

**IN THE SUPREME COURT OF CANADA
(ON APPEAL FROM THE COURT OF APPEAL FOR SASKATCHEWAN)**

B E T W E E N:

MATTHEW DAVID SPENCER

**APPELLANT
(APPELLANT/RESPONDENT)**

- and -

HER MAJESTY THE QUEEN

**RESPONDENT
(RESPONDENT/APPELLANT)**

- and -

**DIRECTOR OF PUBLIC PROSECUTIONS
ATTORNEY GENERAL OF ONTARIO
ATTORNEY GENERAL OF ALBERTA
CANADIAN CIVIL LIBERTIES ASSOCIATION
CRIMINAL LAWYERS' ASSOCIATION OF ONTARIO
PRIVACY COMMISSIONER OF CANADA**

INTERVENERS

**FACTUM OF THE INTERVENER
THE DIRECTOR OF PUBLIC PROSECUTIONS
(Pursuant to Rules 37 and 42 of the *Rules of the Supreme Court of Canada*)**

Public Prosecution Service of Canada
700 EPCOR Tower 10423, 101st Street
Edmonton, AB T4H 0E7
(per Ronald C. Reimer and David
Schernbrucker)
Tel: (780) 495-4079
Fax: (780) 495-6940
E-mail: ron.reimer@ppsc-sppc.gc.ca

Brian Saunders
Director of Public Prosecutions
East Memorial Building, 2nd Floor
284 Wellington Street
Ottawa, ON K1A 0H8
(per: François Lacasse)
Tel: (613) 957-4770
Fax: (613) 941-7865
Email: flacasse@ppsc-sppc.gc.ca

Counsel for the Intervener,
Director of Public Prosecutions

Ottawa Agent for the Intervener,
Director of Public Prosecutions

Aaron A. Fox, Q.C.
Darren K. Kraushaar
McDougall Gauley LLP
1500 - 1881 Scarth Street
Regina, SK S4P 4K9
Tel: (306) 565-5147
Fax: (306) 359-0785
E-mail: afox@mcdougallgauley.com

Counsel for the Appellant

Anthony B. Gerein
Attorney General for Saskatchewan
1874 Scarth Street, 3rd Floor
Regina, SK
S4P 4B3
Tel: (306) 787-5490
Fax: (306) 787-8878
E-mail: tony.gerein@gov.sk.ca

Counsel for the Respondent

Susan Magotiaux
Allison Dellandrea
Attorney General of Ontario
720 Bay Street, 10th Floor
Toronto, ON M5G 2K1
Tel: (416) 326-5238
Fax: (416) 326-4656
E-mail: susan.magotiaux@ontario.ca

Counsel for the Intervener,
Attorney General of Ontario

Jolaine Antonio
Attorney General of Alberta
3rd Floor, Centrium Place
300, 332 - 6 Avenue S.W.
Calgary, AB T2P 0B2
Tel: (403) 592-4902
Fax: (403) 297-3453
E-mail: jolaine.antonio@gov.ab.ca

Counsel for the Intervener,
Attorney General of Alberta

Jeffrey Beedell
McMillan LLP
Suite 300, 50 O'Connor Street
Ottawa, ON
K1P 6L2
Tel: (613) 232-7171 x 122
Fax: (613) 231-3191
E-mail: jeff.beedell@mcmillan.ca

Ottawa agent for the Appellant

Henry S. Brown, Q.C.
Gowling Lafleur Henderson LLP
2600 - 160 Elgin St.
P.O. Box 466, Station "D"
Ottawa, ON K1P 1C3
Tel: (613) 233-1781
Fax: (613) 788-3433
E-mail: henry.brown@gowlings.com

Ottawa agent for the Respondent

Robert E. Houston, Q.C.
Burke-Robertson
70 Gloucester Street
Ottawa, ON K2P 0A2
Tel: (613) 236-9665
Fax: (613) 235-4430
E-mail : rhouston@burkerobertson.com

Ottawa agent for the Intervener,
Attorney General of Ontario

Brian A. Crane, Q.C.
Gowling Lafleur Henderson LLP
2600 - 160 Elgin St
P.O. Box 466, Station "D"
Ottawa, ON K1P 1C3
Tel: (613) 233-1781
Fax: (613) 563-9869
E-mail: brian.crane@gowlings.com

Ottawa agent for the Intervener,
Attorney General of Alberta

Anil K. Kapoor
Kapoor Barristers
20 Adelaide Street East, Suite 210
Toronto, ON M5C 2T6
Tel: (416) 363-2700
Fax: (416) 368-6811
E-mail: akk@kapoorbarristers.com

Counsel for the Intervener,
Canadian Civil Liberties Association

Jill R. Presser and Jonathan Dawe
Schreck Presser LLP
6 Adelaide St. E., 5th floor
Toronto, ON M5C 1H6
Tel: (416) 586-0330
Fax: (416) 977-8513
E-mail: presser@schreckpresser.com

Counsel for the Intervener,
Criminal Lawyers' Association of Ontario

Mahmud Jamal, Patrica Kosseim
Daniel Caron, Sarah Speevak
Osler, Hoskin & Harcourt LLP
P.O. Box 50
1 First Canadian Place
Toronto, ON M5X 1B8
Tel: (416) 862-6764
Fax: (416) 862-6764
Email: mjamal@osler.com

Counsel for the Intervener,
Privacy Commissioner of Canada

Lawrence Greenspon
Greenspon, Brown & Associates
331 Somerset Street West
Ottawa, ON K2P 0J8
Tel: (613) 288-2890
Fax: (613) 288-2896
E-mail: email@lgreenspon.com

Ottawa agent for the Intervener,
Canadian Civil Liberties Association

Marie-France Major
Supreme Advocacy LLP
397 Gladstone Avenue, Suite 100
Ottawa, ON K2P 0Y9
Tel: (613) 695-8855 x 102
Fax: (613) 695-8580
E-mail: mfmajor@supremeadvocacy.ca

Agent for the Intervener,
Criminal Lawyers' Association of Ontario

Daniel Caron
Office of the Privacy Commissioner of
Canada
112 Kent Street, 3rd Floor
Place de Ville, Tower B
Ottawa, ON K1A 1H3
Tel: (613) 947-4634
Fax: (613) 947-4192
E-mail: daniel.caron@priv.gc.ca

Ottawa agent for the Intervener,
Privacy Commissioner of Canada

TABLE OF CONTENTS

PART I: OVERVIEW AND STATEMENT OF FACTS.....	1
PART II: INTERVENER'S POSITION ON THE APPELLANT'S QUESTIONS	1
PART III: ARGUMENT.....	1
A. The appellant had no standing to challenge the alleged police search of his sister's Internet account information.....	1
B. Section 8 does not guarantee a right to publicly use the Internet anonymously.	5
PART IV: COSTS.....	10
PART V: REQUEST TO MAKE ORAL ARGUMENT.....	10
PART VI: TABLE OF AUTHORITIES	11
PART VII – TABLE OF STATUTES.....	14

PART I: OVERVIEW AND STATEMENT OF FACTS

1. The Director of Public Prosecutions (“DPP”) intervenes in this appeal to urge two submissions concerned with the broader implications of the issues in this case. First, in relation to informational privacy, standing to claim a *Charter* remedy requires evidence of sufficient control over the dissemination of the information to demonstrate that the applicant’s personal privacy rights have been implicated. Second, s. 8 of the *Charter* confers no right of anonymity or “public privacy” in respect of a person’s use of a segment of the Internet open to the public.

2. The DPP accepts the facts as stated by the parties and takes no position on any dispute of facts between the parties. The appellant claimed a *Charter* remedy based on police acquisition of his sister’s Internet subscriber information without any evidence about his ability to exercise control over that information. The police were not engaged in any form of electronic surveillance; the information they received, the name and address of an Internet service subscriber and the location where the Internet had been accessed at one moment in time, was a clue towards identifying an unknown suspect.

PART II: INTERVENER’S POSITION ON THE APPELLANT’S QUESTIONS

3. The DPP advances two points. First, the appellant had no standing to challenge the alleged police search of his sister’s Internet subscriber information. Second, s. 8 of the *Charter* does not guarantee a right to openly use the Internet anonymously.

PART III: ARGUMENT

A. The appellant had no standing to challenge the alleged police search of his sister’s Internet account information.

4. In 1996 in *Edwards*¹ this Court firmly established that only a person whose personal rights or freedoms were implicated by state action can seek a remedy under s. 24 of the *Charter*.² The DPP refers to this as the “personal standing” rule, which asks: did the police infringe *this applicant’s* privacy interests? This is distinct from the more generic question

¹ *R v Edwards*, [1996] 1 SCR 128 [Appellant’s Authorities (“A.A.”) Tab 8].

² *Ibid*, per Cory J at para 34.

which asks: does this investigative technique involve a search? The *Edwards* majority specifically and emphatically rejected broader rules of *Charter* s. 24 standing based on an alleged violation of third party rights (“vicarious standing”), or on the prosecution’s proposed use of evidence against the applicant (“target theory” or “automatic standing”).³

5. In *Tessling*⁴ this Court confirmed that determining whether a *Charter* applicant’s reasonable expectation of privacy has been infringed requires examining the “totality of the circumstances”.⁵ In tailoring this test to the FLIR technology used in that case, Binnie J for the *Tessling* court proposed four main questions,⁶ the second of which is: “Did the respondent have a direct interest in the subject matter of the FLIR image?”⁷ This is the crucial issue of personal standing. In the case at bar the Court of Appeal, per Caldwell JA, resiled from this Court’s strong affirmation in *Edwards* and *Tessling* of the rule of personal standing.⁸ Other courts have similarly lapsed.⁹

6. The rule of personal standing is, as Cory J described it in *Edwards*, “of fundamental importance”.¹⁰ He added that: “The reasonable expectation of privacy concept has worked well in Canada. It has proved to be reasonable, flexible, and viable. I can see no reason for abandoning it in favour of the discredited rule of automatic standing.”¹¹

7. The personal standing rule is faithful to the language of *Charter* s. 24(1), which provides that “anyone whose rights or freedoms, as guaranteed by this *Charter*, have been

³ *R v Edwards*, *supra* note 1, per Cory J at paras 28-56.

⁴ *R v Tessling*, 2004 SCC 67, [2004] 3 SCR 432.

⁵ *Ibid* at paras 19, 31; *R v Edwards*, *supra* note 1, per Cory J at para 31.

⁶ *R v Tessling*, *supra* note 4, at para 32. The four questions are: 1. What was the subject matter of the FLIR image? 2. Did the respondent have a direct interest in the subject matter of the FLIR image? 3. Did the respondent have a *subjective* expectation of privacy in the subject matter of the FLIR image? 4. If so, was the expectation *objectively* reasonable? (There then follow (a) – (g) as sub-questions of 4.)

⁷ *Ibid*, underlining added.

⁸ Appellant’s Record (“A.R.”) at 39, para 27. Of the three Court of Appeal judgments, only Caldwell JA addressed standing.

⁹ Re: an accused’s messages retrieved from a third party’s cell phone: *R v Knox* (12 April 2013), Oshawa 998 12 10460 (Ont Ct Jus) at 8-11 [Tab 13]; *R v S.M.*, 2012 ONSC 2949, [2012] OJ no 2833 (QL) at paras 14-17, 24-25 [Tab 21]; *R v Ormston*, 2013 ONCJ 437, [2013] OJ no 3510 (QL) at paras 5, 54 [Tab 19]. Re: an accused simply referred to in intercepted calls: *R v Mah*, 2001 ABQB 394, [2001] AJ no 610 (QL) at paras 22-33 [Tab 16] and *R v Vu*, [2004] OJ no 5681 (QL) at paras 14-16, 64 WCB (2d) 256 [Tab 25]. Re: a search that did not directly affect the accused but was relied upon to support a subsequent search that did: *R v Guilbride*, 2003 BCPC 177, [2003] BCJ no 1258 (QL) at paras 39, 55-57 [Tab 10]; *Cf R v Huynh*, 2008 ABQB 464, [2008] AJ No. 860 at paras. 41-48 [Tab 12].

¹⁰ *R v Edwards*, *supra* note 1, per Cory J at para 34.

¹¹ *Ibid* at para 56.

infringed or denied may apply” for a remedy. Exclusion of evidence under s. 24(2) is available, by its own terms, only “in proceedings under subsection (1)”. The language is clear and must be respected.

8. In *Edwards* this Court adopted the United States Supreme Court’s personal standing rule unequivocally.¹² The USSC had already concluded, *inter alia*, that the undesirable social cost of exclusion easily surpasses any benefit to be gained from enlarging the scope of justiciable rights beyond personal standing.¹³

9. Expanding *Charter* s. 24 standing beyond personal rights, as the Court of Appeal did in this case, wrongly promotes increased litigation about third party interests, and risks greater pressure on our already overburdened justice system, without palpable benefit.

10. *Edwards* requires a *Charter* applicant to allege (and if challenged to establish by calling evidence instead of just relying on “common sense” observations)¹⁴ that his or her rights were in fact directly implicated—the second *Tessling* question. This disciplined approach avoids the spectre of an accused being allowed to bring a *Charter* motion to exclude evidence, with his or her standing assumed, only to see him or her later take the witness box at trial and deny any connection to the evidence.¹⁵

11. The Court of Appeal erred by comingling the narrow question of standing with the broader question of whether what the police did was a search for s. 8 purposes. This error may be explicable, as the jurisprudence on standing has been built almost entirely on territorial privacy, such as searches of dwellings,¹⁶ vehicles¹⁷ and containers,¹⁸ where the broader question was not disputed. Plainly, the two questions may generate different answers even though the same factors are considered in relation to each question. In *Edwards* the applicant had no standing, even though there was a search. In *Tessling* and in *Patrick*¹⁹ the applicant

¹² *R v Edwards*, *supra* note 1 per Cory J at paras 33-35.

¹³ *Rakas v Illinois*, 439 US 128 (1978), per Rehnquist J at 137-138 [Tab 28].

¹⁴ A.R. at 39, para 27; *R v MacInnis*, [2007] OJ no 2930 (QL) at paras. 51-54 (Sup Ct Jus) [Tab 15].

¹⁵ *R v Edwards*, *supra* note 1 at para. 44; *R v Cater*, 2012 NSPC 2, [2012] NSJ no 22 (QL) at para 5 [Tab 5]; *R v Mawut*, 2013 ONSC 1011, [2013] OJ no 1214 (QL) at paras 20-21 [Tab 18].

¹⁶ *R v Edwards*, *supra* note 1; *R v Pugliese*, 1992 CanLII 2781 (ON CA) [Tab 20].

¹⁷ *R v Belnavis*, [1997] 3 SCR 341 [not reproduced].

¹⁸ *R v Buhay*, 2003 SCC 30, [2003] 1 SCR 631 [not reproduced].

¹⁹ *R v Patrick*, 2009 SCC 17, [2009] 1 SCR 579 [A.A. Tab 15; Respondent’s Authorities (“R.A.”) Tab P].

clearly had standing, but there was no search. Standing has not been an issue in this Court's judgments concerning informational privacy,²⁰ and here is this Court's first opportunity to address it. With informational privacy, control is the key.

12. The five factors of the *Edwards* test²¹ are relevant to some aspect of possession or control. With territorial privacy, lawful possession is enough to establish a privacy interest. Concerning informational privacy, by definition there is no equivalent to possession. The inquiry is entirely focussed on control: namely one's ability to determine how, when, and by what means private information may be communicated to others.²²

13. As an example: can an accused person object to the collection of his mother's DNA sample, later used to identify him as the culprit in a sexual assault? Surely not, because his mother has exclusive control over whether or not to provide her bodily sample; any subjective expectation of privacy in that information is unprotected because it is unenforceable.²³

14. In light of this distinction, it is clear that Caldwell JA made three errors in addressing whether the accused had a "personal" or direct interest in the information.²⁴ First, he resuscitated "target theory"²⁵ standing. Second, he unjustifiably defined the information in issue so broadly—"one's activities on one's own computer used in one's own home"—as to predetermine his answer.²⁶ Third, he presumed shared use of a household utility such as an Internet account so as to inevitably but incorrectly lead to a finding that the appellant had a privacy interest in his sister's subscriber information.

15. This last is not an uncommon error.²⁷ It ascribes to the user the same expectation of

²⁰ See e.g. *R v Patrick*, *supra* note 19; *R v Gomboc*, 2010 SCC 55, [2010] 3 SCR 211 [R.A. Tab I]; *R v Kang-Brown*, 2008 SCC 18, [2008] 1 SCR 456 [not reproduced]; *R v A.M.*, 2008 SCC 19, [2008] 1 SCR 569 [R.A. Tab L).

²¹ *R v Edwards*, *supra* note 1 at para 45: (i) presence at the time of the search; (ii) possession or control of the property or place searched; (iii) ownership of the property or place; (iv) historical use of the property or item; (v) the ability to regulate access, including the right to admit or exclude others from the place.

²² *R v Tessling*, *supra* note 4 at para 23.

²³ *R v Thompson*, 1994 CanLII 7402 (ON SC) at paras 2-4, 55-65 [Tab 24].

²⁴ A.R. at 39, para 27, per Caldwell JA.

²⁵ *Ibid.*

²⁶ A.R. at 39, paras 27, 32, per Caldwell JA. See e.g. *R v Patrick*, *supra* note 19 at paras 13, 30.

²⁷ *R v MacInnis*, *supra* note 14 at paras. 52-54; *R v Vasic*, [2009] OJ no 685 (Sup Ct Jus) at para. 45, 185 CRR (2d) 286 [R.A. Tab BB]; *R v Kwok*, [2008] OJ no 2414 (QL) at paras. 13-14 (Ct Jus), 78 WCB (2d) 21 [Tab 14]; *R v S.W.F.*, 2008 ONCJ 740 at para 19, [2008] OJ no 5646 (QL) [Tab 22]; *R v Wilson*, [2009] OJ no 1067 (QL) at para 31 (Sup Ct Jus), 2009 CarswellOnt 2064 [Tab 26]; *R v Mahmood* (2008), 236 CCC (3d) 3 (ONSC) at

privacy in subscriber information as the subscriber herself, without so much as evidence that the user had permission to use the service, let alone any control over the information.²⁸ Absent such evidence, the user is just a third party, a stranger to the contract between the Internet service provider (“ISP”) and the subscriber with no control over the ISP’s use or dissemination of the subscriber information. And this is the decisive point. Lacking any control over the dissemination of the subscriber information, the appellant lacked standing to complain.²⁹

B. Section 8 does not guarantee a right to publicly use the Internet anonymously.

16. This Court’s s. 8 jurisprudence does not support a right of anonymity or public privacy. The claimed right is contradicted by this Court’s statement of principle in *Tessling* that there can be no reasonable expectation of privacy in what one “knowingly exposes to the public, or to a section of the public.”³⁰ This case involves public activity over the Internet, namely using file sharing software to make data available to anyone in the world employing similar software. It does not involve arguably more private Internet activities like using email, or simple web-browsing.

17. In *Ward*,³¹ considering the identical issue in this case, Doherty JA accurately identified the essence of the privacy claim that is being made here—a claim for a right to anonymity or “public privacy,” i.e. the freedom to blend into the “situational landscape” of our interactions with others even in the most public of venues.³² This involves a theory of privacy in which one is with others and expects to be observed but not identified or closely scrutinized. A person driving on the freeway, walking on a busy sidewalk, or attending a hockey game is just another face in the crowd possibly observed but mainly unnoticed.³³ The state is alleged to

paras. 55-56, aff’d 2011 ONCA 693, 282 CCC (3d) 314 [Tab 17]; *R v Deacon*, [2008] OJ no 5756 (QL) at paras. 15-16 (Sup Ct Jus) [Tab 7]; *R v Belcourt*, 2012 BCSC 796, [2012] BCJ no 2636 at paras 8-53 [Tab 4]; *R v Caza*, 2012 BCSC 525, [2012] BCJ no 725 (QL) at para 116 [Tab 6].

²⁸ A.R. at 42-44, paras 31-33; *R v MacInnis*, *supra* note 14 at para 48; *R v Belcourt*, *ibid* at paras 30-34.

²⁹ *R v Pervez*, 2005 ABCA 175, 196 CCC (3d) 521, at paras 13-14 [R.A. Tab Q]; *R v Hutchings*, 1996 CanLII 703 (BC CA) at paras 23-24 [Tab 11]; *R v Edwards*, [1999] OJ no 3819 (QL) at para. 39, 44 (Sup Ct Jus), WCB (2d) 45 [Tab 8]; *R v Fattah*, 2006 ABQB 71, [2006] AJ no 232 (QL) at paras 26-27, 34 [Tab 9].

³⁰ *R v Tessling*, *supra* note 4, per Binnie J at para 40.

³¹ *R v Ward*, 2012 ONCA 660, 112 OR (3d) 321 [R.A. Tab CC].

³² *Ibid*, at paras 70-73.

³³ As Doherty JA observed, this idea was described by the privacy theorist Alan F. West, *Privacy and Freedom* (New York: Athenum, 1967) at 31-32 [Tab 36]. See also: Melvin Gutterman, “A Formulation of the Value and Means Models of the Fourth Amendment in Technologically Enhanced Surveillance” (1998) 39 Syracuse LR 4

violate this private zone when it conducts any form of surveillance that destroys the sense of relaxation and freedom that is enjoyed in this anonymous condition.³⁴ The appellant claims that one ought to enjoy a similar right to get lost in the crowd of the billions of **public** Internet transactions that pass unnoticed each day across the planet.

18. The intervener DPP disputes the proposition that any such right of public privacy or freedom to blend into the situational landscape of the Internet is provided by s. 8 of the *Charter*. The case for a right of anonymity is outweighed by competing societal interests and is contrary to this Court's jurisprudence. The request for a right of anonymity with respect to our public Internet usage is an attempt to carve out a more crime-friendly Internet landscape.

19. The situational landscape of the Internet is strikingly different than the public privacy model on which this claim of privacy rests. Travel on the information superhighway requires more than a personal vehicle such as a computer or smart phone. It also requires a rented vehicle, an Internet protocol address ("IP address"), furnished by an ISP. The privacy implications of car rental are instructive about the analogous condition of having to rent an IP address from an ISP. Renting a car exposes to the car rental company and its employees certain insights into our habits and preferences. We relinquish control over certain private matters that are monitored, documented, and even acted upon by the car rental company to protect its own business and legal interests—the mileage driven, the fact of a fender bender and whether it is repaired, the fact of traffic tickets and when they are paid, and potentially, precise details of a journey if the car is equipped with GPS and electronic-sensor data-recorders.

20. The economic and legal interests of ISPs result in similar exposure of personal biography by their customers. As is apparent from this case, ISPs maintain logs evincing **the precise times** when their vehicles were in use and which of their customers was renting a given vehicle (IP address) at any given time. Scholarly research also tells us that other transactional records are being kept in electronic form by ISPs, web site owners and others

647 [Tab 32]; Matthew M. Werdegar, Note, "Lost? The Government Knows Where You Are: Cellular Telephone Call Location Technology and the Expectation of Privacy" *Lost? The Government Knows Where You Are: Cellular Telephone Call Location Technology and the Expectation of Privacy*, 10 Stan L. & Pol'y Rev 103 (1998) [Tab 35].

³⁴ Gutterman, *ibid* at 706; Werdegar, *ibid* at 111.

that cumulatively record the cybernetic journeys of Internet travelers. This data may also be regularly traded for use in targeting the marketing of products and services.³⁵

21. The reality that one's personal interests and preferences as reflected by Internet usage are being recorded, collated and analyzed by others contradicts the premise that anyone is blending into the landscape, being anonymous or enjoying privacy on the Internet in respect of transactional information. In other words, the public privacy model bears no resemblance to the Internet landscape.

22. The individual interest in publicly using the Internet anonymously has to be weighed against society's critical need to counter the very real threat to public order and security that the Internet represents. In spite of its many social benefits, the Internet is a powerful tool in the hands of those who use it to do harm. It assists organized crime leaders to direct drug trafficking, human smuggling and terrorism without regard for international boundaries, and it aids and abets a wide variety of other serious crimes and harms like fraud, cyber-bullying, harassment, reckless defamation, distribution of child pornography, and the global trade in counterfeit goods and stolen intellectual property.³⁶ It takes little imagination to realize that a right to use the publicly accessible segment of the Internet anonymously would make the Internet even more crime-friendly.

23. There is nothing unusual about trading our anonymity for a safer and more orderly society. As a prominent American defence attorney observed in support of a post-911 proposal for national identity cards, "...privacy and anonymity are not the same. ... taxpayers, voters and drivers long ago gave up any right of anonymity without loss of our right to engage in lawful conduct within zones of privacy." The same commentator questioned whether we can afford to recognize "a right of anonymity in an age of terrorism."³⁷ Even in the more benign context of civil litigation, one important societal interest, the open court principle, outweighs privacy concerns that spawn litigants' requests for anonymity. Only children and rare others able to show a significant potential for harms beyond extreme embarrassment are

³⁵Nathaniel Gleicher, "Neither a Customer Nor a Subscriber Be, Regulating the Release of User Information on the World Wide Web (2008-09) 118 Yale LJ 1945, at 1948-1950 [Tab 31]; Hubbard, DeFreitas & Magotiaux, "The Internet—Expectations of Privacy in a New Context" (2001-02) 45 Crim LQ 170 at 189-191 [Tab 33].

³⁶ *Comprehensive Study on Cyber Crime*, United Nations Office on Drugs and Crime, Draft—February 2013, Chapter 2: *The Global Picture* at 23-51 [Tab 29].

³⁷ Alan M. Dershowitz, "Why Fear National ID Cards?" *New York Times*, (October 13, 2001) [Tab 30].

permitted to use pseudonyms or other mechanisms of anonymity to conceal their identities.³⁸

24. Recognition of a general right to interact anonymously in public is simply incompatible with society's more compelling interest in protection and security. It is plainly at odds with our significant reliance upon essential and highly effective investigative tools, approved by this Court, such as the use of fingerprints³⁹ and DNA comparison.⁴⁰ It is equally at odds with other more rudimentary but equally reliable police work. When a hotel guest is assaulted by someone breaking into her room, the police should not have to seek a warrant before accepting the offer of hotel management to show them contemporaneous security-camera footage of the comings and goings of persons using the hallway outside the scene of the crime.

25. While it is true that this Court's decision in *Wise* employed s. 8 to protect a suspect's vehicular movements along public thoroughfares, the theory of public privacy or a right of anonymity is not mentioned anywhere in the majority's judgment.⁴¹ While that precedent holds that electronic tracking of a person's public vehicular-movements involves a search, it does not provide a sound basis for the inference⁴² that *Wise* supports a general right of anonymity or public privacy. At the same time that it found electronic tracking involved a search, the majority was careful not to proscribe more conventional surveillance of the same public movements.⁴³ The decision plainly evinced concern about state use of extensive electronic surveillance to follow a suspect, even in public areas, but it notably described such tracking as a minimal s. 8 intrusion for which a warrant ought to be available on something akin to reasonable suspicion.⁴⁴

26. There was nothing like electronic monitoring of the appellant's public Internet usage that might be said to violate the proscription established by *Wise*. An undercover police officer interacting with an unknown person accepted an overt offer, broadly and openly available to a large community of persons using similar software, to share a collection of child

³⁸ See e.g.: *B. (A.) v Stubbs*, 1999 CanLII 14801 (ON SC) [Tab 2]; *Doe v Smith*, 2001 ABQB 277 [Tab 3]; *Adult Entertainment Association of Canada v City of Ottawa*, 2005 CanLII 16571 (ON SC) [Tab 1].

³⁹ *R v Beare*; *R v Higgins*, [1988] 2 SCR 387 [not reproduced].

⁴⁰ *R v Rodgers*, 2006 SCC 15, [2006] 1 SCR 554 [not reproduced].

⁴¹ *R v Wise*, [1992] 1 SCR 527 [Tab 27].

⁴² Notably drawn by Justice Doherty in *R v Ward*, *supra* note 31.

⁴³ *R v Wise*, *supra* note 41, at 546.

⁴⁴ *Ibid*, at 548-549.

pornography. The IP address that came along with the shared files provided a clue to finding the unknown file sharer. The investigator simply followed that clue to its logical conclusion.

27. That trail of clues that culminated in the execution of a search warrant might just as easily have met a dead end if the unknown suspect had been using a proxy service or anonymizer⁴⁵ or had been contracting with an ISP with no acceptable use policy that was also unwilling to cooperate with police.⁴⁶ The police eventually found the appellant because a corporate citizen, unwilling to have its facilities used to distribute child pornography, provided a single further clue. The cooperating ISP did not allow the police to electronically monitor anyone's Internet usage and did not provide information equivalent to what could be gathered by such surveillance. No Internet traveler was identified and no travel history was disclosed. The ISP's report to the police said nothing about the nature, quantity, or character of even a single Internet transaction. It merely identified the physical location at which an Internet connection had been accessed by some unknown person at a single moment in time.

28. The proscription against identification flowing from the appellant's proposed right of anonymity must be so broad as to preclude police even from receiving clues toward identification without a warrant. The breadth of the novel right of anonymity claimed here evinces an attempt to use the *Charter* to advance conditions most favorable to criminality. This assertion is made fully mindful of the neutral perspective mandated by this Court's jurisprudence, whereby it is irrelevant that a legitimate expectation of privacy shelters crime along with other lawful private activity. The distinguishing feature here is the very contradiction inherent in claiming freedom to **blend into the landscape** in respect of behavior that **openly** flouts the laws and social mores of society such that it naturally attracts both observation by others and identification of the actor. To accept that principle would call into question whether identifying information or even any clues in that direction could be made available to police without a warrant. Might a warrant be needed before a witness could describe to police a distinctive tattoo on a bank robber's arm? Would it make a difference if the robber was wearing a balaclava?

⁴⁵ A service that accesses the Internet on behalf of the user thus protecting identifying information such as an IP address, for example: www.anonymize.net or www.hidemyass.com [Tab 37]; Hubbard, Magotiaux & Proestos, "The Limits of Privacy: Police Access to Subscriber Information in Canada (2002) 46 Crim L Q, 361 at 371-72 [Tab 34].

⁴⁶ Hubbard, Magotiaux & Proestos, *ibid.*

29. The claim to a right of anonymity in this case involves using s. 8 as a sword to carve out a more crime-friendly Internet landscape rather than as a shield to safeguard a legitimate expectation of privacy. Let's be clear about what is being requested. The appellant claims the right to **openly and publicly** make available child pornography over the Internet with his anonymity protected under the rubric of freedom to **blend into situational landscapes**. Considered in terms of the original paradigm of "public privacy," that is akin to expecting freedom from both observation and identification not only when one is lost in a crowd going to lunch on a busy downtown sidewalk, but also when one is knocking over those pedestrians while making flight after committing a violent crime.

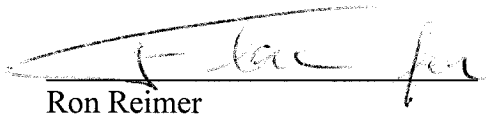
PART IV: COSTS

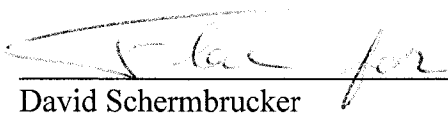
30. The intervener DPP does not seek any costs and makes no submissions as to costs.

PART V: REQUEST TO MAKE ORAL ARGUMENT

31. The intervener DPP asks to present oral argument at the hearing of the appeal.

All of which is respectfully submitted this 26th day of September, 2013.


Ron Reimer


David Schermbrucker
Counsel for the intervener,
Director of Public Prosecutions

PART VI: TABLE OF AUTHORITIES

Case	Para cited
<i>Adult Entertainment Association of Canada v City of Ottawa</i> , 2005 CanLII 16571 (ON SC)	23
<i>B. (A.) v Stubbs</i> , 1999 CanLII 14801 (ON SC)	23
<i>Doe v. Smith</i> , 2001 ABQB 277, [2001] AJ no 428	23
<i>A.M., R v</i> , 2008 SCC 19, [2008] 1 SCR 569	11
<i>Beare, R v; Higgins, R v</i> , [1988] 2 SCR 387	24
<i>Belcourt, R v</i> , 2012 BCSC 796, [2012] BCJ no 2636	15
<i>Belnavis, R v</i> , [1997] 3 SCR 341	11
<i>Buhay, R v</i> , 2003 SCC 30, [2003] 1 SCR 631	11
<i>Cater, R v</i> , 2012 NSPC 2, [2012] NSJ no 22	10
<i>Caza, R v</i> , 2012 BCSC 525, [2012] BCJ no 725	15
<i>Deacon, R v</i> , [2008] OJ no 5756 (ONSC)	15
<i>Edwards, R v</i> , [1996] 1 SCR 128	4, 5, 6, 8, 10, 11, 12
<i>Edwards, R v</i> , [1999] OJ no 3819 (Sup Ct Jus), 44 WCB (2d) 45	15
<i>Fattah, R v</i> , 2006 ABQB 71, [2006] AJ no 232	15
<i>Gomboc, R v</i> , 2010 SCC 55, [2010] 3 SCR 211	11
<i>Guilbride, R v</i> , 2003 BCPC 177, [2003] BCJ no 1258	5
<i>Hutchings, R v</i> , 1996 CanLII 703 (BC CA)	15
<i>Huynh, R v</i> , 2008 ABQB 464, [2008] AJ no 860	5
<i>Kang-Brown, R v</i> , 2008 SCC 18, [2008] 1 SCR 456	11
<i>Knox, R v</i> , (12 April 2013) Oshawa 998 12 10460 (Ont Ct Jus)	5

Case	Para cited
<i>Kwok, R v</i> , [2008] OJ no 2414 (Ct. Jus.), 78 WCB (2d) 21	15
<i>MacInnis, R v</i> , [2007] OJ no 2930 (Sup Ct Jus), 163 CRR (2d) 111	10, 15
<i>Mah, R v</i> , 2001 ABQB 394, [2001] AJ no 610	5
<i>Mahmood, R v</i> , (2008), 236 CCC (3d) 3 (ONSC), [2008] OJ no 3922; aff'd 2011 ONCA 693, 282 CCC (3d) 314	15
<i>Mawut, R v</i> , 2013 ONSC 1011, [2013] OJ no 1214	10
<i>Ormston, R v</i> , 2013 ONCJ 437, [2013] OJ no 3510	5
<i>Patrick, R v</i> , 2009 SCC 17, [2009] 1 SCR 579	11, 14
<i>Pervez, R v</i> , 2005 ABCA 175, 196 CCC (3d) 521	15
<i>Pugliese, R v</i> , 1992 CanLII 2781 (ON CA)	11
<i>Rodgers, R v</i> , 2006 SCC 15, [2006] 1 SCR 554	24
<i>S.M., R v</i> , 2012 ONSC 2949, [2012] OJ no 2833	5
<i>S.W.F., R v</i> , 2008 ONCJ 740, [2008] OJ no 5646	15
<i>Tessling, R v</i> , 2004 SCC 67, [2004] 3 SCR 432	5, 10, 11, 12, 16
<i>Thompson, R v</i> , 1994 CanLII 7402 (ON SC)	13
<i>Vasic, R v</i> , [2009] OJ no 685 (Sup Ct Jus), 185 CRR (2d) 286	15
<i>Vu, R v</i> , [2004] OJ no 5681, 64 WCB (2d) 256	5
<i>Ward, R v</i> , 2012 ONCA 660, 112 OR (3d) 321	17, 25
<i>Wilson, R v</i> , [2009] OJ no 1067 (Sup Ct Jus), 2009 CarswellOnt 2064	15
<i>Wise, R v</i> , [1992] 1 SCR 527	25, 26
<i>Rakas v Illinois</i> , 439 US 128 (1978)	8

Doctrine	
<i>Comprehensive Study on Cyber Crime</i> , United Nations Office on Drugs and Crime, Draft—February 2013, <u>Chapter 2: The Global Picture</u>	22
Alan M. Dershowitz, “Why Fear National ID Cards?” <i>New York Times</i> , October 13, 2001	23
Nathaniel Gleicher, <i>Neither a Customer nor a Subscriber Be, Regulating the Release of User Information on the World Wide Web</i> , 118 Yale L. J. 1945	20
Melvin Gutterman, <i>A Formulation of the Value and Means Models of the Fourth Amendment in Technologically Enhanced Surveillance</i> , 39 Syracuse Law Rev. 647 (1988)	17
Hubbard, DeFreitas & Magotiaux, <i>The Internet—Expectations of Privacy in a New Context</i> , 45 Crim. L.Q. 170 (2001-2002)	20
Hubbard, Magotiaux & Proestos, <i>The Limits of Privacy: Police Access to Subscriber Information in Canada</i> , 46 Crim. L. Q, 361 (2002)	27
Matthew M. Werdegar, note, <i>Lost? The Government Knows Where You Are: Cellular Telephone Call Location Technology and the Expectation of Privacy</i> , 10 STAN. L. & POL’Y REV. 103 (1998)	17
Alan F. West, <i>Privacy and Freedom</i> (New York: Athenum, 1967)	17
Other References	
<u>www.anonymize.net</u> or <u>www.hidemyass.com</u>	27

PART VII – TABLE OF STATUTES

Canadian Charter of Rights and Freedoms, Sections 8 and 24

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

8 Chacun a droit à la protection contre les fouilles, les perquisitions ou les saisies abusives.

24. (1) Anyone whose rights or freedoms, as guaranteed by this Charter, have been infringed or denied may apply to a court of competent jurisdiction to obtain such remedy as the court considers appropriate and just in the circumstances.

24 (1) Toute personne, victime de violation ou de négation des droits ou libertés qui lui sont garantis par la présente charte, peut s'adresser à un tribunal compétent pour obtenir la réparation que le tribunal estime convenable et juste eu égard aux circonstances.

(2) Where, in proceedings under subsection (1), a court concludes that evidence was obtained in a manner that infringed or denied any rights or freedoms guaranteed by this Charter, the evidence shall be excluded if it is established that, having regard to all the circumstances, the admission of it in the proceedings would bring the administration of justice into disrepute.

(2) Lorsque, dans une instance visée au paragraphe (1), le tribunal a conclu que des éléments de preuve ont été obtenus dans des conditions qui portent atteinte aux droits ou libertés garantis par la présente charte, ces éléments de preuve sont écartés s'il est établi, eu égard aux circonstances, que leur utilisation est susceptible de déconsidérer l'administration de la justice.