there is the risk of unfettered police discretion regarding communications surveillance.

> *Kang-Brown supra* para 52 at para 64
> *R v Duarte*, [1990] 1 SCR 30, [1990] SCJ No 2 at para 23 [*Duarte*].

60. It is not sufficient for the court to impose conditions intended to restrict which parts of the data can be looked at—as is routinely done with computer hard drives. Ordinarily, conditions serve the purpose of removing any incentive police officers may have to unnecessarily search private items by rendering anything outside the scope of the conditions inadmissible as evidence on prosecution. This approach is not sufficient where police officers have incentives to look at the tracking data which cannot be defused by the inadmissibility of the data as evidence. In this case, the tracking data may contain the data of friends, family, employees, or romantic partners of the police officers overseeing the data. Thus police officers have motivations to look at the data that go beyond the collection of evidence. Given the lack of oversight, these incentives can only be adequately defused if the courts restrict the collection of the tracking data.
61. Thirdly, a genuine privacy violation is felt when individuals know that their personal information could be looked at without consent. A promise that their information will not be looked at is not enough, especially in the absence of effective oversight. A police camera in every bedroom is still a privacy violation even when accompanied by a promise that recordings will only be looked at once a crime has been committed
62. Even if the subject of the search is confined to the data filtered by the software, there remains a reasonable expectation of privacy in that data. Individuals still have to look through the data. Victorius' data will be looked at once isolated by the filtering software. Police will know which number is Victorius' and his every movement for the past three

months. The software may find more than one number fulfilling the criteria for Victorius' travel schedule. The computer may err and flag an unconnected individual as Victorius. At some point human eyes and minds will need to look over and assess the data-points isolated by the software.

63. The police collected more than the raw numbers of the tracking data. They collected the highly personal information that tracking data can reveal. Basic initiative is needed to identify a person from the data. Tracking data touches on the biographical core of those to whom it relates.

ii. The Interest in the Subject Matter

64. The court has described three types of privacy interests: territorial, personal and informational. Informational privacy is most at stake in this case.

> *Spencer supra* para 49 at para 35.
> *Tessling supra* para 46 paras 21-24.

65. Informational privacy includes three conceptually distinct but overlapping understandings of what privacy is: secrecy, control and anonymity. At the heart of informational privacy is the "the thorny question of how much information about ourselves and activities we are entitled to shield from the curious eyes of the state."

> *Spencer supra* para 49 at para 38.
> *Tessling supra* para 46 at para 23.

66. The informational privacy interest in this case is at least as strong as in other cases where the courts have found a reasonable expectation of privacy. A GPS device tracking a vehicle's location invades a reasonable expectation of privacy because of the information it reveals about a person's location. A sniffer dog provides information about the contents

of the bag and therefore engages the privacy interests relating to its contents. Internet subscriber information implicates privacy interests relating to the identity of the source, possessor or user of that information. Similarly, tracking data implicates privacy interests by linking a specific person to specific movements.

R v Wise, [1992] 1 SCR 527, [1992] SCJ No 16 at paras 19-20.
US v Jones, 132 S.Ct. 945 (2012) at paras 7-8.
R v M (A), 2008 SCC 19, [2008] 1 SCR 569.
Spencer supra para 49.

67. Privacy includes the notion of control over information. When the police demanded access to tracking data without the consent or knowledge of cell phone holders, those cell phone holders lost control over their personal information. Cell phone users expect that their locations will not be disclosed beyond the parties that they explicitly permit to have that information. Cell phone users did not consent to a police search of their cell phones for the purpose for which it was conducted.

Spencer, *supra* para 49 at para 40.

68. Even though the tracking data was voluntarily given to Hammerstein and cannot be thought of as secret or confidential, "situations abound where the reasonable expectations of the individual that the information shall remain confidential to the persons to whom, and restricted to the purposes for which it is divulged, must be protected". Once the police obtained the cell phone tracking data, the information was no longer restricted to the persons and purposes for which it was divulged.

R v Dyment, [1988] 2 SCR 417 at 429-30.
Duarte, *supra* para 59 at para 46.

iii. The Subjective Expectation of Privacy

69. The subjective test has been described as a low hurdle. The shock and outrage expressed in the media once it was disclosed that the police had collected the cell phone tracking data reveals the subjective expectation of privacy felt by affected cell phone holders and Flavellians generally.

    Gomboc supra para 43, per Mclachlin CJC dissent at para 117.

iv. The Objective Expectation of Privacy

70. Flavellians can reasonably expect that their cell phones will not to be used as tracking devices by government agents.
71. The contractual and statutory framework may be relevant to, but not necessarily determinative of whether there is a reasonable expectation of privacy. In *Gomboc*, the terms governing the relationship between the electricity provider and its customer were "highly significant" to Mr. Gomboc's reasonable expectation of privacy. Nevertheless, the terms were treated as "one factor amongst many others which must be weighed in assessing the totality of the circumstances.

    Spencer supra para 49 at para 54.
    Gomboc supra para 43 at paras 31-32.

72. Hammerstein was authorized to collect the tracking data under their service contract. The service contract did not contemplate that this information would be disclosed to the police for the purposes that it was. The issue of disclosure to the police by third parties has recently arisen in both *Spencer* and in *Gomboc*. In her dissenting judgment in *Gomboc*,

McLachlin C.J.C. underlined that disclosure to one party does defeat a privacy interest in the matters disclosed:

> Every day, we allow access to information about the activities taking place inside our homes by a number of people, including those who deliver our mail, or repair things when they break, or supply us with fuel and electricity, or provide television, Internet, and telephone services. Our consent to these "intrusions" into our privacy, and into our homes, is both necessary and conditional: necessary, because we would otherwise deprive ourselves of services nowadays considered essential; and conditional, because we permit access to our private information for the sole, specific, and limited purpose of receiving those services.
>
> *Gomboc supra* para 43 per McLachlin CJC dissent at para 100.

73. Like in *Spencer*, the contractual and statutory framework are of little assistance in this case because their interpretation depends on whether there is a reasonable expectation of privacy in the first place. Cell phone holders can reasonably expect that their every location will not be disclosed to the police incidental to the investigation of a distant crime. The act of carrying a cell phone does not give rise to the expectation that information emanating from it can be made available to the police at any moment on the suspicion of a crime by someone nearby.

> *Spencer supra* para 49 at para 60.

B. There Is No Diminished Expectation of Privacy

74. A diminished expectation of privacy typically occurs in circumstances where the person's physical location gives rise to heightened safety concerns or where the search

has an exceptionally narrow target. Neither are apposite here. Examples of circumstances where there is a diminished expectation of privacy include: airport or bus terminals, searches incident to arrest, searches incident to detention, a border crossing, or schoolgrounds. None of these are comparable to civilians who happened to be in range of a particular cell phone tower on a particular day.

Brown supra para 52 at para 45.
R v Mann, [2004] 3 SCR 59, 2004 SCC 52.
R v Simmons, [1988] 2 SCR 495, [1988] SCJ No 86 at p 528 [*Simmons*].
R v M (MR), [1998] 3 SCR 393.

C. Conclusion on the Expectation of Privacy

75. Flavellian citizens have a reasonable expectation that personal information obtained through tracking data is private. Tracking data can potentially reveal intimate information including a person's medical state, financial status, personal relationships, consumption habits, religious and political affiliations all based on the places they have been. The reasonable expectation of privacy of 20,000 citizens, including Victorius, was violated when the police collected the tracking data of 20,000 phones incidental to their investigation of one suspect. The collection of their tracking data was therefore a search within the scope of s.8 of the Charter.

Issue 3: The search contravenes the right to be free from unreasonable search and seizure

76. The search was unreasonable and violates of s. 8 of the *Charter*. Section 8 provides the right to be secure against unreasonable search and seizure. *R v Collins* held that a search is reasonable if:

> (i) it is authorized by law;
>
> (ii) the law itself is reasonable; and
>
> (iii) the search was carried out in a reasonable manner.
>
> *R v Collins*, [1987] 1 SCR 265 at 23.

77. The search was unreasonable because the law itself is unreasonable. However, in the alternative, even if this Court finds that the authorizing law is reasonable, the search was not authorized by law.

A. Section 400 is unreasonable and violates s. 8 of the *Charter*

78. *Hunter et al v Southam Inc* establishes that a search is reasonable if it is undertaken in compliance with statutory powers that require:

> (i) a prior warrant or authorization;
>
> (ii) issued by an impartial arbiter;
>
> (iii) on a sworn showing of *reasonable and probable grounds to believe* an offence has been committed and that *evidence is to be found* in the place to be searched.
>
> *Hunter, supra* para 46 at 43.

79. Section 400 fails to meet the constitutional standard set out in *Hunter* on two grounds. First, s. 400 requires only "reasonable grounds to suspect", not the higher standard of "reasonable and probable grounds". Second, it requires grounds to believe that the

tracking data will "assist with the investigation of the offence", not that evidence "is to be found" in the place to be searched.

Hunter, *supra* para 46 at para 43.

80. Moreover, s. 400 lacks any accountability. Given the vast amount of personal data that can be revealed, the provision must include a requirement to notify individuals whose privacy interests have been affected.

i. Section 400 must require reasonable and probable grounds

81. The "reasonable suspicion" standard is not sufficient for the search of tracking data. Reasonable suspicion is only constitutionally compliant where it achieves the appropriate balance between an individual's s. 8 rights and the reasonable needs of law enforcement. There is a high expectation of privacy in tracking data and this balance can only be achieved with the baseline "reasonable and probable grounds" standard.

Kang-Brown, *supra* para 52 at para 24.

82. Exceptions to the baseline standard in *Hunter* will rarely be constitutional. As the court noted in *R v Simmons* "the safeguards articulated in *Hunter v. Southam Inc*. should not be lightly rejected" and "departures from the *Hunter v. Southam Inc*. standards that will be considered reasonable will be exceedingly rare".

R v Simmons, *supra* para 74 at para 50.

83. The search of tracking data intrudes into core areas of personal privacy and is not analogous to a sniff dog search. In *Kang-Brown*, the court held that sniff dog searches could be conducted based on a reasonable suspicion because of the "minimal intrusion, contraband-specific nature, and pinpoint accuracy" of the sniff dog investigation. A sniff

dog only signals "yes" or "no" in the presence of a targeted substance. Sniff dogs yield a crude piece of information and no intimate details of private lives could possibly be revealed.

Kang-Brown, *supra* para 52 at para 58.

84. The "reasonable suspicion" standard does not strike the proper balance between s. 8 rights and the demands of law enforcement in the context of bulk searches of metadata. Metadata searches have the potential to reveal months of tracking data from thousands of individuals. This mass data collection is not analogous to the minimally intrusive and contraband specific dog sniff search.

85. The use of the "reasonable suspicion" standard at the border does not provide authority for that standard across all locations. In *Monney*, the court found that "border crossings represent a unique factual circumstance for the purposes of a s. 8 analysis." and permitted the "reasonable suspicion" standard. In *Simmons*, the court permitted an exception to the general rule in *Hunter* in the context of customs. The lower standard for searches at border crossings is permitted because of the right for states to control both who and what enter their domain. Consequently, people "do not expect to cross international borders free from scrutiny". Privacy rights yield to the needs of law enforcement only because of the location. The baseline standard remains reasonable and probable grounds.

R v Monney, [1999] 1 SCR 652 at para 42, 171 DLR (4^{th}) 1.

Simmons, supra para 74 at para 52.

86. The reasonable suspicion standard in s. 400 eviscerates the safeguards against unjustified state intrusion found in s. 8 of the *Charter*. This departure from the constitutional minimum is unacceptable in a free and democratic society.

ii. Section 400 must require reasonable and probable grounds that evidence will be found

87. Section 400 must require reasonable and probable grounds that *evidence will be found in the place to be searched*. The authorizing law only requires a reasonable suspicion that the data will *assist in an investigation*. This additional departure from the *Hunter* standard permits exceptionally broad searches that amount to nothing more than fishing expeditions.

    Hunter, supra para 46 at para 43.

88. A law that permits the search of highly revealing tracking data on merely a suspicion that the data will assist with the investigation violates individuals' s. 8 rights under the *Charter*. Technological advances have made bulk metadata searches simpler than ever. As new technology brings new investigative techniques, it is the role of the Court to act as a guardian of the *Charter* and ensure that these procedures do not violate individual's s. 8 rights.

iii. Section 400 requires accountability

89. Parliament has failed to provide sufficient safeguards of accountability for searches under s. 400. As Justice Dickson noted in *Hunter*, "an unreviewable power would clearly be inconsistent with s. 8 of the *Charter*." Accountability and the review of the s. 400 power require after-the-fact reporting and record-keeping.

    Hunter, *supra* para 78 at para 39.
    R v. Tse, 2012 SCC 16 at para 83, [2012] 1 SCR 531[*Tse*].

90. As this case demonstrates, unless information is leaked to the public or a criminal prosecution results, citizens many never know that their personal tracking data was accessed by law enforcement. Unlike a physical search, the individual is not aware they are being searched. Given the highly intrusive nature of tracking data searches, after-the-fact notice is necessary to inform citizens that their privacy has been invaded. The lack of accountability alone is fatal to the constitutionality of s. 400.

    Tse , *supra* para 89 at para 85.

B. The search was not authorized by s. 400

91. If this Court finds the applicable laws were reasonable, the search was unreasonable because it was not authorized by s. 400. The massive collection of metadata that transpired is better characterized as 20,000 searches that spanned over three months' than one single search. In an effort to track down one individual, the personal information of 19,999 people was incidentally searched. Section 400 cannot constitutionally operate to permit the search of an infinite number of people across an infinite amount of time on the suspicion of criminal activity by a single individual.

92. Section 400 requires a reasonable suspicion that an offence has or will be committed and that the tracking data will assist with the investigation of the offence. A "reasonable suspicion" is distinguished from "reasonable and probable grounds" by the degree of probability. Justice Binnie defines "suspicion" as "the expectation that the targeted individual is possibly engaged in some criminal activity". Reasonable suspicion requires a "constellation of objectively discernible facts".

Kang-Brown, *supra* para 52 at para 75.
R v Chehil, 2013 SCC 39 at para 29, [2013] 3 SCR 220.

93. The Crown has not demonstrated that there was a reasonable suspicion that each individual's data would assist in the investigation of the offence. There was no constellation of facts that suggested each search would assist in the investigation. Section 400 does not permit searches where there is merely a generalized suspicion about a particular location, but no reasonable suspicion focused on a specific person.

R v Chehil, *supra* para 92 at para 28.

94. In *Kang-Brown*, the court notes that in cases where large groups of presumably innocent people could be subject to virtually random searches, *Charter* protection should be an immediate concern. The search of all people who did no more than pass through Austin Airport on a particular day is of great concern to the general public, who have the right under s. 8 to go about their law-abiding business without being subject to unreasonable police searches.

Kang Brown, *supra* para 52 at para 79.

Issue 4: The authorizing laws cannot be upheld by section 1 of the Charter

95. Section 400 permits intrusions on core areas of personal privacy that cannot be justified by s. 1 of the *Charter*. The *Protecting Flavellians from Online Crime Act* purports to protect the citizens of Flavelle from online crime. Reducing online crime is a pressing and substantial objective. However, the law is not rationally connected to its goal, the law is not minimally impairing, and the deleterious effects outweigh the salutary effects. Furthermore, no case to date has found that an unreasonable search or seizure could be considered a reasonable limit prescribed by law. It is well established that the onus for upholding legislation that has been found to infringe the *Charter* is on the Crown.

> *R v Oakes,* [1986] 1 SCR 103 at para 70, 26 DLR (4th) 200.
> *RJR-MacDonald Inc v Canada (Attorney General)*, [1995] 3 SCR 199 at para 60.

A. There is no rational connection between the objective of the law and the measures chosen

96. The measures chosen are not rationally connected to the objective of protecting Flavellians from online crime. Section 400 was an amendment to the *Criminal Code* through the *Protecting Flavellians from Online Crime Act*. The case at hand is illustrative of the use of s. 400 as a general investigative technique for all crimes. The rationale put forward by Parliament does not logically connect with the police powers provided under s. 400. Rather, online crimes, such as cyberbullying, were used as a guise for passing a law that permits broad sweeping police powers that eviscerate privacy rights with respect to tracking data where there is a suspicion of any crime, online or not.

B. Section 400 is not minimally impairing

97. Section 400 is not minimally impairing. The law is not "carefully tailored so that rights are impaired no more than necessary". There are "less harmful means of achieving the legislative goal". Section 400 is not minimally impairing for four main reasons.

> *Alberta v Hutterian Brethren of Wilson Colony,* 2009 SCC 37 at paras 53 and 54, [2009] 2 SCR 567.

98. First, s. 400 allows for searches of metadata on the standard of "reasonable grounds to suspect" that the tracking data will "assist" with the investigation. The law could require *reasonable and probable grounds* that evidence would assist in the investigation. The law could require a reasonable suspicion that evidence *is to be found* in the place to be searched. The law could also require that all reasonable alternative means of investigation have been exhausted before a search is permitted, as is required for a wiretap. These alternatives would improve investigative techniques for online crime without authorizing overly broad collections of metadata.

> *R v Araujo*, 2000 SCC 65 at para 29, [2000] 2 SCR 992.

99. Second, the law could be contained in scope. Limitations on the number of individuals to be searched under one authorization and the amount of time they can be searched would tailor the search powers to impair rights no more than necessary.

100. Third, the legislative goal is the protection of Flavellians from online crime, but s. 400 lacks any language that would retain its use to situations involving online crime. Instead, the law provides broad legal access to metadata in wholly unrelated situations that demonstrate no relation to the objective of the Act.

101. Finally, s. 400 lacks accountability. The provision fails to include a notice requirement or a record-keeping requirement. After-the-fact notice would enhance privacy interests

by creating the opportunity for individuals to identify and challenge an invasion of their privacy and to seek a meaningful remedy without compromising the goal of the search.

102. Section 400 is not minimally impairing. Parliament has failed to narrowly construe the law to infringe the s. 8 rights of Flavellians as little as possible while still achieving its objective.

C. The deleterious effects of section 400 outweigh the salutary effects

103. The deleterious consequences of the law outweigh its salutary effects. A society in which the state has unrestrained access to cell phone metadata might be well equipped to fight crime. However, it would also be a society in which privacy no longer had any meaning. Few things are as important to our way of life as the power given to police to invade the privacy of individuals. In order to maintain a sense of autonomy, dignity and integrity, individuals must be able to live their lives without fear of unreasonable search and seizure by law enforcement. As La Forest J stated in *Dyment*, "the restraints imposed on government to pry into the lives of citizens go to the essence of a democratic state". The claimants do not deny the salutary effects of providing police with broad power to apprehend criminals. However, given the significant negative effects on individuals and on society as a whole, the salutary effects are not great enough to justify the deleterious effects.

> *R v Tessling*, *supra* para 46 at para 13.
> *R v Plant*, *supra* para 51 at 293.
> *R v Dyment*, *supra* para 68 at 427-8.

104. The *Charter* violation of s. 400 is not proportionate to its legislative objective and therefore cannot be saved by s. 1 of the *Charter*.

PART V – ORDER SOUGHT

105. The Appellant seeks an order that the appeal be allowed and the costs be awarded against the Respondents in this Court and in both courts below.

ALL OF WHICH IS RESPECTFULLY SUBMITTED

Signed this 19th day of September, 2014.

_____	_____
Danny Urquart	Lauren Harper
	Counsel for the Appellants

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	**97**
Canadian Council of Churches v R, [1992] 1 SCR 236, [1992] SCJ No 5	**26, 28, 30, 32, 34**
Canada (Attorney General) v Downtown Eastside Sex Workers United Against Violence Society, 2012 SCC 45, [2012] 2 SCR 524	**25, 27, 28, 29, 33, 34, 38, 39**
Finlay v Canada (Minister of Finance), [1986] 2 SCR 607, [1986] SCJ No 73	**28**
Hunter et al v Southam Inc, [1984] 2 SCR 145,11 DLR (4th) 641	**46, 78, 79, 87. 89**
In the Matter of an Application of the United States of America for an Order Authorizing the Release of Historical Cell-Site Information, No 10-MC-897, United States District Court, ED New York (August 22, 2011)	**56,**
Minister of Justice v Borowski, [1981] 2 SCR 575, [1981] SCJ No 103	**26**
Nova Scotia Board of Censors v McNeil, [1976] 2 SCR 265, 12 NSR (2d) 85	**26**
R v Araujo, 2000 SCC 65, [2000] 2 SCR 992	**98**
R v Chehil, 2013 SCC 39 at para 29, [2013] 3 SCR 220.	**92, 93**
R v Cole, 2012 SCC 53, [2012] 3 SCR 34	**51**

Case Law	Paragraph
R. v. Tse, 2012 SCC 16, [2012] 1 SCR 531.	**89, 90**
R. v. Trapp, 2011 SKCA 143, [2011] SJ No 728	**52**
*R. v. Ward***,** 2012 ONCA 660, [2012] OJ No 4587	**43**
R v Wise, [1992] 1 SCR 527, [1992] SCJ No 16	**66**
RJR-MacDonald Inc v Canada (Attorney General), [1995] 3 SCR 199, [1995] SCJ No 68	**95**
Thorson v Canada (Attorney General), [1975] 1 SCR 138, [1974] SCJ No 45	**26, 28, 30**
US v Jones, 132 S.Ct. 945 (2012)	**66**

ii. Secondary Sources

Secondary Sources	Paragraph
Felten, Edward W., "Declaration of Professor Edward W. Felten," *American Civil Liberties Union et al v James R Clapper et al*, No 13-cv-03994 United States District Court, SD New York (August 2013)	**56**

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.