UNIVERSITY OF TORONTO FACULTY OF LAW

Grand Moot 2014: Tracking Data, Privacy and the Charter

Case Overview and Moot Problem

Panel: **Members of the 2014 Grand Moot Panel (Supreme Court of Flavelle)**

The Honourable Madam Justice Rosalie Abella

The Honourable Madam Justice Gloria Epstein

The Honourable Madam Justice Bonnie Croll

Mooters: **For the Appellant:**

Daniel Urquhart
Lauren Harper

For the Respondent:

Kathleen Elhatton-Lake
Samuel Greene

Date: October 2, 2014

Location: Alumni Hall (VC 112)
Victoria College
Toronto, Ontario

Program:

Doors	4:30pm
Opening Remarks	5:00pm
Problem Overview	5:10pm
Grand Moot	5:15pm
Reception	6:45pm

UNIVERSITY OF TORONTO FACULTY OF LAW

Special thanks to:

A. Overview

This memorandum summarizes some of the central legal issues in the 2014 Grand Moot problem, *Flavelle Privacy Advocacy Centre v Her Majesty the Queen*. The Appellant, the Flavelle Privacy Advocacy Centre ("FPAC") has appealed to the Supreme Court of Flavelle to find that the search powers created by section 400 of the Flavellian *Criminal Code* ("*Criminal Code*"), as amended by the *Protecting Flavellians from Online Crime Act*, violate section 8 of the *Flavellian Charter of Rights and Freedoms* (the "*Charter*") and cannot be saved by section 1 of the *Charter*.

The Crown, the Respondent in this case, submits the Court of Appeal for Falconer was correct in finding section 400 was constitutional and asks the Supreme Court of Flavelle to deny the Appellant public interest standing.

Section 400 of the *Criminal Code* allows a court to grant an order for tracking data on a showing of a reasonable suspicion that a crime has or will be committed and that the data will assist in the investigation. The *Criminal Code*, as amended, defines "tracking data" as data that relates to the location of a transaction, individual or thing. In response to a reliable tip that the ringleader of a gun-smuggling ring had travelled through Austin Airport on August 15, 2013, the Flavelle National Policing Authority (FNPA) was granted an order, pursuant to section 400, for the tracking data of 20,000 individuals who were at the airport on that day. The FNPA's aim was to match this data to information that it had regarding the ringleader's travel schedule.

Before the FNPA had the opportunity to analyze the tracking data that it had collected, information was leaked to the Austin Daily Mail that the FNPA was undertaking "bulky" surveillance of individuals. In response, the Appellant, FPAC, brought this application on behalf of those that had been affected by the search. FPAC is a non-profit organization devoted to advocacy, research and raising awareness regarding privacy rights in Flavelle. FPAC is a well-established organization with over 30 years of experience. The Respondent argues that FPAC should not be given public interest standing, submitting that it does not have a genuine interest in this issue and that this claim is not a reasonable and effective means of bringing the case to court.

The Appellant claims that the search, undertaken pursuant to section 400, constitutes an unreasonable search and seizure in violation of section 8 of the *Charter*. The Appellant contends that individuals have a reasonable expectation of privacy in their tracking data. Moreover, the Appellant submits that section 400 is unreasonable and, in the alternative, that the search undertaken in this case was not authorized by law. In light of these arguments, the Appellant seeks a declaration that section 400 of the Flavellian *Criminal Code* is unconstitutional.

The Respondent wishes to uphold the constitutionality of section 400. The Respondent challenges each of the Appellant's submissions, arguing that individuals do not have an expectation of privacy in tracking data and, in the alternative, that section 400 strikes a balance between Flavellian citizens' privacy interests and the legitimate needs of law enforcement. If this Court

does find there to be a section 8 violation, the Respondent also submits that section 400 can be upheld by section 1 of the *Charter*.

As this Court is being asked to determine only matters of law, the standard of review is correctness. Oral arguments are confined to public interest standing, section 8 and section 1 of the *Charter*.

B. Summary of the Case

1. Stern, Austin and Stewart are three cities located within Falconer, a common law province in Flavelle. Flavelle and Falconer have a Constitution, system of government, judicial system and common law history identical to that of Canada and Ontario, respectively.

2. The highest court of Flavelle is the Supreme Court of Flavelle. All Canadian legislation is binding on the Supreme Court of Flavelle, but the Court is not bound by Canadian jurisprudence. This includes jurisprudence from provincial Courts of Appeal; however, decisions from the Supreme Court of Canada are highly persuasive.

3. Between May and August of 2013, the cities of Stern, Austin and Stewart saw a rapid and unprecedented rise in gun crime. This was largely attributed to the increase in illegal guns being smuggled into each of the cities from international dealers. The rise in gun crime had been devastating to these municipalities. Apart from a tragic increase in gun-related injuries and deaths, a sense of panic was beginning to spread in the municipalities and community leaders were speaking out about no longer feeing safe on city streets. Anonymous polls taken in each of the cities found that citizens increasingly felt the need to purchase guns themselves for self-defense.

4. Although the local police departments in each of the four cities were engaging in regular raids and had apprehended a few low-level dealers of these illegal arms, traditional policing techniques were doing little to stem the influx of arms into the cities of Falconer. Given the breadth of the operation, which spanned several municipalities, local police referred the case to the Flavelle National Policing Authority ("FNPA"). However, even the FNPA was unable to make substantial inroads into the investigation. It was clear that a sophisticated gun smuggling ring had taken root.

5. In July 2013, the FNPA discovered that the gun smuggling ring was being run by a criminal organization known as Carnegie. Carnegie is a uniquely de-centralized criminal organization. The organization has satellite units in each of Stern, Austin and Stewart, but the satellite units are largely disconnected from one another. Coordination between the units occurs only through Carnegie's leader and mastermind, known to criminal associates and law enforcement agencies only as Victorius. Given the decentralized nature of the organization, the FNPA was convinced that if they could catch Victorius, the entire organization would collapse.

6. Victorius' identity was known only to his or her closest associates, and despite ardent and meticulous police work by the FNPA, the mastermind's identity remained unknown. The only information that the FNPA was able to uncover from its investigations was that Victorius constantly travelled between Stern, Austin and Stewart on a regular schedule in order to monitor Carnegie's operations. Victorius moved from city to city each week, spending seven days in each city before travelling to the next. Victorius would also constantly keep in touch with criminal associates using an iPhone.

7. In late August 2013, the FNPA received a tip from a reliable informant that Victorius had passed through Austin Airport on August 15, 2013. Although the FNPA had missed its opportunity to track down Victorius, this information gave Constable Fae Herty, an FNPA officer who had been working on the case since May, an inspiration: why not leverage Victorius' regimented travel schedule to try to finally nab this mastermind?

8. Constable Herty and other members of the FNPA had recently received training in response to the enactment of the Flavellian legislation, *Protecting Flavellians from Online Crime Act*, which amended the Flavellian *Criminal Code*. These amendments were designed to update the *Criminal Code* to keep up with modern crime, and specifically to provide updates to investigative tools that would enable police to respond more effectively to crimes using modern technology. The new section 400 of the *Criminal Code* allows law enforcement agencies to apply to a justice or judge to order a person to prepare and produce a document containing tracking data in their possession or control when they receive the order, as long as there are reasonable grounds to suspect that an offence has been or will be committed under any Act of Parliament, and the data will assist in the investigation of the offence. According to FNPA training, applying for an order to obtain tracking data in someone's possession was to be distinguished from applying for a warrant authorizing an officer to install, activate, use, maintain, monitor and remove tracking devices for real-time monitoring.

9. According to the *Criminal Code*, as amended by the *Protecting Flavellians from Online Crime Act*, "tracking data" means data that relates to the location of a transaction, individual or thing.

10. According to the Minister of Justice, the amendments to the *Criminal Code* reflect the new realities for communication technology and the need for modern investigative techniques. The way in which people communicate and use technology has changed dramatically over the years and this has had a significant impact on investigations. The sort of data that police now need to conduct investigations cannot be obtained using traditional investigative techniques. These updates to the law were intended to ensure that a criminal is not able to avoid police investigative techniques because he or she uses modern technology to communicate or conduct his or her affairs.

11. Constable Herty had a breakthrough. Despite not having information regarding the identity of Victorius, historical tracking data held by cell service providers could hold the key to narrowing down a list of possible phone numbers that might belong to Victorius.

12. All cellular service in Stern, Austin and Stewart was provided by a company known as Hammerstein Inc. ("Hammerstein"). Hammerstein kept records of the closest cellular towers to any given phone at any given time for a period of three months as part of a longitudinal study undertaken to improve cellular service. Given the spacing of Hammerstein's cell towers, the company was able to triangulate a subscriber's location to within 50 metres. The collection of this data was well within the scope of Hammerstein's contract with its subscribers, which allowed Hammerstein to collect a wide array of information, including tracking information, in order to, among other things, develop and improve its services and systems.

13. Given that Victorius had passed through Austin Airport on August 15, 2013, his phone number would have been captured by the cell service tower that was proximal to the airport. Constable Herty believed that it would be possible to identify Victorius' phone number by matching the historical cell phone tracking data to Victorius' travel schedule.

14. Pursuant to section 400 of the amended *Criminal Code*, Constable Herty applied to the court for an order for Hammerstein to produce three months of historical tracking data of all of the cell phones that had been captured by the Austin Airport cell tower on August 15, 2013. Constable Herty did not ask for the subscriber information attached to the phone numbers, but only the historical tracking data associated with those numbers. In the production order, Constable Herty did not specify the method by which the FNPA would be analyzing the data.

15. On August 29, 2013, the court granted Constable Herty's application as requested and Hammerstein was ordered to produce tracking data between May 15, 2013 and August 15, 2013 for all of the phone numbers of individuals passing by the Austin Airport cell service tower on August 15, 2013. This order produced tracking data for over 20,000 independent phone numbers. FNPA and Constable Herty received this data on September 10, 2013.

16. FNPA's strategy was, upon the collection of the tracking data, to undertake an analysis of the data to search for patterns in individuals' movements during that period. Specifically, the FNPA would search for phone numbers of individuals whose movements matched the travel schedule of Victorius. In order to process this large quantity of information, the data would be fed into a computer, which would analyze the data using a complex algorithm. The computer would then filter out the phone numbers that did not match the criteria set out in the algorithm. No FNPA officer would directly analyze the data.

17. Before Constable Herty had an opportunity to assess the data, on September 15, 2013, information was leaked to the Austin Daily Mail that the FNPA was undertaking "bulky" surveillance of individuals. The revelation that the FNPA had collected a large amount of metadata sparked outrage from the people of Flavelle. Although the information received by the Austin Daily Mail revealed that the bulky surveillance occurred at the Austin Airport, since the FNPA refused to release information regarding the particular day that the

surveillance had taken place, individuals could not identify whether or not their metadata had actually been tracked.

18. In a public statement by the FNPA following the Austin Daily Mail report, the Director of FNPA described the nature of this type of surveillance in greater detail. She said:

"FNPA's collection of tracking data was performed in full accordance with the requirements of section 400 of the Flavellian Criminal Code. In order to dispel any concerns, I would like to clarify the exact nature of the type of data that we have been collecting.

Metadata is information that is generated as you use technology. The data collected generally does not contain personal or content-specific details. It does not provide information regarding the substance or content of the communication.

The data collected does contain transactional information about the user, the device and activities taking place. For example, telephone metadata would include the phone numbers of the callers, the time of call, the duration of call and the location of each participant. Email metadata could include additional information such as the subject of the email, the priority and category of the message and any read receipt requests.

Tracking data is a specific type of metadata that can be collected. Although tracking data includes locational data, following the Supreme Court of Canada's recent decision in R v Spencer, we would not be able to obtain any details about the subscriber information relating to that specific tracking data without a warrant."

19. In light of these revelations, the Flavelle Privacy Advocacy Centre ("FPAC") brought an application to declare section 400 of the *Criminal Code* unconstitutional. The application stated that by collecting information on individuals' locations through their telephone metadata, the FNPA was conducting unreasonable searches contrary to section 8 of the *Flavellian Charter of Rights and Freedoms* (the "*Charter*"). The application further submitted that the provisions could not be saved under section 1 of the *Charter*.

20. FPAC is a non-profit organization devoted to advocacy, research and raising awareness regarding privacy rights in Flavelle. FPAC is a well-established organization with over 30 years of experience. The organization was established in the early-1980's with a mandate to act as a civic watchdog with respect to potentially privacy-infringing behaviour by the state of Flavelle. Its members are individuals who are interested in ensuring that the government acts in an accountable fashion. They include: academics, journalists, philanthropists and non-government organizations.

21. FPAC frequently intervenes as a party in privacy-related litigation. FPAC has intervened in several other cases involving alleged breaches of section 8, both in the Supreme Court of Flavelle and the Supreme Court of Canada. These cases include a Flavellian case in which the Supreme Court of Flavelle assessed the privacy interest attached to subscriber information as

well as a case recently heard by the Supreme Court of Flavelle, in which the court will consider the degree of privacy attached to certain mobile devices in the context of a search incident to arrest. Additionally, FPAC has been actively involved in the legislating process. They have been invited to speak to government committees preparing legislation at the provincial and federal levels and have made representations before public inquiries. Additionally, they hold public meetings and rallies, publish articles and hold seminars for students and professionals.

22. FPAC claims that they should be granted public interest standing because the individuals whose data has been collected, analyzed, retained or used by law enforcement could not reasonably be expected to bring their own cases to court as law enforcement is not required to provide notice to persons whose data has been collected, analyzed, retained and/or used. In fact, the date that the surveillance at Austin Airport occurred was only revealed through the course of discovery during trial.

C. Judicial History

Falconer Superior Court of Justice

23. At trial, Bessemer J granted FPAC standing to bring their claim and deemed the court competent to adjudicate the issues.

24. Bessemer J first found that there was a reasonable expectation of privacy that attached to tracking data, Bessemer J pointed to the large quantity of information that could be gleaned about a person by looking at metadata alone. Through tracking data, an individual's whereabouts and patterns of movement can be discerned. As stated by Bessemer J,

"*Metadata such as tracking data is far from innocuous. The potential for invasion of privacy of innocent citizens is huge for an enterprising investigator. Metadata may give insight into an individual's medical status, political inclinations, personal and family relationships and professional ambitions. The ability of law enforcement agencies to track the location of citizens on such a broad scale and with such ease has chilling repercussions for personal liberties*."

25. Bessemer J was also unconvinced as to the reasonableness of such intrusion. She stated that although the actions of the FNPA were authorized by law, that law was not reasonable. Bessemer J objected to the legal standard for obtaining the order for collection of metadata. Although an order was obtained on a suspicion standard for the collection of the metadata, due to the private nature of the information Bessemer J held that the standard to obtain a warrant should be reasonable and probable grounds. Bessemer J refused to read down section 400 on the basis that even if the sections were read down to require an order obtained on reasonable and probable grounds, the sections were unreasonable in their scope, both temporally and in terms of the number of people who might be affected. Bessemer J

expressed concern with how, in this case, the tracking data of 20,000 people was obtained with one order.

26. Bessemer J was unwilling to save section 400 under section 1 of the *Charter*. Although she recognized the importance of law enforcement being able to respond to criminals using technological advances, the potential for abuse of these provisions was immense. The lack of clarity on the situations in which collection of metadata could be invoked and the potential to abuse these investigative techniques in a manner that is wholly unrelated to any clear objective meant that these provisions failed the proportionality test.

Falconer Court of Appeal

27. The Falconer Court of Appeal reconsidered and overturned Bessemer J's findings. Keith J wrote the majority opinion of the court (also writing for Xu J), finding that section 400 of the Flavelle *Criminal Code* was not an unconstitutional infringement of an individual's section 8 right to be free from unreasonable search and seizure and that in any case, the law was justified under section 1. Neal J wrote a concurring judgment.

28. On the substantive matters of the case, Keith J held that section 8 of the *Charter* is intended to protect individuals' privacy interests in relation to their "biographical core" of information. Individuals have a reasonable expectation of privacy in information that reveals intimate details about their personal choices. Keith J acknowledged that the digital age has created interpretive dilemmas for both the legislature and the judiciary. In the past, section 8 considerations were much simpler but technological advances have forced courts to determine how broadly they should construe an individual's "zone of privacy" regarding information about themselves.

29. Keith J went on to assess the data that FNPA collected in this case. She held that the individuals who attended the airport did not have a reasonable expectation of privacy in the tracking data. She found that this data did not touch the "biographical core" of those individuals. While FPNA could tell where a certain cell phone had been, they did not know who was in possession of the cell phone at that time or what they were doing at that particular location. Keith J drew a comparison between this type of information and the information that is obtained through physical surveillance. A police officer can physically observe what stores or restaurants an individual goes to or where he or she gets their haircut. While these are indicators of lifestyle, they do not reveal personal details about that person's life.

30. Keith J also noted that individuals whose information was collected remained anonymous. She acknowledged that following *R v Spencer*, FNPA would have to obtain a warrant if it wanted to identify the individuals whose cell phone metadata had been singled out. Although the subscriber information attached a reasonable expectation of privacy for which a warrant obtained on reasonable and probable grounds would be required, an order on a suspicion basis was sufficient for obtaining anonymous metadata, such as the tracking data information in this case.

31. While acknowledging that she did not have to make any findings regarding section 1 of the *Charter*, Keith J chose to make some comments on the issue. She accepted that the government's objective in enacting section 400 was to provide police and prosecutors with the necessary means to investigate offences. She found that this was a pressing and substantial objective. Criminal activity is much more sophisticated in today's "high-tech environment" and the legislature is entitled to put in place measures to combat modern crime. Moreover, Keith J stated that section 400 was proportional. The "reasonable grounds to suspect" standard still imposes checks and balances on the police and prosecutors, while also allowing law enforcement to conduct surveillance. A more onerous standard would not allow the police to take preventive measures to stop crimes before they occur.

32. Neal J, writing a concurring judgment, held that FPAC did not have standing to bring this application. He acknowledged that a party does not necessarily have to be directly affected by the conduct in question to have standing. However, Neal J held that FPAC is not the appropriate group to bring this application. He stated that FPAC's members do not have a direct stake in this matter as they were not directly affected by FPNA's conduct. Neal J held that the application was more appropriately brought by an individual whose tracking data was actually collected by the FNPA.

33. While Neal J noted that it is important not to immunize legislation and state conduct from challenge, he held that courts should scrutinize persons and groups that seek to be parties to such matters. Neal J stated that those with a direct interest in the matter should be given priority in the allocation of judicial resources. He noted that individuals such as frequent flyers or airport employees were well placed to bring this application themselves.

D. Issues on Appeal

The Attorney General has been granted leave to appeal the Court of Appeal's decision to the Supreme Court of Flavelle.

The Court is being asked to decide the following issues:

1. Does FPAC have standing to challenge the constitutionality of section 400 of the Flavelle *Criminal Code*?
2. Pursuant to section 8 of the *Charter*, is there a reasonable expectation of privacy in tracking data?
3. If so, are the search powers created by section 400 "reasonable"?
4. If a breach of section 8 is found, is section 400 nevertheless upheld under section 1 of the *Charter*?

The Supreme Court of Flavelle has not asked the parties to make submissions on the issue of remedy.

Relevant section of the Flavellian *Criminal Code* as amended by the *Protecting Flavellians from Online Crime Act*

Section 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.
(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.

Relevant sections of the Flavellian *Charter of Rights and Freedoms*

Section 1

The Flavellian 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.

Section 8

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