SCC File No. 41538

IN THE SUPREME COURT OF CANADA
(ON APPEAL FROM THE FEDERAL COURT OF APPEAL)

B E T W E E N :

FACEBOOK, INC.

Appellant
(Respondent)

- and -

PRIVACY COMMISSIONER OF CANADA

Respondent
(Appellant)

(Style of cause continued on next page)

FACTUM OF THE INTERVENER, BRITISH COLUMBIA CIVIL LIBERTIES ASSOCIATION

(Pursuant to Rules 37 and 42 of the *Rules of the Supreme Court of Canada*)

TEKHNOS LAW
#284 – 123 Edward Street
Toronto, ON M5G 1E2

Cynthia Khoo

T: 437-374-0144
E: ckhoo@tekhnoslaw.ca

MOUVEMENT LÉGAL INC.
6560, avenue de l'Esplanade, Bureau 305
Montréal, QC H2V 4L5

Mark Phillips

T: 514-441-5054
F: 438-801-0347
E: mark@mouvement.legal

Counsel for the Intervener,
British Columbia
Civil Liberties Association

CHAMP & ASSOCIATES
43 Florence Street
Ottawa, ON K2P 0W6

Bijon Roy

T: 613-237-4740
F: 613-232-2680
E: broy@champlaw.ca

Agent for the Intervener,
British Columbia
Civil Liberties Association

(…style of cause continued)

- and -

SAUL BENARY, CANADIAN CIVIL LIBERTIES ASSOCIATION, OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER FOR BRITISH COLUMBIA, CENTRE FOR FREE EXPRESSION, BRITISH COLUMBIA CIVIL LIBERTIES ASSOCIATION, OPTION CONSOMMATEURS and SAMUELSON-GLUSHKO CANADIAN INTERNET POLICY AND PUBLIC INTEREST CLINIC

Interveners

ORIGINAL TO:

THE REGISTRAR
Supreme Court of Canada
301 Wellington Street
Ottawa, ON K1A 0J1

COPIES TO:

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

Michael A. Feder
Gillian P. Kerr
Barry Sookman
Daniel G.C. Glover
Connor Bildfell

T: 604-643-5983
F: 604-622-5614
E: mfeder@mccarthy.ca

Counsel for the Appellant,
Facebook Inc.

BORDEN LADNER GERVAIS LLP
World Exchange Plaza
100 Queen Street, suite 1300
Ottawa, ON K1P 1J9

Nadia Effendi

T: 613-787-3562
F: 613-230-8842
E: neffendi@blg.com

Agent for the Appellant,
Facebook Inc.

GOLDBLATT PARTNERS LLP
500-30 Metcalfe Street
Ottawa, ON K1P 5L4

Peter C. Engelmann
Colleen Bauman
Louisa Garib
Lucia Shatat

T: 613-235-5327
F: 613-235-3041
E: pengelmann@goldblattpartners.com

Counsel for the Respondent,
Privacy Commissioner of Canada

JENSEN SHAWA SOLOMAN DUGUID HAWKES LLP
800, 304 – 8th Avenue SE
Calgary, AB T2P 1C2

Glenn Solomon, K.C.
Ryan Phillips

T: 403-571-1507
F: 403-571-1528
E: gsoloman@jssbarristers.ca

Counsel for the Intervener,
Saul Benary

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

Eugene Meehan, K.C.

T: 613-695-8855 Ext.: 102
F: 613-695-8580
E: emeehan@supremeadvocacy.ca

Agent for the Intervener,
Saul Benary

LERNERS LLP
225 King Street West, Suite 1600
Toronto, ON M5V 3M2

Jennifer Hunter
Nadia Jandali Chao
Jaime McKibbon

T: 416-601-2659
F: 416-867-9192
E: jhunter@lerners.ca

Counsel for the Intervener,
Canadian Civil Liberties Association

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

Graham Ragan

T: 613-786-8699
F: 613-563-9869
E: graham.ragan@gowlingwlg.com

Agent for the Intervener,
Canadian Civil Liberties Association

ARVAY FINLAY LLP
1512 – 808 Nelson Street
Box 12149, Nelson Square
Vancouver, BC V6Z 2H2

Kate R. Phipps
Hilary Mutch

T: 604-696-9828

E: kphipps@arvayfinlay.ca

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

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

Matthew Estabrooks

T: 613-786-8699
F: 613-563-9869
E: graham.ragan@gowlingwlg.com

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

STOCKWOODS LLP
TD North Tower, suite 4130
77 King Street West, P.O. Box 140
Toronto, ON M5K 1H1

Justin Safayeni
Sarah Fooks

T: 416-593-3494
F: 416-593-9345
E: justins@stockwoods.ca

Counsel for the Intervener,
Centre for Free Expression

CONWAY BAXTER WILSON LLP
411 Roosevelt Avenue, suite 400
Ottawa, ON K2A 3X9

David P. Taylor

T: 613-288-0149
F: 613-688-0271
E: dtaylor@conwaylitigation.ca

Agent for the Intervener,
Centre for Free Expression

BELLEAU LAPOINTE LLP
300, Place d'Youville, bureau B-10
Montréal, QC H2Y 2B6

Violette Leblanc
Maxime Nasr
Marjorie Boyer

T: 514-987-6700
F: 514-987-6686
E: vleblanc@belleaulapointe.com

Counsel for the Intervener,
Option consommateurs

MICHAEL SOBKIN
331 Somerset Street West
Ottawa, ON K2P 0J8

Michael J. Sobkin

T: 613-282-1712
F: 613-288-2896
E: msobkin@sympatico.ca

Agent for the Intervener,
Option consommateurs

SAMUELSON-GLUSHKO CANADIAN INTERNET POLICY AND PUBLIC INTEREST CLINIC
57 Louis Pasteur Street
Ottawa, ON K1N 6N5

David Fewer
Melissa Dupuis-Crane

T: 613-562-5800 Ext.: 2558
F: 613-562-5417
E: dfewer@uottawa.ca

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

TABLE OF CONTENTS

PART I — OVERVIEW AND STATEMENT OF FACTS

1. This appeal concerns a federal regulator's attempt to enforce quasi-constitutional privacy legislation against one of the largest technology companies in the world, Facebook, Inc. ("Facebook"), whose business model relies on monetizing personal information. One of the few preventative safeguards against undue commercial encroachment on privacy rights appears in s. 6.1 of the *Personal Information Protection and Electronic Documents Act* ("PIPEDA").[1] Under s. 6.1, clarifying clause 4.3 of Schedule 1, consent is valid only if it is reasonable to expect the individual "would understand the nature, purpose and consequences" of a company collecting, using, or disclosing personal information. Given PIPEDA's quasi-constitutional status and purpose, the Act must be interpreted dynamically and contextually to determine what is required of large social media companies to meet their s. 6.1 consent obligations.

2. Section 8 jurisprudence under the *Canadian Charter of Rights and Freedoms* ("the *Charter*")[2] provides guiding principles to ensure that privacy rights weather threats posed by novel technological contexts. Three such principles are of particular salience in this case. First, a normative approach governs; the Appellant's consent obligations are determined based on the privacy protections we *ought* to expect of a large social media company when it collects, uses, or discloses personal information in a free and open society. Second, privacy law fails unless it takes into account "modern technological realities";[3] here, consent obligations must incorporate recognition of the extent to which large social media platforms are intertwined with networks of third parties such as data brokers, surveillance vendors, and law enforcement. Third, s. 8 jurisprudence has soundly rejected a "risk analysis"; social media users should not lose privacy rights simply because they choose to use the Appellant's services, and must still be sufficiently informed of the potential consequences of disclosing personal information for consent to be valid.

3. Applying these s. 8 principles to s. 6.1 clarifies that the "consequences" element of consent warrants greater emphasis than it has to date received. Personal information today is more easily than ever collected, linked across sources, centralized, repackaged, and resold as lucrative data analytics products, which are often used to track users even further.[4] Due to this sociotechnological context, the failure to require large social media platforms to meaningfully inform users of potential

---

1 *Personal Information Protection and Electronic Documents Act*, SC 2000, c 5 [PIPEDA].
2 *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, s 8.
3 *R v Bykovets*, 2024 SCC 6 at para 69 [*Bykovets*].
4 *Ibid* at para 77.

downstream consequences, as explicitly required by PIPEDA, would deprive them of the informational self-determination that s. 8 jurisprudence has steadfastly protected for decades.

4. Finally, a regulator must be free to enforce the law against companies that have failed to remain in ongoing compliance relative to the evolving technological and social realities that shape both privacy rights and the legal obligations that give effect to those rights. Deciding otherwise would risk granting regulated entities a *de facto* license to erode our right to privacy at will.

PART II — POSITION ON THE QUESTIONS IN ISSUE

5. The British Columbia Civil Liberties Association ("BCCLA") takes no position on the outcome of the questions in dispute. BCCLA's submissions aim to assist the Court in determining the substance of consent obligations of a large social media company under PIPEDA, which is necessary to answering the first question set out by each party.

PART III — STATEMENT OF ARGUMENT

A. Section 8 Principles Protecting Privacy Against Technological Incursion Over Time Provide Interpretive Guidance

6. PIPEDA must be applied dynamically, contextually, and purposively,[5] to keep pace with "new sociological or technological circumstances".[6] This is due to the Act's central aim of upholding the right to privacy within a shifting technological context and its quasi-constitutional status.[7] BCCLA adopts here the arguments set out in paragraphs 79 to 87 of the Factum of the Respondent making this point in greater detail. Determining whether a regulated entity such as Facebook has met its legal obligations for obtaining consent under s. 6.1 of PIPEDA requires being alive to the evolving technological context in which the company purports to fulfill those obligations.

7. Section 8 jurisprudence under the *Charter* offers significant guidance to inform this determination, through a well-established set of legal principles that have emerged to protect the right to privacy from being digitally dismantled over time. In *R. v. Jarvis*, Chief Justice Wagner explained the value and appropriateness of looking to s. 8 case law when interpreting privacy legislation:

---

5 *Google LLC v Canada (Privacy Commissioner)*, 2023 FCA 200 at para 69, citing *Rizzo & Rizzo Shoes Ltd (Re)*, [1998] 1 SCR 27.

6 *Telus Communications v Federation of Canadian Municipalities*, 2025 SCC 15 at para 34.

7 PIPEDA, *supra* note 1, s 3; *Douez v Facebook, Inc*, 2017 SCC 33 at para 59 [*Douez*]; *Alberta (Information and Privacy Commissioner) v United Food and Commercial Workers, Local 401*, 2013 SCC 62 at paras 19–22.

> Because this Court and other courts in Canada have most frequently had occasion to consider the concept of privacy in the context of s. 8 of the *Charter*, the s. 8 case law represents a rich body of judicial thought on the meaning of privacy in our society. And far from being unmoored from our ordinary perceptions of when privacy can be expected…, judgments about privacy expectations in the s. 8 context are informed by our fundamental shared ideals about privacy as well as our everyday experiences.[8]

8. This case revolves around the "everyday experiences" of typical social media users and will determine the shared ideals that Canadian privacy law upholds regarding the leeway a large Internet company has (if any) when seeking consent to collect, use, or disclose personal information. Examining s. 8 decisions that address the question of preserving privacy in the face of new technological contexts provides three principles of particular relevance to this case: applying a normative approach, integrating an understanding of modern technological realities, and dismissing risk-based analysis. When applied to s. 6.1 of PIPEDA, these principles provide a critical bulwark against the curtailment of individuals' privacy rights by global technology companies wielding power, resources, and capabilities that rival those of nation states.[9]

B. The Normative Approach Governs Determination of Privacy Expectations

9. It is settled law that reasonable privacy expectations follow a "normative rather than a descriptive standard".[10] Determining the substance of this standard is thus "inevitably laden with value judgments about the sort of free and democratic society that reasonable and informed Canadians expect to live in, based on concerns about the long-term consequences of tolerating state intrusion into individual privacy"[11]—or, in this case, commercial intrusion. Applying the normative approach to PIPEDA promotes coherence between Canadian constitutional and quasi-constitutional privacy law, and aligns with PIPEDA's emphasis on a reasonableness standard.[12]

---

[8] *R v Jarvis*, 2019 SCC 10 at para 59 [*Jarvis*].

[9] See e.g. Appellant's Record [AR], Vol 3, Exhibit U at 227 ("[T]he four largest tech companies' capitalization [were valued at] at $2.8 trillion dollars[,] approximately the same amount as France's current GDP"); AR, Vol 14, Exhibit V at 19 ("Since 2016, we have improved our techniques to prevent nation states from interfering in foreign elections…").

[10] *R v Tessling*, 2004 SCC 67 at para 42 [*Tessling*]; see also *Jarvis*, *supra* note 8 at para 68.

[11] *R v Campbell*, 2024 SCC 42 at para 48.

[12] PIPEDA, *supra* note 1, ss 3, 5(3), 6.1; Sch 1, cls 4.3.2, 4.3.5; *Canada (Privacy Commissioner) v Facebook, Inc*, 2024 FCA 140 at paras 60–63 [FCA Reasons].

10. The Appellant commits a key error warned against in *Jones*: "Overemphasizing ... a subjective expectation of privacy cannot be reconciled with the normative nature of the s. 8 inquiry."[13] Rather, the central inquiry should be how far "privacy *ought* to extend to protect individual dignity, autonomy, and personal growth"[14] and to protect the kind of society we would wish to live in.

C. "Modern Technological Realities" Include Social Media Platforms' Enmeshment with Data Brokers, Commercial Surveillance Vendors, and Law Enforcement

11. The s. 8 analysis is adaptive: what it asks of governed actors evolves to meet "new social, political and historical realities",[15] so that the law continues safeguarding individual and collective privacy as technological capabilities advance. The law places greater obligations on police conducting searches of, for example, prospective text messages (considered a Part VI interception despite a different technical mechanism than for phone calls);[16] a computer found during an authorized search or cell phone found incident to arrest (due to fundamental differences between such devices and other physical objects);[17] text messages regardless of on whose phone they were (locating the privacy interest not in each technical message, but in the "electronic conversation" collectively constituted);[18] and IP addresses and basic subscriber information (due to their technical and contextual ability to facilitate "deeply intrusive invasion[s] of privacy"[19]). The jurisprudence clearly traces a throughline that establishes understanding the "social context of the digital world is necessary to a functional approach in defining the privacy interest afforded under the *Charter*".[20] So too must PIPEDA be applied in a way that takes account of this social context and is "supported by modern technological realities"[21]—such as the extensive interconnections between social media companies and third-party data vendors and state actors, respectively.

(i) Data Brokers and Commercial Surveillance Vendors

12. Social media platforms are not standalone entities, but nodes in a sprawling network of commercial third parties, all clamouring for users' data to exploit for a wide range of purposes, many of which

---

[13] *R v Jones*, 2017 SCC 60 at para 20 [*Jones*]; Factum of the Appellant at paras 78, 100 [FOA].
[14] *Bykovets*, *supra* note 3 at para 52 [emphasis added].
[15] *Hunter et al v Southam Inc*, [1984] 2 SCR 145 at 155, cited in *Bykovets*, *supra* note 3 at para 89.
[16] *R v TELUS Communications Co,* 2013 SCC 16 at para 5.
[17] *R v Vu*, 2013 SCC 60 at paras 2–3, 43; *R v Fearon*, 2014 SCC 77 at paras 51, 83 [*Fearon*].
[18] *R v Marakah*, 2017 SCC 59 at paras 17, 19, 54 [*Marakah*]; *TELUS*, *supra* note 16 at para 5.
[19] *Bykovets*, *supra* note 3 at para 10; *R v Spencer*, 2014 SCC 43 at paras 46, 66 [*Spencer*].
[20] *Bykovets*, *supra* note 3 at para 58.
[21] *Ibid* at para 69.

entail inherent or foreseeable harms to those users.[22] These third parties have commonly included data brokers, other major technology companies, and surveillance tool vendors.[23] Such businesses may use their access to Facebook users' data for purposes neither known to nor authorized by those users, including as training or input data for discriminatory decision-making algorithms, or equipping police to surveil protestors.[24] This enmeshment of social media platforms with companies whose business models also depend on voracious collection of personal information must inform the legal analysis of consent under PIPEDA. This would ensure the scope of privacy rights does not shrink in response to, but expands to "offset" the impacts of, myriad commercial actors harvesting "an electronic roadmap of [every] user's cybernetic peregrinations".[25]

13. As this Court has established, there is a categorical difference between the possibility of being incidentally overheard or observed in public and a permanent audio or video recording being made of one's every conversation or movements.[26] Consenting to the former does not and cannot mean relinquishing privacy rights against the latter merely by virtue of technical capabilities enabling the latter.[27] Analogously, there is a substantial difference between Facebook users consenting to share or let their friends share their data, to "foster social connection" or for "enhanced personalization",[28] and the true range of purposes and consequences associated with third-party uses of data potentially facilitated by the Appellant, or even its own uses.[29] PIPEDA should

---

[22] See e.g. *Clearview AI Inc v Information and Privacy Commissioner for British Columbia,* 2024 BCSC 2311 at para 254.

[23] See e.g. David Lie et al, "Automating Accountability? Privacy Policies, Data Transparency, and the Third-Party Problem" (2022), 72:2 UTLJ 155 at 21 (Book of Authorities of the Respondent, Tab 1); AR, Vol 2, Exhibit M at 146–147; Office of the Privacy Commissioner of Canada, *Investigation of the RCMP's collection of open-source information under Project Wide Awake* (Special report to Parliament) (15 February 2024) [*Project Wide Awake*].

[24] See e.g. Office of the Information & Privacy Commissioner for British Columbia, *Always, sometimes, or never? Personal information & tenant screening* (Investigation Report), IR P18-01 (22 March 2018) at 28; *ibid*.

[25] *Tessling, supra* note 10 at para 16; *Bykovets*, *supra* note 3 at 89, 69, citing *R v Morelli*, 2010 SCC 8 at para 3.

[26] *R v Duarte*, [1990] 1 SCR 30 at 48 [*Duarte*]; *R v Wong*, [1990] 3 SCR 36 at 48; see also *Marakah*, *supra* note 18 at para 40.

[27] *R v Reeves*, 2018 SCC 56 at para 42 [*Reeves*], citing *Duarte*, *ibid*.

[28] FOA at paras 9, 12.

[29] See e.g. AR, Vol 4, Exhibit V at 148 (noting the dating app Grindr, which offers account integration with Facebook, shared users' HIV status with marketing analytics companies Apptimize and Localystics); *Douez*, *supra* note 7 at para 7; *Beaulieu c Facebook inc*, 2022

recognize this difference by requiring that users are explicitly informed of the latter kinds of purposes and consequences, which are endemic to the contemporary digital landscape, for their consent to be valid under s. 6.1. Users may not realistically have any later opportunity to provide further prior informed consent nor withdraw consent once their data is already shared.

(ii) Law Enforcement Access to Commercially Collected Personal Information

14. Large Internet intermediaries such as the Appellant have grown to occupy such a pivotal role in the "constitutional ecosystem" that the constitutional relationship under s. 8 is now considered "tripartite". If, by "concentrating [a] mass of information [and having] the tools to aggregate and dissect" unprecedented reams of personal information, "the largest social media companies in the world" have become powerful enough to undermine constitutional privacy guarantees in the course of their normal business operations,[30] this may heighten their legal obligations under PIPEDA.

15. As this Court observed in *Spencer*, "it would be reasonable for an Internet user to expect that a simple request by police would not … defeat *PIPEDA*'s general prohibition on the disclosure of personal information without consent."[31] The dissent in *Gomboc* cautioned against a similar dynamic: "[Electricity customers] cannot be expected to be aware of the details of a complex regulatory scheme … which permits the utility company to pass information on electricity usage to the police".[32] Yet, as noted in *Bykovets*, "technological developments are permitting government actors to expand their surveillance powers significantly, in part by tapping into detailed information collected by the private sector".[33] This is not limited to data collection through constitutionally safeguarded legal paths in criminal or national security law, but includes potentially warrantless access to or outright bulk purchases of personal information.[34] Users may not realize, when consenting to disclose personal information to third parties for purely social or recreational purposes, that their data may also be warrantlessly shared with or sold to police services, intelligence agencies, and possibly foreign law enforcement[35]—nor be conscious of the potential

---

QCCA 1736 at paras 19-20, 23-25 (alleging algorithmic discrimination in targeted ads), leave to appeal to SCC refused, 40620 (31 August 2023).

[30] *Bykovets*, *supra* note 3 at paras 77-78.
[31] *Spencer*, *supra* note 22 at para 62; see also *Jones*, *supra* note 13 at para 20.
[32] *R v Gomboc*, 2010 SCC 55 at para 139, McLachlin CJ and Fish J, dissenting.
[33] *Bykovets*, *supra* note 3 at para 79.
[34] See e.g. *Project Wide Awake*, *supra* note 23; *Clearview AI Inc v Alberta (Information and Privacy Commissioner)*, 2025 ABKB 287 at paras 151–153.
[35] See e.g. *Wakeling v United States of America*, 2014 SCC 72; C-2, *An Act respecting certain measures relating to the security of the border between Canada and the United States and*

repercussions for their constitutional rights. Users thus cannot be considered to have the requisite understanding of potential consequences for their consent to be valid under s. 6.1.

D. Nature of Social Media Platforms Militates Against Already Prohibited Risk Analysis

16. By stressing users *chose* to share personal information, the Appellant relies on an impermissible "risk analysis" to diminish their privacy rights,[36] not least because it ignores the nature of large social media platforms, including the entrenched position they now hold in society and users' lives. The Court has long rejected this line of reasoning as one that, "when taken to its logical conclusion, must destroy all expectations of privacy".[37] Moreover, under s. 8, control over information is not determinative of the privacy right in that information.[38] It is simply wrong to suggest privacy rights are attenuated because "people use Facebook to *share* personal information".[39] The point of informational privacy is the right to control the extent and conditions of sharing; privacy "is not an all-or-nothing concept".[40] Sharing personal data with friends does not equate to consent to disclosing that data to invasive third-party apps, questionable researchers, or politicians' teams.

17. These principles apply with particular force in the case of social media platforms. For many, forgoing the use of social media is tantamount to forgoing genuine relationships, community, political activism, democratic participation, self-expression, and personal flourishing.[41] Users are further governed by platform companies' design choices, which may be deceptive or manipulative, overriding the ability to freely consent.[42] Users may thus be far more limited in real choice than first seems when it comes to participating in social media. To apply a risk or control analysis would present an impossible bind, as recognized in *Jones*, with relevance to interpretation of PIPEDA:

> Canadians are not required to become digital recluses in order to maintain some semblance of privacy in their lives. [Holding that the sender of stored text messages reasonably retains privacy expectations in them despite "relinquished direct control"] comports with

---

respecting other related security measures, 1st Sess, 45th Parl, 2025, cls 158, 194 (first reading 3 June 2025).

36 *Jarvis*, *supra* note 8 at para 68; see also *Marakah*, *supra* note 18 at para 68; FOA at para 64.

37 *Duarte*, *supra* note 26 at 48.

38 See e.g. *Bykovets*, *supra* note 3 at para 46; *Reeves*, *supra* note 27 at paras 37–38; *Marakah*, *supra* note 18 at para 38.

39 FOA at para 53 [emphasis in original].

40 *Jarvis*, *supra* note 8 at para 41.

41 *Douez*, *supra* note 7 at para 56.

42 Jeremy Wiener, "Deceptive Design and Ongoing Consent in Privacy Law" (2021) 53:1 Ottawa L Rev 133.

> contemporary social norms and a purposive approach to s. 8. It also comports with the purpose of PIPEDA, and the approaches adopted by this Court in *Spencer* and *TELUS*.[43]

The more power and influence these platforms wield over users' lives and within society at large, due to their sheer size, network effects, user base, and monopolistic force, the more vulnerable users are to resulting power imbalances[44] and to misuse of their personal data. This factor is one recognized in the European Union's *General Data Protection Regulation*, the predecessor to which PIPEDA was designed to harmonize with.[45] The result is greater need of PIPEDA's protections, such as the requirement to ensure users are meaningfully informed in accordance with s. 6.1.

E. Valid Consent Requires Users to Reasonably Understand Purposes *and Consequences*

18. Section 6.1 of PIPEDA deems consent to be "only valid if it is reasonable to expect [users] would understand the nature, purpose *and consequences* of the … disclosure"[46] of their personal information. Applying the s. 8 principles outlined above—normative approach, taking account of modern technological realities, and rejecting a risk analysis—assists the Court in determining, through dynamic, purposive, and contextual interpretation, the consent standard under s. 6.1 for a large social media company, whether it is satisfied through, for instance, privacy policies, just-in-time consent inquiries, or shutting down features for which complying with s. 6.1 is not possible.

19. These principles are of particular relevance to the notion of consequences in s. 6.1. With respect, the Courts below did not meaningfully engage with this final element of the consent provision: whether it could reasonably be expected that users would understand not just the purpose but the *consequences* of Facebook's disclosure of their personal information to *thisisyourdigitallife* ("TYDL") (for TYDL users), or their own disclosure to Facebook (for TYDL users' friends). Yet consequences were front of mind when Parliament enacted this provision:

> The concept of informed consent is at the very core of PIPEDA…. Informed consent means not just that individuals are told of what is being done with their information, but that they understand the potential consequences of clicking "yes" or "no." The stronger rules included in this bill will make sure that individual Canadians … can understand the potential consequences of the choices they make.[47]

---

[43] *Jones*, *supra* note 13 at para 45.
[44] *Douez*, *supra* note 7 at para 54.
[45] See *AT v Globe24h.com*, 2017 FC 114 at para 49; 2016/679 [GDPR], Recital 75 (risks increase with "a large amount of personal data [and] a large number of data subjects [affected]").
[46] PIPEDA, *supra* note 1, s 6.1 [emphasis added].
[47] *Debates of the Senate*, 41st Parl, 2nd Sess, No 55 (1 May 2014) at 1428 (Hon Leo Housakos).

20. A normative approach suggests that s. 6.1 requires a company in the Appellant's position to explicitly inform users of all potential material consequences of consenting to disclosure of their personal information—regardless of what the company believes the user subjectively expects. Statements such as "anyone who can see it can share it with others, including the games, applications, and websites they use"[48] are overbroad, in communicating so vaguely so as to be meaninglessness, and incomplete, in that it is unreasonable to expect users would understand the range of potential consequences beyond the "mundane examples"[49] implied. This notice fails to capture "modern technological realities" such as the distinction between understanding strangers may see shared posts or photos, and understanding that third-party data vendors may collect more revealing data without the user's consent or knowledge. This may include behavioural patterns, psychological state, inferred health conditions, or location, for instance, extracted through analysis and repurposing of users' activity data.[50] General statements obscuring such consequences violate requirements for valid consent, as also established under substantially similar legislation.[51]

21. As for avoiding a risk analysis, the standard of social media companies' burden to inform users should rise as a function of factors such as size, user base, design choices, market dominance, impacts on society, nature and extent of the company's data flows with third parties in the private sector or law enforcement, and sensitivity and volume of the personal information collected, used, or disclosed. If PIPEDA is to protect individuals' privacy in the context of ever more invasive commercial data practices and technologies,[52] it must require social media companies to be clear, specific, candid, and forthcoming in notices seeking consent under s. 6.1.

F. Regulated Entities Must Comply with Legal Obligations Ongoingly and Autonomously

---

[48] AR, Vol 10, Exhibit E at 366 ("Facebook's Data Use Policy").

[49] FCA Reasons at para 81.

[50] *Bykovets*, *supra* note 3 at paras 66, 76; see also references in note 29, *supra*.

[51] *Joint Investigation of The Cadillac Fairview Corporation Limited* (28 October 2010), PIPEDA #2020-04, online: OPC, ABIPC & BCIPC <canlii.ca/t/jbcq8> at para 86; *Political Parties Investigation (Re)* (6 February 2019), IR P19-01, online: BCIPC <canlii.ca/t/hxk92> at heading 4.15.2.

[52] See e.g. *Lam v Flo Health Inc*, 2024 BCSC 391 at paras 13-15, 21 (alleging the menstrual tracking app Flo disclosed users' pregnancies to third-party companies); *Metro Inc* (18 February 2025), 103799-S, QCCAI <cai.gouv.qc.ca> (facial recognition in a grocery store); *Joint investigation into location tracking by the Tim Hortons App* (1 June 2022), PIPEDA #2022-01, online: OPC, QCCAI, ABIPC & BCIPC <priv.gc.ca>.

22. It is uncontroversial to expect regulated entities to act independently and autonomously to ensure that they are in continuous compliance with the law, regardless of the passage of time and new circumstances arising after the fact.[53] This norm is established across numerous regulatory contexts, including securities (requiring continuous disclosure to investors);[54] pharmaceutics (ongoing obligations after regulatory approval for market, to monitor, report, and inform patients of adverse interactions with "third-party" drugs);[55] and telecommunications (continuous obligations to comply with environmental radiofrequency limits).[56] Similarly sophisticated and well-resourced multinational corporations such as the Appellant have no claim to helplessness and befuddlement when it comes to respecting human rights obligations.

23. In *Lévis*, this Court warned, "Passive ignorance is not a valid defence in criminal law."[57] BCCLA submits that this statement is no less apposite in consumer privacy law. The Appellant should not be granted the illicit right to passivity it seeks in the guise of procedural fairness. In the event of genuine confusion, s. 8 principles again light the way: "faced with real uncertainty, the police should err on the side of caution" in favour of privacy.[58] It is always open to a company in the Appellant's position to "exercise greater caution before interfering with legislatively endorsed privacy rights"[59]—such as those protected under PIPEDA.

PART IV — COSTS

24. BCCLA seeks no costs and asks that no costs be ordered against it.

ALL OF WHICH IS RESPECTFULLY SUBMITTED, this 23rd day of January, 2026.

Counsel for the Intervener,
British Columbia Civil Liberties Association

TEKHNOS LAW
Cynthia Khoo

Counsel for the Intervener,
British Columbia Civil Liberties Association

MOUVEMENT LÉGAL
Mark Phillips

---

[53] *Lévis (City) v Tétreault; Lévis (City) v 2629-4470 Québec inc*, 2006 SCC 12 at para 22 [*Lévis*].
[54] See e.g. *National Instrument 51-102: Continuous Disclosure Obligations*, BC Reg 110/2004.
[55] *Brousseau c Laboratoires Abbott limitée*, 2019 QCCA 801 at paras 130–137, leave to appeal to SCC refused, 38745 (9 April 2020); *Gebien v Apotex Inc*, 2023 ONSC 6792 at para 78.
[56] Industry Canada, *CPC-2-0-03 — Radiocommunication and Broadcasting Antenna Systems*, Issue 6 (July 2022) at heading 7.1.
[57] *Lévis*, *supra* note 63 at para 30.
[58] *Fearon*, *supra* note 19 at para 94.
[59] *Jones*, *supra* note 13 at para 118, Abella J, dissenting.

PART VII — TABLE OF AUTHORITIES

Case Law	Cited in Para(s).
Alberta (Information and Privacy Commissioner) v United Food and Commercial Workers, Local 401, 2013 SCC 62	6
AT v Globe24h.com, 2017 FC 114	17
Beaulieu c Facebook inc, 2022 QCCA 1736, leave to appeal to SCC refused, 40620 (31 August 2023)	13
Brousseau c Laboratoires Abbott limitée, 2019 QCCA 801, leave to appeal to SCC refused, 38745 (9 April 2020)	22
Canada (Privacy Commissioner) v Facebook, Inc, 2024 FCA 140	9, 20
Clearview AI Inc v Alberta (Information and Privacy Commissioner), 2025 ABKB 287	15
Clearview AI Inc v Information and Privacy Commissioner for British Columbia, 2024 BCSC 2311	12
Douez v Facebook, Inc, 2017 SCC 33	6, 17
Gebien v Apotex Inc, 2023 ONSC 6792	22
Google LLC v Canada (Privacy Commissioner), 2023 FCA 200	6
Hunter et al v Southam Inc, [1984] 2 SCR 145	11
Lam v Flo Health Inc, 2024 BCSC 391	21
Lévis (City) v Tétreault; Lévis (City) v 2629-4470 Québec inc, 2006 SCC 12	22, 23
R v Bykovets, 2024 SCC 6	2, 3, 10, 11, 12, 14, 15, 16, 20
R v Campbell, 2024 SCC 42	9
R v Duarte, [1990] 1 SCR 30	13, 16
R v Fearon, 2014 SCC 77	11, 23
R v Gomboc, 2010 SCC 55	15
R v Jarvis, 2019 SCC 10	7, 9, 16
R v Jones, 2017 SCC 60	10, 15, 17, 23
R v Marakah, 2017 SCC 59	11, 13, 16
R v Morelli, 2010 SCC 8	12
R v Reeves, 2018 SCC 56	13, 16
R v Spencer, 2014 SCC 43	11, 15
R v TELUS Communications Co, 2013 SCC 16	11
R v Tessling, 2004 SCC 67	9, 12