SCC Court File No: 37524

IN THE SUPREME COURT OF CANADA
(ON APPEAL FROM THE COURT OF APPEAL FOR BRITISH COLUMBIA)

B E T W E E N:

HER MAJESTY THE QUEEN IN RIGHT OF BRITISH COLUMBIA
APPELLANT
(Appellant)

- and -

PHILIP MORRIS INTERNATIONAL, INC.
RESPONDENT
(Respondent)

- and -

ATTORNEY GENERAL OF ONTARIO, INFORMATION AND PRIVACY COMMISSIONER FOR BRITISH COLUMBIA, AND SAMUELSON-GLUSHKO CANADIAN INTERNET POLICY AND PUBLIC INTEREST CLINIC

INTERVENERS

FACTUM OF THE INTERVENER, SAMUELSON-GLUSHKO CANADIAN INTERNET POLICY AND PUBLIC INTEREST CLINIC

Samuelson-Glushko Canadian Internet Policy & Public Interest Clinic (CIPPIC)
University of Ottawa, Faculty of Law,
Common Law Section
57 Louis Pasteur Street
Ottawa, ON, K1N 6N5

David Fewer

Tel: (613) 562-5800 x 2558
Fax: (613) 562-5417
Email: dfewer@uottawa.ca

Counsel for the Proposed Intervener

Samuelson-Glushko Canadian Internet Policy & Public Interest Clinic (CIPPIC)
University of Ottawa, Faculty of Law,
Common Law Section
57 Louis Pasteur Street
Ottawa, ON, K1N 6N5

David Fewer

Tel: (613) 562-5800 x 2558
Fax: (613) 562-5417
Email: dfewer@uottawa.ca

Agent for the Proposed Intervener

TO: **THE REGISTRAR**

COPY TO:

SISKINDS LLP
680 Waterloo Street
PO Box 2520, Station B
London, ON N6A 3V8

James D. Virtue

Tel: (519) 672-2121
Fax: (519) 672-6065
Email: jim.virtue@siskinds.com

Counsel for the Appellant,
Her Majesty the Queen in Right of British Columbia

SUPREME ADVOCACY LLP
100-340 Gilmour Street
Ottawa, ON K2P 0R3

Marie-France Major

Tel: (613) 695-8855 Ext: 102
Fax: (613) 695-8580
Email: mfmajor@supremeadvocacy.ca

Agent for the Appellant,
Her Majesty the Queen in Right of British Columbia

AND TO:

McCARTHY TÉTRAULT LLP
Suite 2400, 745 Thurlow Street
Vancouver, BC, V6E 0C5

Michael A. Feder

Tel: (604) 643-5983
Fax: (604) 622-5614
Email: mfeder@mccarthy.ca

Counsel for the Respondent,
Philip Morris International, Inc.

GOWLING WLG (CANADA) LLP
160 Elgin Street, Suite 2600
Ottawa, ON, K1P 1C3

D. Lynne Watt

Tel: (613) 786-8695
Fax: (613) 788-3509
Email: lynne.watt@gowlingwlg.com

Agent for the Respondent,
Philip Morris International, Inc.

AND TO:

LOVETT WESTMACOTT
12-2544 Dunlevy St.
Victoria, British Columbia V8W 1G2

Angela Westmacott, Q.C
Tel: (250) 480-7475
Fax: (250) 480-7455
E-mail: aw@lw-law.ca

Counsel for the Intervener,
Information and Privacy Commissioner for British Columbia

SUPREME ADVOCACY LLP
100-340 Gilmour Street
Ottawa, ON K2P 0R3

Marie-France Major
Tel: (613) 695-8855
Fax: (613) 695-8580
Email:
mfmajor@supremeadvocacy.ca

Agent for the Intervener,
Information and Privacy Commissioner for British Columbia

AND TO: **Ministry of the Attorney General of Ontario**
Crown Law Office-Civil
720 Bay Street, 8th Floor
Toronto, Ontario
M7A 2S9

Sunil Mathai
Farzin Yousefian
Antonin I. Pribetic
Tel: (416) 326-0486
Fax: (416) 326-4181
E-mail: sunil.mathai@ontario.ca

Counsel for the Intervener, Attorney General of Ontario

SUPREME ADVOCACY LLP
100-340 Gilmour Street
Ottawa, ON K2P 0R3

Marie-France Major
Tel: (613) 695-8855
Fax: (613) 695-8580
Email:
mfmajor@supremeadvocacy.ca

Agent for the Intervener, Attorney General of Ontario

TABLE OF CONTENTS

Page

PART I – OVERVIEW

1. This Court is asked to mediate a conflict of values: do privacy rights of third parties bar a defendant from accessing large health datasets in order to challenge the results of the plaintiff's analysis of that data? CIPPIC argues that the dual protections of industry-standard anonymization techniques and judicial access order safeguards will mediate this conflict.

2. Health data are some of Canadians' most private personal information. Anonymization techniques may permit the sharing of such information, but such techniques go far beyond the simple "stripping of identifiers" ordered by the courts below. Re-identification risks demand anonymization consistent with established guidelines already recognized by Canadian health information regulators.

3. The right to a fair civil trial requires that defendants gain access to the information that forms the basis of the case against them. Analysis of data is not neutral: where government bases decisions on datasets, there will be a need to disclose the underlying data in order to understand those analyses. Pre-trial discovery must include an ability to challenge the data itself and to test (and contest) the algorithms used by an adverse party to arrive at their conclusions.

4. Judicial disclosure orders for data and its analyses may respect personal information embedded in those datasets by including privacy-enhancing conditions. Such conditions might include requiring anonymization consistent with industry-standard guidelines, restricting time, manner and place of access, and requiring credentials of accessing parties. Future cases may involve demands for access to data and analyses undertaken by technologies for algorithmic decision making such as artificial intelligence. Accountability, transparency, explicability and scrutability of decision-making in such cases will demand similarly creative judicially-crafted conditions for explaining how such technologies arrive at decisions that affect Canadians.

PART II – POSITION ON APPELLANTS' QUESTIONS

5. CIPPIC takes no position on the questions posed by the Appellant in this case.

PART III – STATEMENT OF ARGUMENT

A. PRIVACY AND RE-IDENTIFICATION RISKS

6. Privacy is a fundamental value in modern democratic states. Canadian courts have recognized the importance of privacy as a constitutionally protected legal value, requiring the common law to develop in a manner that is consistent with and protective of privacy.[1] Canadian legislation designed to protect privacy is treated as quasi-constitutional, giving it pre-eminence over ordinary legislative initiatives in recognition of the important interests being protected. [2]

7. The Supreme Court of Canada has characterized privacy as "a crucial element of individual freedom which requires the state to respect the dignity, autonomy and integrity of the individual."[3] Harm to privacy interests lies not merely in the misuse of personal information or the infliction of damage in invading such interests, but also in the loss of control over one's personal information.

8. Health data are among Canadians' most sensitive and private personal information. In British Columbia, health records containing such data are protected by the *Freedom of Information and Protection of Privacy Act*.[4] They remain so when stripped of personal identifiers in the fashion considered by the Court of Appeal.

9. The test for whether information is "personal information" under Canada's privacy laws is not restricted to information that on its face personally identifies an individual, but includes information for which there is a reasonable expectation that an individual may be identified upon disclosure of the information.[5]

10. Anonymized data are potentially re-identifiable. It now well recognized that many data fields may be identifying, and that it is frequently possible to cross-reference to other datasets with common fields but that also include the identities of data subjects. While name and address are obvious identifying fields, location, payment, temporal data and even medical tests may also serve as keys to unlocking identity. Merely stripping out personal identifiers does not transform personal

---

[1] *Jones v Tsige*, 2012 ONCA 32, paras 39, 44-46.
[2] *Cash Converters Inc v Oshawa (City)*, 2007 ONCA 502, para 29.
[3] *Schreiber v. Canada (Attorney General)*, [1998] 1 S.C.R. 841 at para 19.
[4] [RSBC 1996] Ch. 165.
[5] *Ontario (Attorney General) v. Pascoe*, 2002 CanLII 30891 at para 1 (ON CA); *Schindler Elevator Corporation (Re)*, 2012 BCIPC 25 at para 82 (CanLII).

information into something other than personal since such meagre anonymization techniques are ineffective against eliminating the risk of re-identification.[6]

11. The reality of re-identification risk is particularly well understood in the context of health data. For this reason, American health information protection regulations have implemented a safe harbour for de-identifying data. The *Health Insurance Portability and Accountability Act (HIPAA)* Privacy Rule requires that either (a) suppression of 18 fields of data, including explicit identifiers (such as names or social security numbers), "quasi-identifiers" (such as dates and geocodes), and unique keys (such as medical device identifiers), or (b) certification by an expert that there is only a small risk of individually identifying data subjects.[7]

12. Canadian privacy regulators have similarly published guidelines on data anonymization, including guidelines applicable to health data.[8]

13. In *Her Majesty the Queen in Right of the Province of New Brunswick v. Rothmans Inc.*, Justice Cyr was alive to this reality. At para 52 of his decision, he wrote:

> I conclude that simply removing direct identifiers from a patient record does not produce de-identified or anonymized data. This is especially true if that data can be linked to other records belonging to the same individual either within a single database or across several databases.

At para 59, Justice Cyr connected the inadequacy of the approach adopted by the British Columbia Court of Appeal in the present case to the legislation, and concluded that "[r]emoving the individuals' names and other identifying information... is, in my view, insufficient to avoid the potential harm that subsection 2(5) is intended to prevent."[9]

14. In *Ontario (Community Safety and Correctional Services) v. Ontario (Information and Privacy*

---

[6] Latanya Sweeney, "Simple Demographics Often Identify People Uniquely", Carnegie Mellon University, Data Privacy Working Paper 3. Pittsburgh 2000 < https://dataprivacylab.org/projects/identifiability/index.html >; Paul Ohm, "Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization" (August 13, 2009), UCLA Law Review, Vol. 57, p. 1701, 2010; U of Colorado Law Legal Studies Research Paper No. 9-12, < https://ssrn.com/abstract=1450006 >; Ravi V. Atreya, Joshua C Smith, Allison B McCoy, Bradley Malin and Randolph A Miller, "Reducing patient re-identification risk for laboratory results within research datasets" J Am Med Inform Assoc 2013; 20:95–101 < https://doi.org/10.1136/amiajnl-2012-001026 >.

[7] U.S. Department of Health and Human Services, *Standards for Privacy of Individually Identifiable Health Information, Final Rule*, Federal Register, 45 CFR, Parts 160–4.

[8] Information and Privacy Commissioner of Ontario, "De-identification Guidelines for Structured Data" June 2016; Khaled El-Emam et al., "Pan-Canadian De-Identification Guidelines for Personal Health Information" (May 2007) (published pursuant to the Federal Office of the Privacy Commissioner's Contributions Program).

[9] 2016 NBQB 106 [*HMTQ(NB) v Rothmans*]

Commissioner), this Court considered the argument that release of data in a different context - pursuant to an access to information request - constituted a re-identification risk. The Court expressed skepticism about this risk, noting that the party advancing it had relied on "unconvincing and generic scholarly research" relating to identifiability, which did not address the specific facts in the case at hand.10

15. Professor Teresa Scassa and Amy Conroy have expressed concern that the decision in *Community Safety and Correctional Services* will "inform decisions made by those responsible for releasing government-held information" in different contexts. Scassa and Conroy identify that:

> … privacy risks are amplified by several factors that will become increasingly important over time, specifically that (i) more and more data is being collected by both public and private sector actors; (ii) the full nature and amount of data that is currently held by private sector actors is unknown; (iii) an increasing amount of data is becoming available in the online world; (iv) information technologies that will assist in reidentifying individuals are continuously advancing while also becoming more accessible and affordable; and finally (v) anonymization techniques are proving to be less reliable than previously believed.[11]

Community Safety and Correctional Services arises in an access to information context, which has the express goal of facilitating broad public dissemination. That goal is absent in the present context of discovery in private litigation. Nonetheless, CIPPIC shares the authors' concern over the Court's approach to re-identification in *Community Safety and Correctional Services.* CIPPIC submits that a different approach is required in the very different context of the present case. In the context of health information, privacy values and re-identification risks are well understood, and regulatory bodies have adopted guidelines for addressing such risk.

B. TRANSPARENCY AND ACCOUNTABILITY: DECISIONS USING DATA

16. Neither data nor the decisions based on that data are neutral. Analysis of data will not produce objective results. There is need to disclose both the underlying data and its overlaying analysis to subject them to testing.

17. Where parties to litigation rely on analyses performed on large datasets, there must be an ability for an adverse party to access the data to perform its own analyses or to contest the merits of an antagonist's analysis. By providing access to the data, the Court allows the defendant to test (and

---

[10] 2014 SCC 31, [2014] 1 SCR 674 at para 60 [*Community Safety and Correctional Services*].
[11] Amy Conroy and Teresa Scassa, "Promoting Transparency while Protecting Privacy in Open Government in Canada" (2015) 53:1 Alberta Law Review 175 at 19.

to contest) the data and algorithms used by the province to arrive at its analysis. Ordinarily, this would be through discovery rules.[12]

18. CIPPIC takes no position on the nature or accuracy of the Province's data or analyses. What is significant is the parties' right, recognized by the Court of Appeal, to look behind the output of a data analytics process to examine the data itself.

19. This is particularly important with data and analytics based on that data. Neither data nor its analyses are neutral. Data and its analyses are always subjective, not objective or free of bias. Data may not necessarily contain patterns or relationships that are meaningful or truthful, and the interpretation of such patterns and relationships always occurs within a specific human context. These human contexts need to be subject to scrutiny.[13]

20. Such scrutiny is required to hold adverse parties accountable for their decisions. Transparency, explicability and scrutability of algorithmic decision-making will demand creative judicially-crafted conditions for explaining how such technologies arrive at decisions that affect Canadians.

C. MEDIATING PRIVACY PROTECTION AND FAIRNESS

21. CIPPIC observes that while this case arose in the context of litigation involving a public data holder - the Province of British Columbia - and a third party, other contexts will arise that will pit values such as personal privacy or commercial trade secrets against other values such as trial fairness or simply the right to know the basis upon which a decision has been made. These contexts may include civil litigation among private litigants, challenges to benefits entitlement decisions made by public bodies (*e.g.*, review sought of a denial of employment benefits), or challenging decisions made by businesses that are adverse to a consumer's interest (e.g., challenging denial of a loan). Other applications of algorithmic decision making could conceivably extend to policing regulatory or even criminal behaviour.

[12] Supreme Court Civil Rules, B.C. Reg. 168/2009, Rule 7-1.
[13] Rob Kitchin "Thinking critically about and researching algorithms, Information, Communication & Society", (2017) 20:1, 14-29.

22. In the present case, values fundamental to our legal system conflict: the rights of individuals to expect the state will honour its obligation to protect their privacy rights conflict with the Respondent's right to fairness in the adversarial process. The key to mediating such conflicts lies in the Court's power to construct orders that are responsive to both values.

23. First, the nature of the legal proceeding may offer protections that, in some cases, are sufficient to justify granting an order to access the data and the analyses of that data. For example, the implied undertaking on all parties in a civil litigation to use material obtained within the process of discovery strictly for the purposes of the court case serves as a mechanism that permits data to flow to a litigant but not further.[14]

24. This approach may be appropriate where the risks of misuse of or loss of control over personal information are small and the value or significance of the data is trivial.

25. Second, courts may construct an access order that responds to the conditions of each case. Questions the court might consider include:

    - What is the nature of the harm to which the data subjects are exposed should access to their personal information be granted?
    - What are the risks of re-identification?
    - What are the relationships between the data subjects and the parties?
    - Is there a risk of the data proliferating?
    - Is there a risk of the data leaving the jurisdiction?
    - Will the data recipient undertake to implement legal, administrative, and technological safeguards against data proliferation and data breach?

26. Similarly, a court may order restricted access to the data. For example, a court may order that only certain persons with authenticated qualifications may access the data, or that the data may not leave a facility or jurisdiction.

[14] *Hunt v. Atlas Turner Inc.*, 1995 CanLII 1800 (BC CA).

27. This form of accommodation was arguably reached by Justice Cyr in *HMTQ(NB) v. Rothmans*. In that case, Justice Cyr was satisfied that privacy interests and the defendant's interest in a fair trial were satisfied by the parties entering to an agreement with a third party, Statistics Canada [at para 45]:

> In light of the very sensitive private information requested, I believe the StasCan Agreement to be reasonable in the circumstances.... The record discloses that the restrictions which will be imposed on any expert accessing the data are standard and appropriate for such data, and do not impair rigorous statistical analysis. Moreover, access to data beyond the scope contemplated by the StatsCan Agreement is not necessary for rigorous research, to validate results, or to comment on the reliability of the data.

28. Such orders may also look to mitigate against the risk of loss of privacy by ordering that data be anonymized in a fashion that mitigates against the risk of re-identification. As we have argued above, merely stripping personal "identifiers" from data is insufficient to protect the privacy interests at stake. Rather, courts should make orders to anonymize data consistent with fair information practices and according to accepted standards or guidelines applicable to such data.

29. Third, the Court must consider the nature of the technological tools implicated by an access order. In the present case, the databases in question are large and complex, but do not involve technologically intricate algorithms. In such cases it will be possible to identify how the data was analyzed to reach the decision-maker's conclusion.

30. However, where analyses of data involves advanced algorithms such as neural nets, machine learning systems or other "black box" artificial intelligence tools, it may prove impossible to say exactly how a decision was arrived at. In such cases, a standard of scrutability may prove unreachable. For these reasons, it is worth asking whether the state should employ such tools at all in the service of decision making that implicates human rights and dignity.[15]

[15] See, *e.g.*, B Goodman and S Flaxman, 'European Union Regulations on Algorithmic Decision Making and a "Right to Explanation"' (2016) ICML Workshop on Human Interpretability in Machine Learning, (v3); (2017) 38 AI Magazine 50, arguing that the European Union's new General Data Protection Regulation will (a) restrict automated individual decision-making that "significantly affect" users and (b) effectively create a "right to explanation" whereby individuals may demand explanation of an algorithmic decision made about them.

31. CIPPIC suggests that, when such tools are used in the service of state decision-making, alternative tools must be brought to bear to ensure accountability and transparency in the face of what would otherwise appear opaque and inexplicable. These may include audits that focus on system functionality, or the integrity of the rules followed by artificial intelligence systems in reaching decisions, rather than tracing the reasons for a case-specific outcome.[16]

32. Other judicial tools will include ordering inspection of source code and, as in the present case, conditioned access to the data upon which the decision is based constrained by time, location, credentials, and/or trust among experts.

33. In such cases, courts called upon to require a decision-maker to give an account of its analysis will have to structure their orders in ways that are alive to the limits of algorithmic transparency, but equally so to the utility of non-traditional discovery mechanisms to safeguard our confidence in the integrity of the decision-making process itself - or to reveal when that confidence is misplaced.

PART IV – COSTS

34. The intervener will not seek costs and asks that no costs be awarded against it.

ALL OF WHICH IS RESPECTFULLY SUBMITTED this 21st day of December, 2017

[*original signed by*]

David Fewer

Director, CIPPIC

University of Ottawa, Faculty of Law

FTX 102, 57 Louis Pasteur Street

Ottawa, ON, K1N 6N5

Counsel for the Intervener, Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic (CIPPIC)

[16] Finale Doshi-Velez and Mason Kortz, "Accountability of AI Under the Law: The Role of Explanation", MIT Technology Review (November 15, 2017).

PART VI – TABLE OF AUTHORITIES

Authority		Reference in Factum
Statutes		
1	*Freedom of Information and Protection of Privacy Act* [RSBC 1996] Ch. 165 < http://www.bclaws.ca/Recon/document/ID/freeside/96165_01 >	8
2	U.S. Department of Health and Human Services, Standards for Privacy of Individually Identifiable Health Information, Final Rule. Federal Register, 45 CFR, Parts 160–4 < https://www.federalregister.gov/documents/2000/12/28/00-32678/standards-for-privacy-of-individually-identifiable-health-information >	11
3	Supreme Court Civil Rules, B.C. Reg. 168/2009, Rule 7-1 < http://www.bclaws.ca/civix/document/id/complete/statreg/168_2009_01 >	17
Cases		
4	*Jones v Tsige*, 2012 ONCA 32 < http://canlii.ca/t/fpnld >	6
5	*Cash Converters Inc v Oshawa (City)*, 2007 ONCA 502 <http://canlii.ca/t/1rxpx>	6
6	*Schreiber v. Canada (Attorney General)*, [1998] 1 S.C.R. 841 < https://scc-csc.lexum.com/scc-csc/scc-csc/en/item/1620/index.do >	7
7	*Ontario (Attorney General) v. Pascoe*, 2002 CanLII 30891 (ON CA), <http://canlii.ca/t/1chz2>	9
8	*Her Majesty the Queen in Right of the Province of New Brunswick v. Rothmans Inc. et al.*, 2016 NBQB 106	13, 27
9	*Ontario (Community Safety and Correctional Services) v. Ontario (Information and Privacy Commissioner)*, 2014 SCC 31, [2014] 1 SCR 674 at para 60 < https://scc-csc.lexum.com/scc-csc/scc-csc/en/item/13613/index.do >	14-15
10	*Hunt v. Atlas Turner Inc.*, 1995 CanLII 1800 (BC CA), <http://canlii.ca/t/1ddhw>	23
Regulatory Decisions		
11	Information and Privacy Commissioner of Ontario, "De-identification Guidelines for Structured Data" June 2016 < https://www.ipc.on.ca/wp-content/uploads/2016/08/Deidentification-Guidelines-for-Structured-Data.pdf >	12
12	*Schindler Elevator Corporation (Re)*, 2012 BCIPC 25 (CanLII), <http://canlii.ca/t/fvfdl>	9

Academic		
13	Latanya Sweeney, “Simple Demographics Often Identify People Uniquely”, Carnegie Mellon University, Data Privacy Working Paper 3, Pittsburgh 2000 < https://dataprivacylab.org/projects/identifiability/index.html >	10
14	Paul Ohm, “Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization” (2010) 57 UCLA Law Review 1701 < https://ssrn.com/abstract=1450006 >	10
15	Ravi V. Atreya, Joshua C Smith, Allison B McCoy, Bradley Malin and Randolph A Miller, “Reducing patient re-identification risk for laboratory results within research datasets” (2013) 20 J Am Med Inform Assoc 95 < https://doi.org/10.1136/amiajnl-2012-001026 >	10
16	Khaled El-Emam et al., “Pan-Canadian De-Identification Guidelines for Personal Health Information” (May 2007) < http://www.ehealthinformation.ca/wp-content/uploads/2014/07/2007-Pan-Canadian-De-Identification-Guidelines.pdf >	12
17	Amy Conroy and Teresa Scassa, “Promoting Transparency while Protecting Privacy in Open Government in Canada” 53:1 Alberta Law Review 175 (2015) < https://www.albertalawreview.com/index.php/ALR/article/view/284/282 >	15
18	Rob Kitchin (2017) Thinking critically about and researching algorithms” 20:1 Information, Communication & Society < https://doi.org/10.1080/1369118X.2016.1154087 >	19
19	B Goodman and S Flaxman, ‘European Union Regulations on Algorithmic Decision Making and a “Right to Explanation” (v3); (2017) 38 AI Magazine 50, (2016) ICML Workshop on Human Interpretability in Machine Learning, < https://arxiv.org/pdf/1606.08813v3.pdf >	30
20	Finale Doshi-Velez and Mason Kortz, “Accountability of AI Under the Law: The Role of Explanation”, MIT Technology Review (November 15, 2017) < https://arxiv.org/pdf/1711.01134.pdf >	31