SUPREME COURT OF CANADA

CITATION: R. *v.* Reeves, 2018 SCC 56

APPEAL HEARD: May 17, 2018
JUDGMENT RENDERED: December 13, 2018
DOCKET: 37676

BETWEEN:

Thomas Reeves
Appellant

and

Her Majesty The Queen
Respondent

- and -

Director of Public Prosecutions, Director of Criminal and Penal Prosecutions, Attorney General of British Columbia, Criminal Lawyers' Association (Ontario) and Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic
Interveners

CORAM: Wagner C.J. and Abella, Moldaver, Karakatsanis, Gascon, Côté, Brown, Rowe and Martin JJ.

REASONS FOR JUDGMENT: (paras. 1 to 69)	Karakatsanis J. (Wagner C.J. and Abella, Gascon, Brown, Rowe and Martin JJ. concurring)
CONCURRING REASONS: (paras. 70 to 103)	Moldaver J.
CONCURRING REASONS: (paras. 104 to 141)	Côté J.

R. *v.* REEVES

Thomas Reeves *Appellant*

v.

Her Majesty The Queen *Respondent*

and

Director of Public Prosecutions,
Director of Criminal and Penal Prosecutions,
Attorney General of British Columbia,
Criminal Lawyers' Association (Ontario) and Samuelson-Glushko
Canadian Internet Policy and Public Interest Clinic *Interveners*

Indexed as: R. *v.* Reeves

2018 SCC 56

File No.: 37676.

2018: May 17; 2018: December 13.

Present: Wagner C.J. and Abella, Moldaver, Karakatsanis, Gascon, Côté, Brown, Rowe and Martin JJ.

ON APPEAL FROM THE COURT OF APPEAL FOR ONTARIO

Constitutional law — Charter of Rights — Search and seizure — Remedy — Exclusion of evidence — Accused's spouse consenting to police entry into home and seizure of computer from shared space — Child pornography found on seized computer and accused charged with possessing and accessing child pornography — Whether police infringed accused's rights to be secure against unreasonable search and seizure by entering shared home and seizing shared computer without warrant — If so, whether evidence ought to be excluded — Canadian Charter of Rights and Freedoms, ss. 8, 24(2).

The accused shared a home with his common-law spouse. Following charges of domestic assault against the accused, a no-contact order was issued which prohibited the accused from visiting the home without his spouse's prior, written and revocable consent. When the spouse contacted the accused's probation officer to withdraw her consent for him to enter the home, she reported that she had found what she believed to be child pornography on the home computer which she shared with the accused. A police officer came to the family home without a warrant. The accused's spouse allowed the officer to enter and signed a consent form authorizing him to take the computer, which was located in a shared space in the home. The police detained the computer without a warrant for more than four months before searching it. They also failed to report the seizure of the computer to a justice, despite the requirements of s. 489.1 of the *Criminal Code*. When the police finally obtained a warrant to search the computer, they found 140 images and 22 videos of child pornography. The accused was charged with possessing and accessing child

pornography but applied to exclude the computer-related evidence claiming that his right to be secure against unreasonable search or seizure pursuant to s. 8 of the *Canadian Charter of Rights and Freedoms* had been violated. The application judge agreed. Accordingly, he excluded the computer evidence under s. 24(2) of the *Charter* and the accused was acquitted. The Court of Appeal allowed the Crown's appeal from the acquittal, set aside the exclusionary order and ordered a new trial.

Held: The appeal should be allowed, the evidence excluded and the acquittal restored.

Per Wagner C.J. and Abella, **Karakatsanis**, Gascon, Brown, Rowe and Martin JJ.: The police infringed the accused's *Charter* rights when they took the computer from his home. Although the computer was shared, the accused maintained a reasonable expectation of privacy in it. The consent of the accused's spouse did not nullify his reasonable expectation of privacy, or operate to waive his *Charter* rights in the computer. The warrantless seizure of the computer and the search of it without a valid warrant were unreasonable, and the admission of the child pornography evidence would bring the administration of justice into disrepute.

It is not necessary in this case to decide whether the entry into the home constituted a separate violation of the accused's rights under s. 8 of the *Charter*. Even if the officer had lawfully been in the home, this would not make the seizure of the computer lawful. The officer testified that he asked for the spouse's consent to seize the computer because he did not believe he had grounds to obtain a warrant. Further,

whether police entry into a shared home with the consent of one resident violates the *Charter* raises complex questions that require a considered response. They are best answered in a case that directly turns on the issue, with the benefit of full submissions.

There is a presumption that the taking of an item by the police without a warrant violates s. 8 of the *Charter* unless the claimant has no reasonable expectation of privacy in the item or has waived his *Charter* rights. In assessing whether a claimant has a reasonable expectation of privacy in an item that is taken, courts must consider the totality of the circumstances. In particular, they must determine (1) the subject matter of the alleged seizure; (2) whether the claimant had a direct interest in the subject matter; (3) whether the claimant had a subjective expectation of privacy in the subject matter; and (4) whether this subjective expectation of privacy was objectively reasonable.

In this case, the accused had a reasonable expectation of privacy in the shared computer. The subject matter of the seizure was the computer, and ultimately the data it contained about the accused's usage, including the files he accessed, saved and deleted. When the police seize a computer, they not only deprive individuals of control over intimate data in which they have a reasonable expectation of privacy, they also ensure that such data remains preserved and thus subject to potential future state inspection. Thus, seizing the computer interfered with the accused's expectation of privacy in its informational content. The accused undoubtedly had a direct interest

and subjective expectation of privacy in the computer and the data it contained, as he used the computer and stored personal data on it. Finally, the accused's subjective expectation of privacy was objectively reasonable. While control is relevant in assessing whether a subjective expectation of privacy is objectively reasonable, it is not an absolute indicator of a reasonable expectation of privacy, nor is a lack of control fatal to a privacy interest. In this case, the accused's control over the computer was limited, as compared to someone who is the sole user of a personal computer. However, shared control does not mean no control. By choosing to share a computer with others, people do not relinquish their right to be protected from the unreasonable seizure of it by the state. Similarly, ownership is relevant, but not determinative, in assessing whether a subjective expectation of privacy is objectively reasonable. The joint ownership of the computer does not render the accused's subjective expectation of privacy objectively unreasonable.

While it is reasonable to ask citizens to bear the risk that a co-user of their shared computer may access their data on it, and even perhaps discuss this data with the police, it is not reasonable to ask them to bear the risk that the co-user could consent to the police taking this computer. By choosing to share their computers with friends and family, Canadians are not required to give up their *Charter* protection from state interference in their private lives, and to accept that their friends and family can unilaterally authorize police to take things that they share. In light of the deeply intimate nature of information that can be found on a personal computer, the accused's subjective expectation of privacy in this case was objectively reasonable.

His spouse's consent could not nullify his reasonable expectation of privacy in the computer data. Because someone is always likely to have a reasonable expectation of privacy in a personal computer, the taking of a personal computer without a warrant and without valid consent will constitute a presumptively unreasonable seizure.

The presumptive warrant requirement for seizures captured by s. 8 of the *Charter* is not triggered if an accused's *Charter* rights were waived. However, waiver by one rights holder does not constitute waiver for all rights holders. To hold that there is no seizure within the meaning of the *Charter* when a party with an equal and overlapping privacy interest provides consent would effectively permit the consenting party to waive the privacy rights of the other parties. While the accused's spouse undoubtedly had constitutionally protected privacy interests in the shared computer, this did not entitle her to relinquish the accused's constitutional right to be left alone. The accused had a reasonable expectation of privacy in the shared computer and his rights had not been waived. Accordingly, the taking of the computer by the police constituted a seizure within the meaning of s. 8 of the *Charter*. This warrantless seizure was not reasonable because it was not authorized by any law. It therefore violated the accused's rights under s. 8 of the *Charter*.

The *Charter*-infringing state conduct in this case was serious. The police service's specialized cyber-crime unit should have been aware of the unique and heightened privacy interests in computers and should have known that a third party cannot waive another party's *Charter* rights. Because there were multiple serious

Charter breaches throughout the investigative process, the police conduct undermined public confidence in the rule of law. While society's interest in the adjudication of this case on its merits was strong and the alleged offences were serious, given the seriousness of the state conduct and its impact on the accused's *Charter*-protected interests, the admission of the evidence would bring the administration of justice into disrepute.

Per **Moldaver** J.: There is agreement with the majority that the accused had a reasonable expectation of privacy in the shared computer and that in the circumstances, its warrantless seizure constituted a breach of the accused's rights under s. 8 of the *Charter*, despite his spouse's consent. There is also agreement that the resulting evidence should be excluded under s. 24(2).

While counsel for the accused here did not challenge the police entry into the home and conceded that police entry into a shared residence is not a search, the importance of the entry provides a compelling reason to consider this issue. A possible alternate basis for concluding that the police entry in this case was lawful is that the police had the power to enter the shared residence at common law under the ancillary powers doctrine. The analysis under this doctrine, which is used to assess whether the police have the authority at common law to take an action that interferes with an individual's liberty or property, proceeds in two stages: whether the police conduct at issue falls within the general scope of their statutory or common law duties

and whether the conduct involves a justifiable use of police powers associated with that duty.

At the first stage, entering into a shared residence when invited to take a witness statement in connection with a criminal investigation falls within the scope of police duties. Entering a home to take a witness statement in connection with a criminal investigation furthers the police's mandate to encourage crime prevention within the community, apprehend criminals and assist victims of crime. At the second stage, the proposed power may well be a reasonably necessary interference with individuals' privacy interests in their homes. The ability of the police to enter into a home to take a statement when invited serves an important investigative function. Further, it may well be necessary for police to intrude on a co-resident's expectation of privacy in his or her home to do so.

In addition, the extent of the interference with the expectation of privacy occasioned by that action is minimal. When the police enter a home, they interfere with the expectation of privacy of all residents who did not consent to that entry. However, properly constrained, entering a home when invited by an occupant to take a witness statement is minimally intrusive on the other resident's privacy interests. Specifically, five constraints on the police entry power operate to minimize the extent of the interference with the expectation of privacy: (1) the police must offer the authorizing resident, and any other cooperating occupants, a suitable alternative interview location — if one is available — that does not potentially intrude upon the

reasonable expectations of privacy of co-residents in their home; (2) the purpose of the entry must be limited to taking a statement from the authorizing resident or one or more willing occupants in connection with a criminal investigation; (3) the police are only permitted to enter the home's common areas into which they have been invited; (4) the police can only enter if invited in by a resident with the authority to consent and that consent must be voluntary, informed and continuous; and (5) unless the police obtain the necessary grounds to take further investigative action, the duration of the entry must be limited to taking a statement from the authorizing resident or one or more willing occupants. These constraints act to limit the impact of the police entry on the non-consenting resident's privacy interests while allowing the police to engage in an important and necessary facet of their duty to investigate crime. This entry power may well be a reasonably necessary, and therefore justifiable, incursion on an individual's expectation of privacy.

Per **Côté** J.: There is agreement with the majority that the evidence should be excluded under s. 24(2) of the *Charter*, and therefore that the appeal should be allowed. However, there is disagreement that the issue of the entry into the home should not be addressed and that the police removal of the computer was unlawful.

The issue of whether the police can lawfully enter common areas of a shared home with the consent of one cohabitant should be addressed as it was argued by the parties and is relevant to the analysis pursuant to s. 24(2) of the *Charter*. One cohabitant can validly consent to a police entry into common areas of a shared

residence, obviating the need for a warrant. The alternative rule — that the police may enter the common areas of a shared home only if they obtain consent from each and every person who lives there — is entirely unworkable. It is not objectively reasonable for a cohabitant, who shares a residence with others, to expect to be able to veto another cohabitant's decision to allow the police to enter any areas of the home that they share equally. Other persons with overlapping privacy interests in and right to common spaces can validly permit third parties, including the police, to enter those spaces. To hold otherwise would be to interfere with the consenting cohabitant's liberty and autonomy interests with respect to those spaces. However, the ability of law enforcement officials to enter on the basis of consent is not without limits. The consenting person must have the authority to consent; the consent must be limited to shared places or things; the consent must be informed and voluntary; and the police must respect the limits of the consent, which is freely revocable at any point during the entry or search.

In this case, the accused's spouse permitted a police officer to enter the home she shared with the accused. Not only do the police have a common law power to enter a shared residence for the purpose of taking a statement, but there is no violation of s. 8 in any event, because the accused's expectation of privacy was not objectively reasonable in a context where a cohabitant, his spouse, provided her consent for the police to enter common areas of the home. The reason that the entry by the police was lawful was not because the accused's spouse waived the accused's *Charter* rights. The accused's spouse did not waive anyone's rights except her own.

In the context of a shared home, the scope of the accused's reasonable expectation of privacy was limited in recognition of the fact that his spouse was a first-party rights holder who should be permitted to freely exercise her rights of access and control over common areas. The accused's reasonable expectation of privacy was not sufficiently capacious to afford constitutional protection against his spouse's decision to give the police access to common areas, particularly since he had no legal right to enter the home at the time of the police entry.

As with the police entry into the home, the accused's expectation of privacy with respect to the computer he shared with his spouse was attenuated by the realities of joint ownership and use. It was not objectively reasonable for him to expect that his spouse could not exercise her own authority and control over the computer to consent to a seizure by the police. The subject matter of the seizure, that is, what the police were really after through the seizure of the computer, was only the physical device, not the data itself. At no point were the computer's contents ever searched or examined by the police prior to obtaining a warrant. The law enforcement objective in seizing the computer was simply to preserve potential evidence. The seizure did nothing to interfere with the accused's expectation of privacy in its informational content because that content remained private. When the subject matter of the seizure is properly defined as the physical computer, it is clear that it was not objectively reasonable for the accused to expect that he could prohibit his spouse from exercising her own authority and control over the computer to consent to a police seizure. Further, it is not objectively reasonable for the accused's subjective

expectation of privacy to act as a veto on his spouse's ability to exercise her own property rights in the physical device. The scope of the accused's s. 8 protection is limited by the fact that the computer was jointly owned and used by another person. His spouse's rights in the computer — including her property rights in the device and her right to waive her own privacy protections — would be rendered meaningless if the accused could prevent her from consenting to the physical removal of the computer.

Even though the entry into the home and the seizure of the computer were both lawful, the evidence should still be excluded under s. 24(2) of the *Charter* based on the other violations of law in this case — specifically, the fact that the police failed to comply with ss. 489.1 and 490 of the *Criminal Code* by improperly detaining the computer and the fact that the search warrant was ultimately found to be invalid.

Cases Cited

By Karakatsanis J.

Applied: *R. v. Cole*, 2012 SCC 53, [2012] 3 S.C.R. 34; **referred to:** *Hunter v. Southam Inc.*, [1984] 2 S.C.R. 145; *R. v. Edwards*, [1996] 1 S.C.R. 128; *R. v. Dyment*, [1988] 2 S.C.R. 417; *R. v. Borden*, [1994] 3 S.C.R. 145; *R. v. Wills* (1992), 12 C.R. (4th) 58; *R. v. Monney*, [1999] 1 S.C.R. 652; *R. v. Collins*, [1987] 1 S.C.R. 265; *R. v. Silveira*, [1995] 2 S.C.R. 297; *R. v. Tessling*, 2004 SCC 67, [2004] 3 S.C.R. 432; *R. v. T. (R.M.J.)*, 2014 MBCA 36, 311 C.C.C. (3d) 185; *R. v. Clarke*, 2017

BCCA 453, 357 C.C.C. (3d) 237; *R. v. Squires*, 2005 NLCA 51, 199 C.C.C. (3d) 509; *R. v. Marakah*, 2017 SCC 59, [2017] 2 S.C.R. 608; *R. v. Spencer*, 2014 SCC 43, [2014] 2 S.C.R. 212; *R. v. Patrick*, 2009 SCC 17, [2009] 1 S.C.R. 579; *R. v. Ward*, 2012 ONCA 660, 112 O.R. (3d) 321; *R. v. Wong*, [1990] 3 S.C.R. 36; *R. v. Vu*, 2013 SCC 60, [2013] 3 S.C.R. 657; *R. v. Plant*, [1993] 3 S.C.R. 281; *R. v. Morelli*, 2010 SCC 8, [2010] 1 S.C.R. 253; *R. v. Fearon*, 2014 SCC 77, [2014] 3 S.C.R. 621; *R. v. Buhay*, 2003 SCC 30, [2003] 1 S.C.R. 631; *R. v. Duarte*, [1990] 1 S.C.R. 30; *R. v. M. (M.R.)*, [1998] 3 S.C.R. 393; *R. v. Gomboc*, 2010 SCC 55, [2010] 3 S.C.R. 211; *R. v. Belnavis*, [1997] 3 S.C.R. 341; *R. v. Orlandis-Habsburgo*, 2017 ONCA 649, 352 C.C.C. (3d) 525; *R. v. Grant*, 2009 SCC 32, [2009] 2 S.C.R. 353; *R. v. Tse*, 2012 SCC 16, [2012] 1 S.C.R. 531; *R. v. Paterson*, 2017 SCC 15, [2017] 1 S.C.R. 202.

By Moldaver J.

Applied: *R. v. Waterfield*, [1963] 3 All E.R. 659; **referred to:** *R. v. Evans*, [1996] 1 S.C.R. 8; *R. v. Spencer*, 2014 SCC 43, [2014] 2 S.C.R. 212; *R. v. Tessling*, 2004 SCC 67, [2004] 3 S.C.R. 432; *R. v. Bartle*, [1994] 3 S.C.R. 173; *R. v. Grant*, [1993] 3 S.C.R. 223; *R. v. Collins*, [1987] 1 S.C.R. 265; *R. v. Stillman*, [1997] 1 S.C.R. 607; *Dedman v. The Queen*, [1985] 2 S.C.R. 2; *R. v. Mann*, 2004 SCC 52, [2004] 3 S.C.R. 59; *Cloutier v. Langlois*, [1990] 1 S.C.R. 158; *R. v. Godoy*, [1999] 1 S.C.R. 311; *R. v. Kang-Brown*, 2008 SCC 18, [2008] 1 S.C.R. 456; *R. v. MacDonald*, 2014 SCC 3, [2014] 1 S.C.R. 37; *R. v. Bui*, 2002 BCSC 289, [2002] B.C.J. No. 3185 (QL); *R. v. Caslake*, [1998] 1 S.C.R. 51; *R. v. Jones*, 2011 ONCA 632, 107 O.R. (3d)

241; *R. v. Borden*, [1994] 3 S.C.R. 145; *R. v. Wills* (1992), 12 C.R. (4th) 58; *Hunter v. Southam Inc.*, [1984] 2 S.C.R. 145; *R. v. M. (M.R.)*, [1998] 3 S.C.R. 393; *R. v. Simmons*, [1988] 2 S.C.R. 495.

By Côté J.

Distinguished: *R. v. Cole*, 2012 SCC 53, [2012] 3 S.C.R. 34; **referred to:** *R. v. Law*, 2002 SCC 10, [2002] 1 S.C.R. 227; *R. v. Edwards*, [1996] 1 S.C.R. 128; *R. v. Marakah*, 2017 SCC 59, [2017] 2 S.C.R. 608; *R. v. Quesnelle*, 2014 SCC 46, [2014] 2 S.C.R. 390; *R. v. M. (M.R.)*, [1998] 3 S.C.R. 393; *R. v. Patrick*, 2009 SCC 17, [2009] 1 S.C.R. 579; *R. v. Reeves*, 2017 ONCA 365, 350 C.C.C. (3d) 1; *R. v. Clarke*, 2017 BCCA 453, 357 C.C.C. (3d) 237; *R. v. T. (R.M.J.)*, 2014 MBCA 36, 311 C.C.C. (3d) 185; *R. v. Squires*, 2005 NLCA 51, 199 C.C.C. (3d) 509; *R. v. Morelli*, 2010 SCC 8, [2010] 1 S.C.R. 253; *R. v. Vu*, 2013 SCC 60, [2013] 3 S.C.R. 657; *R. v. Buhay*, 2003 SCC 30, [2003] 1 S.C.R. 631; *R. v. Mercer* (1992), 7 O.R. (3d) 9; *R. v. Stevens*, 2011 ONCA 504, 106 O.R. (3d) 241; *R. v. Ward*, 2012 ONCA 660, 112 O.R. (3d) 321; *R. v. Spencer*, 2014 SCC 43, [2014] 2 S.C.R. 212; *R. v. Belnavis* (1996), 29 O.R. (3d) 321, aff'd [1997] 3 S.C.R. 341; *R. v. Garcia-Machado*, 2015 ONCA 569, 126 O.R. (3d) 737; *R. v. Grant*, 2009 SCC 32, [2009] 2 S.C.R. 353; *R. v. Villaroman*, 2018 ABCA 220, 363 C.C.C. (3d) 141.

Statutes and Regulations Cited

Canadian Charter of Rights and Freedoms, ss. 8, 24(2).

Criminal Code, R.S.C. 1985, c. C-46, ss. 487.11, 489(2), 489.1, 490.

Police Services Act, R.S.O. 1990, c. P.15, s. 42(1).

Authors Cited

Fontana, James A., and David Keeshan. *The Law of Search and Seizure in Canada*, 10th ed. Toronto: LexisNexis, 2017.

Stewart, Hamish. "Normative Foundations for Reasonable Expectations of Privacy" (2011), 54 *S.C.L.R.* (2d) 335.

APPEAL from a judgment of the Court of Appeal for Ontario (LaForme, Rouleau and Brown JJ.A.), 2017 ONCA 365, 350 C.C.C. (3d) 1, 38 C.R. (7th) 87, [2017] O.J. No. 3038 (QL), 2017 CarswellOnt 7617 (WL Can.), setting aside a decision of Guay J., 2015 ONCJ 724, [2015] O.J. No. 6750 (QL), 2015 CarswellOnt 19460 (WL Can.). Appeal allowed.

Brad Greenshields and *Julianna Greenspan*, for the appellant.

Frank Au, *Michelle Campbell* and *Randy Schwartz*, for the respondent.

James C. Martin and *Eric Marcoux*, for the intervener the Director of Public Prosecutions.

Ann Ellefsen-Tremblay and *Nicolas Abran*, for the intervener the Director of Criminal and Penal Prosecutions.

Written submissions only by *Daniel M. Scanlan*, for the intervener the Attorney General of British Columbia.

Michael Lacy and *Bryan Badali*, for the intervener the Criminal Lawyers' Association (Ontario).

Jill R. Presser and *Kate Robertson*, for the intervener the Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic.

The judgment of Wagner C.J. and Abella, Karakatsanis, Gascon, Brown, Rowe and Martin JJ. was delivered by

KARAKATSANIS J. —

I. Overview

[1] Police discovered child pornography on a home computer that the accused, Thomas Reeves, shared with his spouse. His spouse consented to the police entry into the home and the taking of the computer from a shared space. The officer did not have a warrant. Reeves claims that the police obtained the child pornography evidence in a manner that infringed his rights under s. 8 of the *Canadian Charter of*

Rights and Freedoms, and that it should be excluded under s. 24(2) of the *Charter*. The key issue in this case is whether the police officer could rely on the consent of Reeves' spouse to take the shared computer from their home.

[2] Section 8 of the *Charter* protects all Canadians against unreasonable search and seizure. In assessing whether s. 8 has been infringed, courts consider whether an individual's privacy interests must give way to the state's interest in law enforcement. The challenge of s. 8 is that courts are most often called on to interpret its scope in cases, like this, where the police have found evidence that the claimant has engaged in criminal activity. Child pornography offences are serious and insidious, and there is a strong public interest in investigating and prosecuting them. However, in applying s. 8, the question is not whether the claimant broke the law, but rather whether the police exceeded the limits of the state's authority. The answer in this case impacts not only Reeves, but also the privacy rights of *all* Canadians in shared personal computers.

[3] The judge hearing the *Charter* application concluded that the police infringed Reeves' s. 8 *Charter* rights, and excluded the child pornography evidence under s. 24(2) (2015 ONCJ 724). Reeves was acquitted at trial. The Court of Appeal did not agree with the application judge that the police infringed s. 8 when they took the computer with the consent of Reeves' spouse (2017 ONCA 365, 350 C.C.C. (3d) 1). It allowed the appeal, admitted the evidence, and ordered a new trial.

[4] I agree with the application judge that the police infringed Reeves' *Charter* rights when they took the computer from his home, and that the child pornography evidence should be excluded. Although the computer was shared, Reeves maintained a reasonable expectation of privacy in it. The consent of Reeves' spouse did not nullify his reasonable expectation of privacy, or operate to waive his *Charter* rights in the computer. The warrantless seizure of the computer and the search of it without a valid warrant were unreasonable, and the admission of the child pornography evidence would bring the administration of justice into disrepute.

[5] I would allow the appeal and restore the acquittal.

II. Background

[6] Thomas Reeves, the appellant, shared a home with Nicole Gravelle, his common-law spouse. They were joint titleholders and had lived with their two daughters in this home for ten years. In 2011, Reeves was charged with domestic assault following an altercation with Gravelle and her sister. After this incident, a no-contact order was issued which prohibited Reeves from visiting the family home without Gravelle's prior, written, and revocable consent. In October 2012, Gravelle contacted Reeves' probation officer to withdraw her consent. She also reported that she and her sister had found what they believed to be child pornography on the home computer. They had found it in 2011.

[7] Later that day, a police officer arrived at the family home without a warrant. Gravelle allowed the officer to enter. Gravelle signed a consent form authorizing the officer to take the home computer, which was located in the basement, a shared space in the home. The officer testified that he sought Gravelle's consent because he did not believe he had reasonable grounds to obtain a warrant to search the home and seize the computer. The computer was owned and used by both spouses. Reeves was in custody on unrelated charges when the computer was taken by the police.

[8] The police detained the computer without a warrant for more than four months, but did not search it during this time. They failed to report the seizure of the computer to a justice, as required by s. 489.1 of the *Criminal Code*, R.S.C. 1985, c. C-46, during this period. In February 2013, the police finally obtained a warrant to search the computer and executed it two days later. The police found 140 images and 22 videos of child pornography on the computer. Reeves was charged with possessing and accessing child pornography.

[9] The application judge, Guay J., concluded that the police had violated Reeves' s. 8 *Charter* rights. First, the warrantless search of the home and seizure of the home computer breached s. 8. While the police obtained the consent of Reeves' spouse to enter the home and remove the home computer, a third party cannot waive another party's *Charter* rights. Reeves had a reasonable expectation of privacy in the home and the home computer, and he did not consent to the entry of the police and

the removal of the computer. Second, the police failed to comply with ss. 489.1 and 490 of the *Criminal Code* by detaining the computer for over four months without reporting its seizure to a justice. Third, the information to obtain a search warrant (ITO) was goal-oriented, misleading, unbalanced, and unfair, and the search warrant should not have been granted. The application judge excluded the computer evidence under s. 24(2) of the *Charter* given "the flagrant disregard of the accused's section 8 *Charter* rights" (para. 49). At trial, Reeves was acquitted.

[10] The Court of Appeal allowed the Crown's appeal from the acquittal, set aside the exclusionary order, and ordered a new trial. LaForme J.A., writing for the court, determined that the entry of the police into the home and the taking of the home computer did not violate Reeves' s. 8 rights. He explained that, while one resident cannot waive the *Charter* rights of another, co-residency is relevant in assessing a claimant's expectation of privacy. In this case, Reeves' expectation of privacy in the shared spaces of the home and the computer was "greatly diminished" (para. 59). Therefore, it was reasonable for him to expect that Gravelle would be "able to consent to police entry into the common areas of the home or to the taking of the shared computer" (para. 62). However, the Court of Appeal agreed with the application judge that the continued detention of the computer and the subsequent computer search both violated s. 8 of the *Charter*. While noting that this was a "borderline case", the Court of Appeal concluded that the evidence should not have been excluded under s. 24(2) (para. 109).

III. Analysis

A. *Section 8 of the Charter*

[11] Under s. 8 of the *Charter*, "[e]veryone has the right to be secure against unreasonable search or seizure." The purpose of this provision is "to protect individuals from unjustified state intrusions upon their privacy" (*Hunter v. Southam Inc.*, [1984] 2 S.C.R. 145, at p. 160). The s. 8 analysis is geared towards determining "whether in a particular situation the public's interest in being left alone by government must give way to the government's interest in intruding on the individual's privacy in order to advance its goals, notably those of law enforcement" (pp. 159-60).

[12] Section 8 of the *Charter* is only engaged if the claimant has a reasonable expectation of privacy in the place or item that is inspected or taken by the state (*R. v. Cole*, 2012 SCC 53, [2012] 3 S.C.R. 34, at paras. 34 and 36). To determine whether the claimant has a reasonable expectation of privacy, courts examine "the totality of the circumstances" (*R. v. Edwards*, [1996] 1 S.C.R. 128, at paras. 31 and 45(5)).

[13] Further, "the essence of a seizure under s. 8 is the taking of a thing from a person by a public authority without that person's consent" (*R. v. Dyment*, [1988] 2 S.C.R. 417, at p. 431 (emphasis added)). In contrast, valid consent acts as a waiver of the claimant's s. 8 rights. In such cases, there is no search or seizure within the meaning of the *Charter*, even though the claimant would ordinarily enjoy a

reasonable expectation of privacy in the thing the police have taken or inspected (*R. v. Borden*, [1994] 3 S.C.R. 145, at pp. 160-62; *R. v. Wills* (1992), 12 C.R. (4th) 58 (Ont. C.A.), at p. 81).

[14] If s. 8 of the *Charter* is engaged, "the court must then determine whether the search or seizure was reasonable" (*Cole*, at para. 36). A warrantless search or seizure is presumptively unreasonable, and the Crown bears the burden of rebutting this presumption (*Hunter*, at p. 161; *R. v. Monney*, [1999] 1 S.C.R. 652, at para. 29). A search or seizure is reasonable "if it is authorized by law, if the law itself is reasonable and if the manner in which the search [or seizure] was carried out is reasonable" (*R. v. Collins*, [1987] 1 S.C.R. 265, at p. 278).

[15] The only s. 8 issues raised before this Court are whether the police infringed Reeves' *Charter* rights by (1) entering the shared home without a warrant; and (2) taking the shared computer without a warrant. The Court of Appeal agreed with the application judge that the police infringed Reeves' *Charter* rights by detaining the computer and subsequently searching it, and the Crown now concedes these points.

[16] In his written submissions, the appellant, Reeves, argues that the search of his home and the seizure of the home computer violated his rights under s. 8 of the *Charter*. He had a reasonable expectation of privacy in the home and computer and his spouse's consent did not render the police's conduct *Charter*-compliant. Concluding otherwise would be contrary to this Court's rejection of the third-party

consent doctrine in *Cole*. While Reeves may not have had exclusive control over the home and computer, control does not need to be exclusive to support a reasonable expectation of privacy. By assuming the reasonable risks of shared living, a person does not assume the risk that the police can enter a shared home and seize its contents at the sole discretion of a co-resident.

[17] In his oral submissions, Reeves' counsel maintained that the seizure of the computer violated the *Charter*, but submitted that the police entry into the home did not.

[18] The respondent, Her Majesty the Queen, submits that the police did not infringe the *Charter* by entering the home and taking the home computer. The *Charter* permits police to access shared places without a warrant when they act on the consent of a party who has a privacy interest in the place that is equal to and overlapping with the privacy interests of the other co-residents. A consent search or seizure is not a "search or seizure" within the meaning of the *Charter*. It is not reasonable for one cohabitant to expect that his or her right to exclude others will trump another cohabitant's right to admit others. While one cohabitant cannot waive another cohabitant's *Charter* rights by providing consent, it is reasonable to recognize that a cohabitant can permit police access in her own right.

(1) <u>The Police Entry</u>

[19] The application judge concluded that "the officer's entry into a private residence without the consent of both owners or occupants constituted a search of those premises for section 8 *Charter* purposes" (para. 11). He noted the police officer entered the shared home for the purpose of obtaining the computer. In his view, Gravelle's consent did not render the officer's entry *Charter*-compliant because a third party cannot waive another party's *Charter* rights. The Court of Appeal disagreed, and concluded that Gravelle could consent to the search of shared areas of the home.

[20] While the lower courts assessed whether the police entry into the home violated the *Charter*, given my conclusions on the other issues raised in this case, it is not necessary for me to decide whether the entry into the home constituted a separate violation of Reeves' rights. Indeed, in oral submissions, Reeves' counsel submitted that the entry was lawful.

[21] Even if the officer had lawfully been in the home, this would not make the seizure of the computer lawful. Section 489(2) of the *Criminal Code* provides that a police officer "who is lawfully present in a place pursuant to a warrant or otherwise in the execution of duties may, without a warrant, seize any thing that the officer believes on reasonable grounds" was used in the commission of an offence or would afford evidence of an offence. Here, however, this section was not available; the officer testified that he asked for Gravelle's consent to seize the computer *because* he did not believe he had grounds to obtain a warrant. Irrespective of whether the officer

was "lawfully present" in the home, by his own admission, he did not have "reasonable grounds" to seize the computer.

[22] Therefore, in this case, the legality of the police entry does not affect the legality of the taking of the computer. As such, I proceed on the assumption that the entry was lawful.

[23] In any event, I do not think it prudent to explore this issue in the absence of full submissions, given that many competing considerations arise in determining whether and when police entry into a shared home on the consent of one resident violates the *Charter*.

[24] Of course, the law has long recognized the prime importance of privacy within our homes (*R. v. Silveira*, [1995] 2 S.C.R. 297, at para. 140; see also *R. v. Tessling*, 2004 SCC 67, [2004] 3 S.C.R. 432, at para. 22). However, if a resident cannot consent to police entry to a shared home without the consent of all the other residents, it could undermine the dignity and autonomy of that resident — especially for a victim of a crime.

[25] Several provincial appellate courts have concluded that a resident has the right to permit police entry into common areas of the home without the consent of all other residents (*R. v. T. (R.M.J.)*, 2014 MBCA 36, 311 C.C.C. (3d) 185, at paras. 41-52; *R. v. Clarke*, 2017 BCCA 453, 357 C.C.C. (3d) 237, at paras. 55-56 and 62-63; *R. v. Squires*, 2005 NLCA 51, 199 C.C.C. (3d) 509, at para. 34). However, without

deciding the issue, police entry into a shared home with the consent of only one resident raises a number of important questions. Would police also be authorized to search common areas of the home? Should the privacy interests of other residents affect the authority to seize evidence, even if in plain view? Could another resident who is present object to the police entry? What if the officers seek entry for the specific purpose of investigating one of the other residents?

[26] In short, the issue of whether police entry into a shared home with the consent of one resident violates the *Charter* raises complex questions that require a considered response. They are best answered in a case that directly turns on this issue, with the benefit of full submissions.

(2) The Taking of the Shared Computer

[27] The key issue in this case is whether the police violated Reeves' *Charter* rights when they took the shared computer without a warrant but with Gravelle's consent. There is a presumption that the taking of an item by the police without a warrant violates s. 8 of the *Charter* unless the claimant has no reasonable expectation of privacy in the item or has waived his *Charter* rights. I start by assessing whether Reeves had a reasonable expectation of privacy in the shared computer.

[28] In assessing whether a claimant has a reasonable expectation of privacy in an item that is taken, courts must consider "the totality of the circumstances" (*Edwards*, at para. 45(5)). In particular, they must determine (1) the subject matter of

the alleged seizure; (2) whether the claimant had a direct interest in the subject matter; (3) whether the claimant had a subjective expectation of privacy in the subject matter; and (4) whether this subjective expectation of privacy was objectively reasonable (*Cole*, at para. 40; *R. v. Marakah*, 2017 SCC 59, [2017] 2 S.C.R. 608, at para. 11). The reasonable expectation of privacy standard is normative, rather than descriptive (*Tessling*, at para. 42; *R. v. Spencer*, 2014 SCC 43, [2014] 2 S.C.R. 212, at para. 18; *R. v. Patrick*, 2009 SCC 17, [2009] 1 S.C.R. 579, at para. 14). The question is whether the privacy claim must "be recognized as beyond state intrusion absent constitutional justification if Canadian society is to remain a free, democratic and open society" (*R. v. Ward*, 2012 ONCA 660, 112 O.R. (3d) 321, at para. 87, per Doherty J.A.). Further, the inquiry must be framed in neutral terms — "[t]he analysis turns on the privacy of the area or the thing being searched and the impact of the search on its target, not the legal or illegal nature of the items sought" (*Spencer*, at para. 36; see also *R. v. Wong*, [1990] 3 S.C.R. 36, at pp. 49-50; *Patrick*, at para. 32).

[29] Turning first to the subject matter of the alleged seizure, in oral argument, the Crown distinguished between the taking of the physical hardware and a subsequent search of the computer's data, which, in this case, occurred pursuant to a search warrant. However, this Court has held that the subject matter must not be defined "narrowly in terms of the physical acts involved or the physical space invaded, but rather by reference to the nature of the privacy interests potentially compromised by the state action" (*Marakah*, at para. 15, citing *Ward*, at para. 65).

The guiding question is "what the police were really after" (*Marakah*, at para. 15, citing *Ward*, at para. 67).

[30] Here, the subject matter of the seizure was the computer, and ultimately the data it contained about Reeves' usage, including the files he accessed, saved and deleted. I acknowledge that the police could not actually search the data until they obtained a warrant (see *R. v. Vu*, 2013 SCC 60, [2013] 3 S.C.R. 657, at paras. 3 and 49). Nevertheless, while the privacy interests engaged by a seizure may be different from those engaged by a search, Reeves' informational privacy interests in the computer data were still implicated by the seizure of the computer. When police seize a computer, they not only deprive individuals of *control* over intimate data in which they have a reasonable expectation of privacy, they also ensure that such data remains *preserved* and thus subject to potential future state inspection.

[31] Thus, I disagree with the Court of Appeal's assertion that "[s]eizing the computer did not interfere with Reeves' heightened expectation of privacy in its informational content; it did not imperil any of his legitimate interests, beyond mere property rights" (para. 61). Clearly, the police were not after the physical device (to collect fingerprints on it, for example), but rather sought to preserve and permit access to the data it contained. To focus exclusively on the property rights at issue (that is, on Reeves' interest in *the computer*) neglects the important privacy rights in *the data* that are also engaged by the seizure.

[32] Reeves undoubtedly had a direct interest and subjective expectation of privacy in the home computer and the data it contained. He used the computer and stored personal data on it (see *Cole*, at para. 43). The computer was password-protected. The threshold for establishing a subjective expectation of privacy is low (*Marakah*, at para. 22).

[33] The final question is whether Reeves' subjective expectation of privacy was objectively reasonable. Section 8 seeks to protect "a biographical core of personal information which individuals in a free and democratic society would wish to maintain and control from dissemination to the state" (*R. v. Plant*, [1993] 3 S.C.R. 281, at p. 293). Although a seizure of a computer may be less intrusive than a search of its contents, both engage important privacy interests when the purpose of the seizure is to gain access to the data on the computer. Privacy includes "control over, access to and use of information" (*Spencer*, at para. 40). Thus, the personal or confidential nature of the data that is preserved and potentially available to police through the seizure of the computer is relevant in determining whether the claimant has a reasonable expectation of privacy in it (*Marakah*, at para. 32).

[34] Personal computers contain highly private information. Indeed, "[c]omputers often contain our most intimate correspondence. They contain the details of our financial, medical, and personal situations. They even reveal our specific interests, likes, and propensities" (*R. v. Morelli*, 2010 SCC 8, [2010] 1 S.C.R. 253, at para. 105; see also *Vu*, at paras. 40-41; *Cole*, at paras. 3 and 47-48).

Computers act as portals — providing access to information stored in many different locations (*Vu*, at para. 44; *R. v. Fearon*, 2014 SCC 77, [2014] 3 S.C.R. 621, at paras. 131-32). They "contain information that is automatically generated, often unbeknownst to the user" (*Vu*, at para. 42). They retain information that the user may think has been deleted (*Vu*, at para. 43). By seizing the computer, the police deprived Reeves of control over this highly private information, including the opportunity to delete it. They also obtained the means through which to access this information. Indeed, these are the reasons why the police seized the computer.

[35] Given the unique privacy concerns associated with computers, this Court has held that specific, prior judicial authorization is required to search a computer (*Vu*, at para. 2) and that police officers cannot search cell phones incident to arrest unless certain conditions are met (*Fearon*, at para. 83). The unique and heightened privacy interests in personal computer data clearly warrant strong protection, such that specific, prior judicial authorization is presumptively required to seize a personal computer from a home. This presumptive rule fosters respect for the underlying purpose of s. 8 of the *Charter* by encouraging the police to seek lawful authority, more accurately accords with the expectations of privacy Canadians attach to their use of personal home computers and encourages more predictable policing.

[36] The Crown's submissions and the Court of Appeal's analysis emphasize the fact that Reeves shared control over, and access to, his computer with others. I accept that control is also relevant in assessing whether a subjective expectation of

privacy is objectively reasonable (*Marakah*, at para. 38). Reeves' control over the computer was limited, as compared to someone who is the sole user of a personal computer. He shared the computer with his spouse and, at the time of the seizure, he could only access the home (where the computer was stored) with her consent, which had been revoked. As this Court has recognized, "in certain circumstances, sharing control of subject matter diminishes an individual's privacy interest therein" (*Marakah*, at para. 68). I agree with the Court of Appeal that Reeves' shared control over his home computer diminished his privacy interest in it.

[37] That said, "control is not an absolute indicator of a reasonable expectation of privacy, nor is lack of control fatal to a privacy interest" (*Marakah*, at para. 38). On numerous occasions, this Court has recognized a reasonable expectation of privacy in places and things that are not exclusively under the claimant's control. In *R. v. Buhay*, 2003 SCC 30, [2003] 1 S.C.R. 631, it held that a person had a reasonable expectation of privacy in a bus depot locker where he had stored and locked belongings, even though a company owned the lockers and could access them at any time (paras. 22-23). In *Cole*, it held that an employee had a reasonable expectation of privacy in the data he stored on his work computer, even though "both policy and technological reality deprived him of exclusive control over — and access to — the personal information he chose to record on it" (para. 54; see also *Marakah*, at paras. 38-45). Shared control does not mean *no* control. By choosing to share a computer with others, people do not relinquish their right to be protected from the unreasonable seizure of it.

[38] In any event, lack of control is not fatal to finding a reasonable expectation of privacy (*Marakah*, at para. 38). As Moldaver J. stated in *Marakah*, "[w]here a loss of control over the subject matter is involuntary, such as where a person is in police custody or the subject matter is stolen from the person by a third party, then a reasonable expectation of personal privacy may persist" (para. 130). Here, Reeves was in police custody when the computer was seized and he was restrained from accessing the house by court order. At no point did Reeves voluntarily relinquish control of his personal computer. Any resulting lack of control over the computer therefore cannot be said to be voluntary.

[39] Like control, ownership is relevant, but not determinative, in assessing whether a subjective expectation of privacy is objectively reasonable (*Edwards*, at para. 45(6)(iii); *Cole*, at para. 51). The joint ownership of the computer does not render Reeves' subjective expectation of privacy objectively unreasonable. Indeed, in *Cole*, this Court concluded that the accused had a reasonable expectation of privacy in a work computer, even though the device and the data were owned *solely* by his employer (paras. 50-51 and 58).

(3) Gravelle's Consent to the Police Seizure of the Shared Computer

[40] The Crown further submits that, because Reeves' spouse had an equal and overlapping privacy interest in the computer, its removal with her consent did not constitute a "seizure" within the meaning of the *Charter*. In the Crown's view, it is reasonable to recognize that a co-user of a device can permit police access in her own

right, so a claimant's reasonable expectation of privacy is not violated when this right is exercised. Similarly, the Court of Appeal held that "[i]t was not reasonable for Reeves to expect [his spouse] would not be able to consent to . . . the taking of the shared computer" (para. 62). Effectively, these arguments mean either that Reeves had *no* reasonable expectation of privacy in the computer when it was taken by the police, or that his spouse's consent operated to waive Reeves' *Charter* rights. I will deal with these two propositions in turn.

[41] I cannot agree with the first proposition — that Reeves had no reasonable expectation of privacy in the computer. The consent of Reeves' spouse cannot nullify a reasonable expectation of privacy that he would otherwise have in the shared computer. Admittedly, when we share a computer with other people, we take the risk that they will access information we hoped to keep private. They may wish to share the information they find with others, including the police. But, as noted above, the reasonable expectation of privacy standard is normative, not descriptive. The question is not which risks the claimant has taken, but which risks should be imposed on him in a free and democratic society.

[42] Thus, in *R. v. Duarte*, [1990] 1 S.C.R. 30, this Court concluded that the surreptitious electronic surveillance of a conversation by the police without a warrant violated s. 8 of the *Charter*, even if one of the participants in the conversation had consented to the surveillance. In reaching this conclusion, the Court distinguished between the "tattletale" risk (the risk that someone will tell the police what you said)

and the risk that someone will consent to the police making an electronic record of your words (p. 48). The Court concluded that "[t]hese risks are of a different order of magnitude" — the tattletale risk is one that is reasonable to ask citizens to bear in a free and democratic society, whereas the surveillance risk is not (p. 48.).

[43] Similarly, while it is reasonable to ask citizens to bear the risk that a co-user of their shared computer may access their data on it, and even perhaps discuss this data with the police, it is not reasonable to ask them to bear the risk that the co-user could consent to the police *taking* this computer. In *Marakah*, this Court held that, when a claimant shares information with another person through a text message, he accepts the risk that this information may be disclosed to third parties. But that does not mean the claimant "give[s] up control over the information or his right to protection under s. 8" (para. 41).

[44] I cannot accept that, by choosing to share our computers with friends and family, we are required to give up our *Charter* protection from state interference in our private lives. We are not required to accept that our friends and family can unilaterally authorize police to take things that we share. The decision to share with others does not come at such a high price in a free and democratic society. As the intervener Criminal Lawyers' Association (Ontario) pointed out, such an approach to s. 8 may also disproportionately impact the privacy rights of low income individuals, who may be more likely to share a home computer.

[45] The Crown argues that failing to recognize Gravelle's right to consent to the taking of the computer grants insufficient protection to *her* privacy rights. It submits that privacy is not just a right to exclude, but also a right to admit. I disagree. Although the legitimate interests of third parties can, in some circumstances, attenuate a reasonable expectation of privacy (see *R. v. M. (M.R.)*, [1998] 3 S.C.R. 393, at paras. 31-34; *R. v. Gomboc*, 2010 SCC 55, [2010] 3 S.C.R. 211, at para. 109, per McLachlin C.J. and Fish J., dissenting, but not on this point), they cannot eliminate it. I would note that Gravelle was of course free to, and did, notify the police about what she saw on the computer. Further, while Gravelle also had a reasonable expectation of privacy in the computer data, she is not the claimant in this appeal. This Court has acknowledged that several parties can have a reasonable expectation of privacy in the same place or thing, and thus distinct s. 8 *Charter* claims (*R. v. Belnavis*, [1997] 3 S.C.R. 341, at paras. 19-25).

[46] The Crown also argues that rejecting its approach will prevent victims of crime who have received threatening or harassing text messages from showing them to the police. However, the issue of whether s. 8 of the *Charter* is engaged when a private citizen *offers* information or an item to the police in which another person may have a reasonable expectation of privacy does not arise in this case (see *Marakah*, at para. 50; *Dyment*, at p. 432; *R. v. Orlandis-Habsburgo*, 2017 ONCA 649, 352 C.C.C. (3d) 525, at paras. 21-35). Indeed, Gravelle did not bring the computer to the police, but rather signed a consent form authorizing them to take it. (She testified that she signed the form because she did not think she had a choice).

The issue of whether s. 8 is engaged when a citizen voluntarily brings an item to the police remains for another day. This case deals squarely with the *taking* of a computer by the state.

[47] In short, in light of the deeply intimate nature of information that can be found on a personal computer, Reeves' subjective expectation of privacy was objectively reasonable. His spouse's consent could not nullify his reasonable expectation of privacy in the computer data. Indeed, both the Crown and the Court of Appeal appear to have recognized that Reeves had a reasonable (although diminished) expectation of privacy. While Reeves' reasonable expectation of privacy in the computer was limited, given that he shared control over the computer with his spouse, it still suffices to trigger the protection of s. 8 of the *Charter* (see *Buhay*, at para. 22). Indeed, "[a] reasonable though diminished expectation of privacy is nonetheless a reasonable expectation of privacy, protected by s. 8 of the *Charter*" (*Cole*, at para. 9).

[48] I turn now to the alternative proposition that underlies the Crown's argument — that Reeves' *Charter* rights were waived by Gravelle's consent. The presumptive warrant requirement for seizures captured by s. 8 of the *Charter* is not triggered if Reeves' *Charter* rights were waived. The Crown's argument that there is no seizure within the meaning of the *Charter* when a party with an equal and overlapping privacy interest provides consent would effectively permit the consenting

party to waive the privacy rights of the other parties. This would be inconsistent with this Court's decision in *Cole*.

[49] This Court has long held that a *claimant* can waive his or her s. 8 *Charter* rights by consenting to a search or seizure (*Borden*, at p. 162). In addition, "[t]he force of the consent given must be commensurate with the significant effect which it produces" (*Borden*, at p. 162, citing *Wills*, at p. 72).

[50] In *Cole*, this Court considered whether this first-party consent doctrine should be extended to third parties. A school board had discovered child pornography files on the work computer of the accused, a teacher. The school board consented to a warrantless search and seizure of the computer by the police. The Crown argued that the taking of the computer and the examination of its data by the police complied with the *Charter* because the school board (a third party) could waive the accused's privacy rights. This Court rejected this argument, concluding that the doctrine of third-party consent should not be adopted in Canada, despite its acceptance in the United States. *Cole* explains that this doctrine would be "inconsistent with this Court's jurisprudence on *first party* consent", which requires consent to be "voluntarily given by the rights holder" and "based on sufficient information in his or her hands to make a meaningful choice" (paras. 77-78). The Court also held that the adoption of this doctrine in the United States was based on the type of "risk analysis" that had been rejected in *Duarte* (*Cole*, at paras. 75-76). The approach in *Cole* aligns with *Wong*, where this Court held that video surveillance of a hotel room violated the

occupant's rights under s. 8 of the *Charter*, even though the hotel management had agreed to the surveillance (pp. 42 and 52).

[51] The Crown endeavors to distinguish *Cole* by arguing that Gravelle is not a "true" third party because she had an equal and overlapping privacy interest in the computer. In contrast, in *Cole* the school board was a true third party because it did not have a privacy interest in the personal data the accused stored on the computer.

[52] In my view, *Cole* cannot be distinguished on this basis. There was no suggestion in *Cole* that the school could not consent to the search because it had no equal and overlapping privacy interests in the computer. While Gravelle undoubtedly has constitutionally-protected privacy interests in the shared computer, this does not entitle her to relinquish *Reeves'* constitutional right to be left alone (*Cole*, at para. 78; see also *Borden*, at p. 162). Waiver by one rights holder does not constitute waiver for all rights holders. This Court has set a high bar for first-party consent because waiving s. 8 rights has significant consequences (*Borden*, at p. 162). It insists that consent must be informed and voluntary because it wants to ensure that a waiver by the holder of a *Charter*-protected right is an expression of his or her free will. Allowing Gravelle's consent to waive Reeves' rights is completely inconsistent with this jurisprudence.

[53] As the intervener Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic aptly remarked, although the privacy interests of co-occupants or co-users over some shared premises or items may be "overlapping", it does not

follow that those interests are "coextensive". Indeed, where the consent giver and the claimant are not the same person, the s. 8 *Charter* inquiry does not concern the legitimacy of the former's privacy interests in the subject matter of the search or seizure, but rather the latter's expectation of privacy in it.

[54] I recognize that rejecting the Crown's approach may interfere with criminal investigations. But *Charter* rights often do. Judicial pre-authorization protects the unique and heightened privacy interests in home computers. At the same time, in appropriate circumstances, police may exercise other common law powers. For example, in exigent circumstances, police may conduct warrantless seizures (see s. 487.11 of the *Criminal Code*).

[55] Further, adopting the Crown's approach based on equal and overlapping privacy interests would raise practical issues. Before taking a computer, it may be difficult, if not impossible, for police to know whether the privacy interests in the data they are after are "equal and overlapping," and thus whether the taking would be *Charter*-compliant if the consent of only one user was obtained. Additionally, it is unclear how police could proceed if the target of the investigation were at home when the police arrived, and explicitly refused to consent to the computer's removal.

[56] For these reasons, the taking of the computer without Reeves' consent interfered with his reasonable expectation of privacy and thus constituted a seizure within the meaning of the *Charter* (*Cole*, at para. 59). A warrantless seizure is presumptively unreasonable, and the burden falls to the Crown to rebut this

presumption (*Hunter*, at p. 161; *Monney*, at para. 29). Indeed, because *someone* is always likely to have a reasonable expectation of privacy in a personal computer, the taking of a personal computer without a warrant and without valid consent will constitute a presumptively unreasonable seizure. The Crown has not endeavored to rebut the presumption in this case, as it relies on Gravelle's consent to show that no seizure occurred.

[57] Further, no statutory or common law authority could have justified the computer seizure in this case. If the police had had a warrant to search the home, *Vu* would have justified the seizure — but not the search — of the computer. In *Vu*, this Court held that, while a warrant to search a place generally entitles police to search anything they find in that place, this is not true for computers (paras. 23-24). Given the unique privacy concerns that computers raise, *Vu* specifies that

> [i]f, in the course of a warranted search, police come across a computer that may contain material for which they are authorized to search but the warrant does not give them specific, prior authorization to search computers, they may seize the device but must obtain further authorization before it is searched. [Emphasis added; para. 3; see also para. 49.]

As the police did not have a warrant to search the home in this case, *Vu* does not authorize the seizure of the device.

[58] In short, Reeves had a reasonable expectation of privacy in the shared computer and his rights had not been waived. Accordingly, the taking of the computer

by the police constituted a seizure within the meaning of s. 8 of the *Charter*. This warrantless seizure was not reasonable because it was not authorized by any law. The seizure therefore violated Reeves' rights under s. 8 of the *Charter*.

B. *Should the Evidence Be Excluded Under Section 24(2) of the Charter?*

[59] Under s. 24(2), evidence obtained in a manner that infringed *Charter* rights "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." In this analysis, courts must consider (1) the seriousness of the *Charter*-infringing state conduct; (2) the impact of the breach on the *Charter*-protected interests of the accused; and (3) society's interest in the adjudication of the case on its merits (*R. v. Grant*, 2009 SCC 32, [2009] 2 S.C.R. 353, at para. 71).

[60] The application judge determined that the evidence should be excluded under s. 24(2). The Court of Appeal conducted a fresh *Grant* analysis, given its determination that the application judge erred in concluding that the entry into the home and the taking of the home computer violated s. 8 of the *Charter*. It assessed whether the computer evidence should be excluded on the basis of the two other *Charter* breaches — the detention of the computer in violation of ss. 489.1 and 490 of the *Criminal Code* and the computer search without a valid warrant. The Court of Appeal noted that these breaches had a significant impact on Reeves' *Charter*-protected privacy interests and that this was "a borderline case" (para. 109). However, it ultimately concluded "that the repute of the administration of justice would be

undermined more than bolstered by excluding the evidence" (para. 109). It therefore set aside the application judge's exclusionary order.

[61] I agree with the application judge that the seizure of the home computer breached s. 8 of the *Charter* and that the computer evidence should be excluded.

[62] Although I am assuming (without deciding the issue) that the police entry was lawful, I agree with the application judge that the *Charter*-infringing state conduct in this case was serious. With respect to the seizure of the shared computer, while the officer believed that Gravelle's consent allowed him to take it, the police service had a specialized cyber-crime unit that should have been aware of the unique and heightened privacy interests in computers. The unit also should have known that a third party cannot waive another party's *Charter* rights. Although this Court's decision in *Cole* was released only a few days before the computer was seized in this case, the Ontario Court of Appeal decision in *Cole*, which found the school board could not consent to the search of an employee's computer, was released over a year earlier.

[63] With respect to the other *Charter* breaches found in the courts below, the officer could not explain why the police had detained the computer for months without respecting the reporting requirements in ss. 489.1 and 490 of the *Criminal Code*. Under s. 489.1, police must report a warrantless seizure to a justice "as soon as is practicable". Under s. 490(2), the seized item cannot be detained for over three months unless certain conditions are met. In this case, the police only made a report

to a justice as required by s. 489.1 of the *Criminal Code* after the computer was searched and almost five months after it was initially seized. These reporting requirements are important for *Charter* purposes, as they mandate police accountability for seizures that have not been judicially authorized (see *R. v. Tse*, 2012 SCC 16, [2012] 1 S.C.R. 531, at paras. 82 and 84).

[64] Additionally, as in *Morelli*, the ITO upon which the search warrant was obtained was "[a]t best . . . improvidently and carelessly drafted" (para. 100). The application judge concluded that the computer search breached the *Charter* because the ITO reflected "'a goal-oriented, selective presentation of the facts' that resulted in an 'unfair, unbalanced and misleading' portrayal of the applicant" and was insufficient to have justified granting the warrant (para. 38).

[65] In short, there were serious *Charter* breaches throughout the investigative process. Overall, the police conduct in this case undermined "public confidence in the rule of law" and favours exclusion of the evidence (*Grant*, at para. 73).

[66] I see no reason to disturb the application judge's conclusion that the state conduct had a serious impact on Reeves' *Charter*-protected interests. The fact that Reeves had a *reduced* reasonable expectation of privacy in the home computer diminishes the seriousness of the unreasonable search and seizure of this computer (*Cole*, at paras. 91-92; *Grant*, at para. 78; *R. v.* **Paterson, 2017 SCC 15, [2017] 1 S.C.R. 202, at para. 49;** J.A. Fontana and D. Keeshan, *The Law of Search and Seizure in Canada* (10th ed. 2017), at p. 23). Nonetheless, as this Court held in

Morelli, "[i]t is difficult to imagine a search more intrusive, extensive, or invasive of one's privacy than the search and seizure of a personal computer", given the extremely private nature of the data that a personal computer may contain (para. 2, see also para. 105).

[67] With respect to society's interest in the adjudication of this case on its merits, I agree with the application judge that it was strong. The unconstitutional search and seizure of the computer revealed reliable evidence that was important to the prosecution's case (see *Grant*, at paras. 81 and 83). Further, as the application judge and the Court of Appeal both noted, the alleged offences were serious. Child pornography offences are "particularly insidious" (*Morelli*, at para. 8). Cases in which a court must decide whether to exclude probative evidence of a serious crime are always challenging. However, the seriousness of the offence "has the potential to cut both ways" in assessing whether evidence should be excluded (*Grant*, at para. 84; see also *Paterson*, at para. 55). Indeed, "while the public has a heightened interest in seeing a determination on the merits where the offence charged is serious, it also has a vital interest in having a justice system that is above reproach" (*Grant*, at para. 84).

[68] Ultimately, the application judge concluded that, despite society's strong interest in the adjudication of this case on the merits, the evidence should be excluded due to "the flagrant disregard of the accused's section 8 *Charter* rights" (para. 49). This approach aligns with *Paterson*, where this Court remarked that "[i]t is . . . important not to allow the third *Grant* 2009 factor of society's interest in adjudicating

a case on its merits to trump all other considerations, particularly where (as here) the impugned conduct was serious and worked a substantial impact on the appellant's *Charter* right" (para. 56). Given the seriousness of the state conduct and of its impact on Reeves' *Charter*-protected interests, I agree with the application judge that the admission of the evidence would bring the administration of justice into disrepute.

IV. Conclusion

[69] For these reasons, I would allow the appeal, set aside the judgment of the Court of Appeal, exclude the evidence obtained from the seizure and subsequent search of Reeves' computer, and restore the acquittal entered at trial.

The following are the reasons delivered by

MOLDAVER J. —

[70] I have read the reasons of my colleague, Justice Karakatsanis for the majority, and I am in substantial agreement with her analysis and conclusion. In particular, I agree that Mr. Reeves had a reasonable expectation of privacy in the shared computer and that, in the circumstances, its warrantless seizure constituted a breach of his rights under s. 8 of the *Canadian Charter of Rights and Freedoms*, despite Ms. Gravelle's consent. I further agree, for the reasons expressed by my colleague, that the resulting evidence should be excluded under s. 24(2).

[71] My purpose in writing this concurrence is to express some tentative views on the issue of police entry into a shared residence, a matter of considerable importance to the administration of criminal justice — and one which Parliament has to date left unaddressed.

I. Should the Court Accept Counsel's Concession?

[72] As the majority notes, counsel for Mr. Reeves conceded during oral submissions before this Court that he was not challenging the police entry into the Reeves-Gravelle residence. Counsel explained that characterizing police entry into a home for the purpose of interviewing a witness as a "search" for s. 8 purposes "would be a tough argument . . . to make" (transcript, at p. 38). The jurisprudence, however, defines a "search" under s. 8 as any state action that intrudes upon a reasonable expectation of privacy: see, e.g., *R. v. Evans*, [1996] 1 S.C.R. 8, at para. 11; *R. v. Spencer*, 2014 SCC 43, [2014] 2 S.C.R. 212, at para. 16; *R. v. Tessling*, 2004 SCC 67, [2004] 3 S.C.R. 432, at para. 18; and H. Stewart, "Normative Foundations for Reasonable Expectations of Privacy" (2011), 54 *S.C.L.R.* (2d) 335, at p. 335. That being so, the effect of counsel's concession could be taken to mean that Mr. Reeves lacked a reasonable expectation of privacy in the common areas of his home — a contentious proposition to be sure, albeit one which my colleague Justice Côté has assiduously considered and resolved against Mr. Reeves, in favour of the state.

[73] This Court, of course, is not bound by counsel's concession. Evaluating whether to accept it in this case necessitates a particularly cautious approach for two

reasons. First, the issue is an important one. The police entry into the Reeves-Gravelle residence on the strength of Ms. Gravelle's consent was the catalyst giving rise to a chain of events that culminated in the discovery of child pornography on the shared computer. If the entry contravened s. 8, it follows that the evidence discovered during the search of the computer was "obtained in a manner that infringed or denied" Mr. Reeves' rights, bringing it within s. 24(2)'s exclusionary reach: see, generally, *R. v. Bartle*, [1994] 3 S.C.R. 173, at p. 209; *R. v. Grant*, [1993] 3 S.C.R. 223, at p. 255.

[74] Second, the legality of the police entry has implications beyond the four corners of this case. Police frequently attend residences to investigate suspected or ongoing criminal activity. Many of those residences are inhabited by more than one person with authority to permit third parties to enter the home. Counsel's concession that police entry into a shared residence is not a "search" therefore has the potential to affect a large swath of Canadian society by shifting our understanding of the right to be free from unreasonable search or seizure.

[75] In sum, counsel conceded an important issue, with broad implications beyond this case. In these circumstances, I am of the view that caution is warranted in deciding whether to accept counsel's concession. That said, the importance of the entry, in particular, its legality — as it relates to this case and the permissible scope of police power more generally — provides a compelling reason to consider the issue. While I am prepared to accept counsel's concession that the entry in this case was lawful — I offer an alternate route as a possible basis for so concluding, namely: that

the police conceivably had the authority to enter the shared residence at common law under the ancillary powers doctrine. Let me explain.

II. The Common Law Power to Enter a Shared Residence to Take a Statement

[76] I accept for the purpose of this analysis that Mr. Reeves had a reasonable expectation of privacy in the common areas of the home that he and Ms. Gravelle jointly owned and that Ms. Gravelle's consent to the police entry did not serve to negate that expectation. The police entry was therefore a "search" within the meaning of the *Charter* and it will only have complied with s. 8 if it was authorized by law, if the law was reasonable, and if the search was carried out in a reasonable manner: *R. v. Collins*, [1987] 1 S.C.R. 265, at p. 278; *R. v. Stillman*, [1997] 1 S.C.R. 607, at para. 25. What follows is a tentative articulation of the lawful authority under which the police officer acted when he entered the residence to take Ms. Gravelle and her sister's statements. I say "tentative" because the paradigm I am proposing was not raised by the parties. Therefore, any final determination of whether police may lawfully enter a joint residence when invited by one of the occupants must be left for another day.

[77] Whether police have the authority at common law to take an action that interferes with an individual's liberty or property is assessed using the framework set out by the U.K. Court of Criminal Appeals in *R. v. Waterfield*, [1963] 3 All E.R. 659, at pp. 660-62, per Ashworth J. Canadian courts have used the *Waterfield* framework — sometimes referred to as the ancillary powers doctrine — to affirm many common

law police powers now considered fundamental. For example, the R.I.D.E. program stops (*Dedman v. The Queen*, [1985] 2 S.C.R. 2), investigative detentions (*R. v. Mann*, 2004 SCC 52, [2004] 3 S.C.R. 59), searches incident to arrest (*Cloutier v. Langlois*, [1990] 1 S.C.R. 158), 911 home entries (*R. v. Godoy*, [1999] 1 S.C.R. 311), sniffer dog searches (*R. v. Kang-Brown*, 2008 SCC 18, [2008] 1 S.C.R. 456), and safety searches (*R. v. MacDonald*, 2014 SCC 3, [2014] 1 S.C.R. 37) were all affirmed through the *Waterfield* framework.

[78] As this Court explained in *MacDonald*, at paras. 34-37, the *Waterfield* analysis proceeds in two stages:

(1) Does the police conduct at issue fall within the general scope of their statutory or common law duties? Common law duties include keeping the peace, preventing crime, and protecting life and property.

(2) Does the conduct involve a justifiable use of police powers associated with that duty? The conduct is justifiable if it is reasonably necessary, with regard to:

(a) the importance of the performance of the duty to the public good;

(b) the necessity of the interference with an individual's liberty or property for the performance of the duty; and

(c) the extent of the interference.

[79] Commencing with stage one, there can be no doubt that entering into a shared residence when invited to take a witness statement in connection with a criminal investigation falls within the scope of police duties. Investigating crime is a primary police function: *Kang-Brown*, at para. 52, per Binnie J., concurring. Police officers in Ontario are statutorily duty-bound to encourage crime prevention within the community, apprehend criminals, and assist victims of crime: *Police Services Act*, R.S.O. 1990, c. P.15, s. 42(1). Entering a home to take a witness statement in connection with a criminal investigation furthers all three of these mandates.

[80] Turning to stage two, in my view, the proposed power may well be a reasonably necessary interference with individuals' privacy interests in their homes. The ability to enter into a home to take a statement when invited serves an important investigative function. As I have noted, police officers routinely seek to make contact with individuals within their homes. At times, the police themselves initiate contact with the occupant — for example, when canvassing a neighbourhood for information about a violent crime perpetrated in the area. This routine investigative tactic can yield fruitful information that would otherwise have eluded police: see, e.g., *R. v. Bui*, 2002 BCSC 289, [2002] B.C.J No. 3185 (QL), at para. 10.

[81] The importance of taking a statement in connection with a criminal investigation becomes even more apparent when a resident contacts the police to provide information about past or ongoing criminal activity within the home. In some cases, the reporting resident is the victim of a crime committed by a co-resident, such

as the spouse who calls the police to report that her partner has physically abused her. The reporting resident may also contact the police to provide information about harmful activities or items present in the home, such as a concerned spouse who believes there may be child pornography on the family computer used by the children or a roommate who believes another roommate may be trafficking in prohibited firearms. Finally, as the Crown points out, the reporting resident may have a legitimate interest in contacting police to report illegal activity within the home to dispel suspicion against him or her. In my view, no quarrel can be taken with the importance of taking statements from the reporting residents in these examples.

[82] The next consideration in deciding whether the impugned police action is justified is the necessity of the interference for the performance of the duty. To be more specific, although taking statements — especially from victims of crime — is of doubtless importance, is it necessary for police to intrude on a co-resident's expectation of privacy in his or her home to do so? In my view, the answer may well be yes.

[83] For a variety of reasons, individuals who are prevented from speaking with the police in their homes may be unwilling, or unable, to speak with them at all. Individuals who live in high-crime neighbourhoods may fear for their safety if they are seen speaking to police, and may well refuse to do so outside the privacy of their homes. For the elderly, chronically ill, or parents taking care of small children, leaving the home to speak with police may simply not be feasible. In cases of

suspected child abuse, the police may need to interview children in their home, in a parent or guardian's presence. Canadians living in rural areas are often situated far from the nearest police station. Even for urban Canadians, inclement weather or competing obligations may preclude a trip to the local police station.

[84] Returning to the domestic violence example, assume the complainant calls the police and informs them that her partner has physically abused her but has left the house. There is no emergency that would allow the police to enter the home under the emergency search power articulated in *Godoy*. Without each occupant's consent, the police would be unable to enter the home. At present, the police would appear to have two options. They could ask the complainant, who has just been assaulted, to suffer the embarrassment of speaking to the police outside of her home — a request that could understandably be met with a refusal. Or, they could try to obtain the consent from the co-resident who allegedly perpetrated the abuse — an exercise almost guaranteed to prove futile.

[85] Further complications arise in cases where several occupants reside at the same address. Are the police, after being called by a resident who reports a theft of property from a home she shares with six roommates, required to (1) determine how many people live in the home, and (2) seek out and obtain the consent of each before entering the home to take a statement?

[86] In each of the foregoing examples, short of intruding on the co-resident's expectation of privacy, the police would effectively be powerless to investigate the reported criminal offences.

[87] The final factor in assessing whether a particular police action is reasonably necessary is the extent of the interference occasioned by that action. As I have observed, when the police enter a home, they interfere with the expectation of privacy of all residents who did not consent to that entry. However, properly constrained, entering a home when invited by an occupant to take a witness statement is minimally intrusive on the other residents' privacy interests. I appreciate that the home is unquestionably a private place. Our homes have the potential to reveal the most intimate details about our personal lives. Individuals therefore typically have a heightened expectation of privacy within their homes: *Evans*, at para. 42; *Tessling*, at para. 22. That said, five constraints on the police entry power that I am articulating operate to minimize the extent of the interference with that expectation.

[88] First, the police must query whether conducting the interview in the person's home is necessary. If, after being presented with the option of having the interview at home or elsewhere, the person is ambivalent as to where it takes place, then the interview should be conducted outside the home. On the other hand, if the person indicates a preference to speak with the police at home, the police may act upon that preference. They need not attempt to weigh the strength of the person's conviction not to be interviewed outside the home. Nor ought the police to cross-

examine the person about his or her underlying fears and motivations, in an effort to determine whether the person will leave the home if pressed or cajoled.

[89] Second, the scope of the entry power would be narrowly tailored to its purpose. Courts regularly focus on the purpose of a particular police action to evaluate its legality. For example, in *Evans*, this Court held that residents are deemed to grant the public, including police, an implied licence to approach their home and knock. However, the police may only approach a residence under the implied licence to knock doctrine if their purpose in approaching is to communicate with an occupant: *Evans*, at paras. 13-16. Similarly, a search incident to arrest is only lawful if the purpose of the search relates to the purpose of the arrest: *R. v. Caslake*, [1998] 1 S.C.R. 51, at paras. 19-25.

[90] The purpose of the entry power that I am articulating is to take one or more statements in connection with a criminal investigation, whether from the authorizing resident, or from other willing occupants, as the authorizing resident may permit. Thus, in the present case, the police would be entitled to speak with Ms. Gravelle, who let the officer in, and her sister, who agreed to give a statement. Absent further lawful authority, the legality of the entry ends when the police exceed that purpose.

[91] To be precise, the police may not go further and lawfully search the residence or seize evidence from it unless they obtain the necessary grounds in the course of taking the statement or statements. For example, if after taking one or more

statements, the police develop reasonable grounds to believe that a computer in the house has child pornography on it, they would be able to seize that computer: see *Criminal Code*, R.S.C. 1985, c. C-46, s. 489(2). Similarly, the police might be able to seize evidence of a crime discovered inadvertently in plain view: see *R. v. Jones*, 2011 ONCA 632, 107 O.R. (3d) 241, at para. 56. I wish to stress, however, that the lawfulness of any subsequent police investigative action hinges on them having the necessary grounds to justify that action.

[92] Third, the police would only be permitted to enter the common areas of the home. This too flows from the purpose of the entry. Because the police are only in the residence to take a statement, there is no need to enter any private areas, such as bedrooms, where a resident's expectation of privacy is generally at its highest. In contrast, each co-resident has a reduced expectation of privacy in common areas of their home. In this regard, I agree with LaForme J.A. that when two people share a home, each "knows from the outset that the other co-resident has the right to invite others into the shared spaces": 2017 ONCA 365, 350 C.C.C. (3d) 1, at para. 48. Limiting the police entry to these shared spaces — specifically, the common area into which the police have been invited — reduces the intrusiveness of that entry.

[93] Fourth, the police can only enter if invited in by an occupant with the authority to consent. Unlike many of the other statutory and common law police entry powers, forced entry would be strictly prohibited. Furthermore, the consent must be voluntary and informed: see *R. v. Borden*, [1994] 3 S.C.R. 145; *R. v. Wills* (1992), 12

C.R. (4th) 58 (Ont. C.A.). Requiring a valid consent greatly reduces the intrusiveness of the subsequent entry. Furthermore, the resident's consent must be continuous and may therefore be revoked. The police must respect the resident's wishes if he or she revokes the consent.

[94] Fifth, the entry would only be for a limited duration. If, after taking the statement, or statements, the police do not obtain the requisite grounds to undertake any further investigative action, they must immediately leave the residence.

[95] These constraints act to limit the impact of the police entry on the non-consenting resident's privacy interests while allowing the police to engage in an important and necessary facet of their duty to investigate crime. In short, the entry power I am articulating may well be a reasonably necessary, and therefore justifiable, incursion on an individual's expectation of privacy. Without conclusively deciding the issue, a narrow entry power to take a statement from an individual with the authority to grant police entry, or from other willing occupants, as the authorizing resident may permit, along the lines that I have articulated, would appear to meet the two-pronged *Waterfield* framework.

[96] To summarize, the common law police power that I have tentatively described above has five criteria:

(1) The police must offer the authorizing resident, and any other cooperating occupants, a suitable alternative interview location — if one is available —

that does not potentially intrude upon the reasonable expectations of privacy of co-residents in their home.

(2) The purpose of the entry must be limited to taking a statement, or statements, from the authorizing resident, or one or more willing occupants, in connection with a criminal investigation. The police may not go further and search for or seize evidence unless they obtain the necessary grounds to do so in the course of taking the statement or statements.

(3) The police are only permitted to enter the home's common areas into which they have been invited.

(4) The police can only enter if invited in by a resident with the authority to consent and that consent must be voluntary, informed and continuous.

(5) Unless the police obtain the necessary grounds to take further investigative action, the duration of the entry must be limited to taking a statement, or statements, from the authorizing resident, or one or more willing occupants.

III. The Constitutionality of the Proposed Entry Power

[97] The existence of a legal authority to search, however, does not end the analysis. In order to meet s. 8's reasonableness requirement, any law purporting to authorize a search or seizure must itself be reasonable: *Collins*, at p. 278. *Hunter v. Southam Inc.*, [1984] 2 S.C.R. 145, at p. 168, sets the presumptive constitutional benchmark at reasonable grounds to believe that the search would uncover evidence

of an offence. I acknowledge that the police purporting to rely on the entry power I have articulated would rarely, if ever, have reasonable grounds to believe either that an offence had been committed or that evidence of an offence would be found within the home. Indeed, predicating the entry power on that standard would render it redundant, as police who have reasonable grounds to believe that an offence has been committed and that entry into the house would provide evidence of that offence could obtain a warrant to enter the home.

[98] Despite falling short of *Hunter*'s presumptive justificatory standard, in my view, the proposed power may nonetheless be constitutional. This is because "the jurisprudence . . . accepts a measure of flexibility when the demands of reasonableness require": *Kang-Brown*, at para. 59. Several search powers authorized on a lower standard of justification have met s. 8's reasonableness requirement. For example, a reasonable suspicion constitutionally authorizes school searches (*R. v. M. (M.R.)*, [1998] 3 S.C.R. 393), sniffer dog searches (*Kang-Brown*), and border-crossing searches (*R. v. Simmons*, [1988] 2 S.C.R. 495). Searches incident to arrest have no probability threshold whatsoever. Rather, their constitutionality hinges on their purpose and the manner in which they are carried out: *Cloutier*, at pp. 185-86.

[99] The entry power I am articulating is similarly constrained. The five limitations I set out above narrowly constrain the entry power in a way that may well meet s. 8's reasonableness requirement.

IV. Application

[100] As indicated, the common law power that I have been discussing is a tentative articulation of the lawful authority under which the police could enter a shared residence. Assuming it were to pass constitutional muster, it is quite possible that the police entry in this case would not have constituted a breach of Mr. Reeves' s. 8 rights up to the point where the officer seized the computer. The officer testified that his purpose in entering the residence was not to seize a computer, but rather "to investigate what possibly was a computer crime": A.R., vol. III, at p. 41. He asked for and received Ms. Gravelle's consent before entering. Both lower courts found that Ms. Gravelle's consent was voluntary and informed. Once inside, the officer took statements from Ms. Gravelle and her sister in the kitchen.

[101] On the other hand, it is not clear on this record whether — assuming there was an alternative suitable location — the officer offered to interview Ms. Gravelle and her sister elsewhere. The answer to this question would go a long way to determining whether the police were authorized at common law to enter the Reeves-Gravelle residence. Thus, I can only say with confidence that the officer met four out of five of the proposed criteria articulated above.

[102] In any event, the officer proceeded to seize the shared computer. As discussed, the officer would only have been lawfully entitled to seize the computer had he gained the requisite grounds to do so in the course of taking the statements. As the majority points out, the officer himself testified that he did not have reasonable grounds to believe that the computer would afford evidence of an offence. The

seizure therefore constituted a s. 8 breach which, in combination with the invalid ITO and the failure to comply with the *Criminal Code* evidence retention regime, warrants exclusion of the evidence.

[103] I would therefore allow the appeal and restore Mr. Reeves' acquittal.

The following are the reasons delivered by

CÔTÉ J. —

I. Overview

[104] This case presents two principal issues. First, can the police lawfully enter common areas of a shared home with the consent of one cohabitant, or are they required to obtain the unanimous consent of all persons who live in that home in order to enter on the basis of consent? Second, can the police lawfully seize a jointly-owned computer (i.e., physically remove the computer, without searching its contents) when that computer is located in a common area of a shared home and one of the computer's co-owners provides her consent?

[105] Karakatsanis J. for the majority declines to discuss the first issue. Since it was ably argued by the parties, and since the lawfulness of the police entry into the home is relevant to the analysis pursuant to s. 24(2) of the *Canadian Charter of*

Rights and Freedoms, I will address it directly. In my view, one cohabitant can validly consent to a police entry into common areas of a shared residence, obviating the need for a warrant. The alternative rule — that the police may enter the common areas of a shared home only if they obtain consent from each and every person who lives there — is entirely unworkable. It also has no basis in our existing s. 8 jurisprudence as it pertains to physical spaces.

[106] On the second issue, the majority concludes that the police removal of the computer was invalid because Ms. Gravelle, on her own, was not capable of providing valid consent. I respectfully disagree. If instead of what happened here, Ms. Gravelle had physically taken the computer to a police station and turned it over, surely the police would not have been prohibited from accepting it. There is no coherent way to distinguish that scenario, on constitutional grounds, from a situation where the police request consent to physically remove jointly owned property and that consent is subsequently provided. Regardless, it is important to be precise about the privacy interests that are implicated by a *seizure* of a computer as opposed to a *search* of its contents. Much of the majority's analysis focuses on informational privacy concerns that simply do not arise when the police physically remove an electronic device from a home without searching its contents.

[107] Nevertheless, even though I am of the view that the entry into the home and the seizure of the computer were both lawful, I would still exclude the evidence under s. 24(2) of the *Charter* based on the other violations of law in this case —

specifically, the fact that the police failed to comply with ss. 489.1 and 490 of the *Criminal Code*, R.S.C. 1985, c. C-46, by improperly detaining the computer and the fact that the search warrant was ultimately found to be invalid.

II. Analysis

A. *Police Entry Into the Home*

[108] A police entry into a home based on valid consent does not run afoul of s. 8. As the majority notes, valid consent means that there is no search or seizure within the meaning of the *Charter* (para. 13). Here, Ms. Gravelle permitted a police officer to enter the home she shared with Mr. Reeves. At the time of the police entry, Mr. Reeves had no authority to enter the home himself, as Ms. Gravelle had exercised her right, pursuant to a no-contact order, to keep him out of the house. The question, then, is whether Mr. Reeves' *Charter* rights were violated by the police entry into common areas of the home on the basis of Ms. Gravelle's consent.

[109] Although I agree with the result that Moldaver J. reaches with respect to this question — namely that the police entry did not violate Mr. Reeves' s. 8 rights — in what follows, I offer what I view as a more compelling basis for reaching that result. Not only do the police have a common law power to enter a shared residence for the purpose of taking a statement (a power that satisfies the reasonableness requirement), but there is no violation of s. 8 in any event, because Mr. Reeves'

expectation of privacy was not objectively reasonable in a context where a cohabitant, Ms. Gravelle, provided her consent for the police to enter common areas of the home.

[110] As this Court has routinely recognized, s. 8 of the *Charter* protects against unreasonable intrusions by the state into the privacy interests of an accused (*R. v. Law*, 2002 SCC 10, [2002] 1 S.C.R. 227, at para. 15). This constitutional protection extends only to expectations of privacy that are objectively reasonable, having regard to the totality of the circumstances (*R. v. Edwards*, [1996] 1 S.C.R. 128). In drawing the line between expectations that are reasonable and those that are not, it is important to recognize that privacy itself is not an all or nothing concept (*R. v. Marakah*, 2017 SCC 59, [2017] 2 S.C.R. 608, at para. 143; *R. v. Quesnelle*, 2014 SCC 46, [2014] 2 S.C.R. 390, at para. 29). Expectations of privacy in respect of certain objects or spaces may be recognized as objectively reasonable in some circumstances, but not in others (*R. v. M. (M.R.)*, [1998] 3 S.C.R. 393, at para. 33).

[111] Here, it is clear that Mr. Reeves had a reasonable expectation of privacy in the home he shared with Ms. Gravelle in at least some contexts. But what is really at issue in this case is the scope or extent of a resident's expectation of privacy with respect to the common areas of a shared home when another resident of that home wishes to give the police access.

[112] In my view, it is not objectively reasonable for a cohabitant, who shares a residence with others, to expect to be able to veto another cohabitant's decision to allow the police to enter any areas of that home that they share equally. Although

Mr. Reeves did have an expectation of privacy in those areas, that expectation was attenuated and limited by the reality of cohabitation. Other persons with overlapping privacy interests in and rights to common spaces can validly permit third parties to enter those spaces. This includes the police. To hold otherwise would be to interfere with the consenting cohabitant's liberty and autonomy interests with respect to those spaces. Thus, I would reject the argument that the entry was invalid because Ms. Gravelle could not waive Mr. Reeves' *Charter* rights. That is beside the point. Properly understood, Ms. Gravelle did not waive anyone's rights except her own. But in the context of a shared home, Mr. Reeves' reasonable expectation of privacy was not sufficiently capacious to afford constitutional protection against a cohabitant's decision to give the police access to common areas. This is especially true on the facts of this case, where Mr. Reeves had no legal right to be in the home at the time of the police entry because Ms. Gravelle had revoked her permission for him to enter it earlier that day pursuant to the no-contact order. The analysis is of course different concerning private areas of a shared residence, such as an individual's exclusive bedroom or office — types of spaces that are not involved in this case.

[113] Moreover, this Court has repeatedly recognized that s. 8 strikes a balance between privacy and law enforcement interests: "The need to balance 'societal interests in protecting individual dignity, integrity and autonomy with effective law enforcement' has been specifically identified as a key consideration informing the reasonable expectation of privacy test" (*Marakah*, at para. 179 (per Moldaver J.,

dissenting, but not on this point), quoting *R. v. Patrick*, 2009 SCC 17, [2009] 1 S.C.R. 579, at para. 20).

[114] The effect of Mr. Reeves' position — that the police must obtain the unanimous consent of all cohabitants before entering common areas — is unworkable and would substantially undermine effective law enforcement. It would require the police to identify, locate and obtain the consent of every person who lives in the home, or has any expectation of privacy with respect to common areas of the home, no matter how onerous that task might be. This would effectively negate all investigative advantages of entering on the basis of consent. In some cases, it would tip off potential suspects to an investigation. In others, it would likely render consent entries too burdensome or impractical. The police would be forced to obtain a warrant, rather than entering on the basis of consent, in all but the most straightforward of circumstances, creating additional procedural burdens. The rule might also result in entries or searches that are more extensive (and therefore more invasive of privacy interests) than consent searches, which must be limited in accordance with the scope of the consent. And, of course, warrants require a sufficient evidentiary basis. In some instances, a suspect who cohabitates with others may wish to consent to a police entry or a search, even where a warrant could not otherwise be obtained, in order to quickly dispel suspicion or for other reasons. But under Mr. Reeves' proposed approach, any other cohabitant could veto that suspect's ability to do so. In fact, a cohabitant could even be precluded from permitting the police to search his or her *own* bedroom — one that is completely private and not

shared with others — if accessing that bedroom would require entering shared areas of the home.

[115] This is to say nothing of the more consequential implications of Mr. Reeves' reasoning when applied to other contexts. In *Marakah*, a majority of this Court held that the sender of a text message may have a reasonable expectation of privacy in the contents of an electronic conversation. But that case did not address a related question: can the recipient of a text message consent to a police search of that electronic conversation on his or her phone? Or, for that matter, can the recipient volunteer to turn over the contents of the message to the police? If Mr. Reeves' position were to be adopted, the answer would be no. This is because *Marakah* recognized that both parties to a text message chain can have a reasonable expectation of privacy in that electronic conversation, just as two cohabitants can have a shared and overlapping expectation of privacy with respect to a common area in a shared home. If Mr. Reeves is correct that he could veto Ms. Gravelle's ability to consent to a police entry into common areas of their home, it must also be the case that the sender of text messages can veto the recipient's ability to consent to a search of their messages stored on the recipient's own phone. It is clear, then, that the autonomy implications of Mr. Reeves' argument extend beyond entries into physical spaces and threaten to undermine effective law enforcement in other contexts as well.

[116] That said, the ability of law enforcement officials to enter on the basis of consent is not without limits. As the Crown acknowledges, the consenting person

must have the authority to consent (as a first-party rights holder with his or her own *Charter*-protected privacy right in the shared place or thing); the consent must be limited to shared places or things; the consent must be informed and voluntary; and the police must respect the limits of the consent, which is freely revocable at any point during the entry or search. Each of these requirements was satisfied here.

[117] Finally, it is telling that every provincial appellate court in the country including the lower court in this case that has considered this issue has come to the same conclusion: the consent of one co-resident is sufficient to permit the police to enter common areas of a shared home (see, e.g., *R. v. Reeves*, 2017 ONCA 365, 350 C.C.C. (3d) 1, at paras. 32, 43 and 46-52; *R. v. Clarke*, 2017 BCCA 453, 357 C.C.C. (3d) 237, at paras. 55-56 and 62-63; *R. v. T. (R.M.J.)*, 2014 MBCA 36, 311 C.C.C. (3d) 185, at paras. 41-52; *R. v. Squires*, 2005 NLCA 51, 199 C.C.C. (3d) 509, at para. 34). Mr. Reeves does not point to a single case that has held otherwise. Instead, in the absence of any directly relevant authority, he relies heavily on *R. v. Cole*, 2012 SCC 53, [2012] 3 S.C.R. 34, where this Court found that a search of an employee's computer on the basis of his employer's consent was unlawful. But *Cole* is inapposite for two reasons.

[118] First, the outcome in *Cole* was inextricably tied to the informational privacy concerns that were implicated by the police search of Mr. Cole's computer. Fish J., writing for the Court, stressed that a search of a computer can reveal extremely private information that falls within the "biographical core" protected by

s. 8, including browsing history that may offer an intimate account of an individual's private life. Likewise, in *R. v. Morelli*, 2010 SCC 8, [2010] 1 S.C.R. 253, at para. 105, Fish. J. observed that "it is difficult to imagine a more intrusive invasion of privacy than the search of one's home and personal computer." Subsequent case law has confirmed that searches of computers raise distinctive privacy concerns that justify special rules — for example, a rule requiring specific authorization to search a computer that is found in the place of search, which departs from the general rule that applies to other types of physical receptacles (*R. v. Vu*, 2013 SCC 60, [2013] 3 S.C.R. 657, at paras. 1, 47 and 51).

[119] A search of a common area of a shared home does not present the same privacy implications as a search of the electronic contents of a computer. Simply put, an entry into a common area is unlikely to yield the same intensely private information going to a person's biographical core as a search of a computer hard drive. The physical contents of a living room shared by roommates, for example, are less likely to immediately reveal "our most intimate correspondence", "the details of our financial, medical, and personal situations", "our specific interests, likes, and propensities", or "the information we seek out and read, watch, or listen to" (*Morelli*, at para. 105). This is precisely why *Vu* distinguished computers from other types of objects by requiring specific judicial authorization to search computers that are found in places the police are otherwise permitted to search. I would therefore decline to extend *Cole* from the context of computer searches to the context of physical searches

of shared spaces in dwellings — an issue that *Cole* did not address because it was not before the Court (see *T. (R.M.J.)*, at paras. 51-52).

[120] Second, unlike Ms. Gravelle in the present case, the school board in *Cole* was not a first-party rights holder. The school board's interest in the laptop was only proprietary in nature, and mere ownership of the laptop was found not to be a sufficient basis for the board to be able to consent to a police search of the data stored on it (*Cole*, paras. 51 and 58). This principle applies equally to physical spaces. For example, the owner of an apartment or a hotel cannot validly consent to a search of a unit occupied by a tenant or guest based only on the fact that he or she owns the premises (see, e.g., *R. v. Buhay*, 2003 SCC 30, [2003] 1 S.C.R. 631, at para. 22; *R. v. Mercer* (1992), 7 O.R. (3d) 9 (C.A.); *R. v. Stevens*, 2011 ONCA 504, 106 O.R. (3d) 241). *Cole*'s rejection of a third-party consent doctrine must be understood in this context. This case, however, is different. Ms. Gravelle is not merely an owner (or co-owner) of the home. She is also a resident — and as a result, she has her own privacy and autonomy interests in the home's common areas. Those interests are significantly more compelling in the case of a resident who lives in a home, as opposed to an owner who merely rents out an apartment (or, in the case of *Cole*, an employer who provides an employee with a laptop). And as I have described, Ms. Gravelle's consent to enter the home is not properly understood as a waiver of Mr. Reeves' rights. Rather, the scope of Mr. Reeves' reasonable expectation of privacy is limited in recognition of the fact that Ms. Gravelle is a first-party rights holder who should be permitted to freely exercise her rights of access and control

over common areas. Therefore, *Cole* does not support a finding that the police entry into the home was in breach of s. 8.

B. *Police Removal of the Computer From the Home*

[121] The second issue in this case is whether the fact that the police physically took (i.e., seized) the computer from the home with Ms. Gravelle's consent violated Mr. Reeves' s. 8 rights. As with the police entry into the home, my view is that Mr. Reeves' expectation of privacy with respect to the computer he shared with Ms. Gravelle was attenuated by the realities of joint ownership and use. It was not objectively reasonable for him to expect that Ms. Gravelle could not exercise her own authority and control over the computer to consent to a seizure by the police. As a result, I disagree with both Karakatsanis J. and Moldaver J. on this issue. My reasoning with respect to the police entry — specifically, the fact that Mr. Reeves' objectively reasonable expectation of privacy was attenuated by the realities of cohabitation and co-ownership — necessarily leads to the conclusion that the physical taking of the shared computer was also lawful.

[122] First, it is necessary to define the subject matter of the seizure. The majority correctly observes (at para. 29) that the subject matter must be carefully defined "by reference to the nature of the privacy interests potentially compromised by the state action" (*Marakah*, at para. 15, quoting *R. v. Ward*, 2012 ONCA 660, 112 O.R. (3d) 321, at para. 65). In certain cases, this may require examining "the connection between the police investigative technique and the privacy interest at

stake" (*R. v. Spencer*, 2014 SCC 43, [2014] 2 S.C.R. 212, at para. 26). Ultimately, in defining the subject matter of the search or seizure, the court's task "is to determine 'what the police were really after'" (*Marakah*, at para. 15, quoting *Ward*, at para. 67).

[123] The majority defines the subject matter of the seizure as "the computer, and ultimately the data it contained" (para. 30). But "what the police were really after" through the *seizure* of the computer was *only* the physical device, not the data itself. At no point were the computer's contents — that is, the data stored on the hard drive — ever searched or examined by the police prior to obtaining a warrant. That makes this case quite different from *Cole*, where the teacher's laptop was actually *searched* without a warrant, raising concerns about the suspect's informational privacy. Here, though, the law enforcement objective in seizing the computer was simply to preserve potential evidence. As LaForme J.A. held in the court below, the seizure of the computer did nothing to interfere with Mr. Reeves' expectation of privacy in its informational content because that content remained private. Thus, the "privacy interests potentially compromised by the state action" suggest that the subject matter of the search should be defined as the physical device alone, and not the data on the hard drive.

[124] Recognizing that the informational content of the computer was not made available to the police by the seizure, the majority pivots to a different argument for defining the subject matter of the search to include the data: Mr. Reeves was deprived of his *control* over that data. But with respect, this too is misguided. Since

Ms. Gravelle had exercised her authority to prohibit Mr. Reeves from entering the home in accordance with the terms of the no-contact order, Mr. Reeves would have had no ability to access the computer even if the seizure had not occurred. Thus, the seizure did nothing to alter his ability (or lack of ability) to access the informational content of the hard drive. In any event, any alleged deprivation of control over the data is properly characterized as an interference with his property rights in that data, not as a violation of his privacy rights, since the informational content remained private from the police. The majority suggests that the Court of Appeal's focus on property rights neglects "important privacy rights in *the data*" (at para. 31 (emphasis in original)); but without further explanation as to exactly what those privacy rights were (as distinct from his proprietary rights in the data) and how they were at all affected by the seizure, this assertion rings hollow.

[125] Turning, then, to the question of whether Mr. Reeves had an objectively reasonable expectation of privacy with respect to the subject matter of the seizure, the majority repeats the same arguments by focusing on the informational content of the hard drive. Although I agree that computers "contain highly private information", "retain information that the user may think has been deleted" and therefore present "unique privacy concerns" (at paras. 34 and 35), none of this is relevant here. As the majority acknowledges, "the police could not actually search the data until they obtained a warrant" (para. 30). These concerns are therefore not at issue.

[126] When the subject matter of the seizure is properly defined as the physical computer, it is clear that it was not objectively reasonable for Mr. Reeves to expect that he could prohibit Ms. Gravelle from exercising her own authority and control over the computer to consent to a police seizure.

[127] As with the police entry, I agree that Mr. Reeves' expectation of privacy in the physical computer might be objectively reasonable in some circumstances. For example, had Ms. Gravelle not consented to the removal, I do not dispute that a warrantless seizure would have violated Mr. Reeves' s. 8 rights. But in my view, it is not objectively reasonable for his subjective expectation of privacy to act as a veto on Ms. Gravelle's ability to exercise her own property rights in the physical device. The scope of Mr. Reeves' s. 8 protection is limited by the fact that the computer was jointly owned and used by another person. Ms. Gravelle's rights in the computer — including her property rights in the device and her right to waive her own privacy protections — would be rendered meaningless if Mr. Reeves could prevent her from consenting to the physical removal of the computer. This would, in essence, subjugate her rights to his.

[128] By failing to recognize that privacy is contextual and that subjective expectations may be objectively reasonable in some circumstances but not in others (*M. (M.R.)*, at para. 33), the majority presents a false dichotomy: either Mr. Reeves' expectation of privacy in the computer was *never* objectively reasonable, or Ms. Gravelle waived Mr. Reeves' constitutional protections on his behalf. I would

reject this approach. As I have described with respect to both the entry and the seizure, the question here is not whether Mr. Reeves' privacy interest was *ever* constitutionally protected. It is simply whether his expectation of privacy should be recognized as objectively reasonable *in this context* — where the subject matter of the seizure was jointly owned and used, and where the other joint owner and user consented to the seizure. In my view, that expectation exceeds the bounds of objective reasonableness. Three other points inform this conclusion.

[129] First, there is no doubt that Ms. Gravelle could exercise her property rights in the computer by taking the device to a police station and handing it to an officer. Otherwise, as the Crown aptly suggests, victims of crime who receive threatening text messages would be prohibited from showing those messages to the police unless and until the police obtain a warrant. What makes this case any different? If the majority's analysis holds, it would establish an unworkable doctrine whereby a joint owner/user of an object could voluntarily give the object to the police but could not consent to an affirmative request to seize it. Delineating the boundaries of such a distinction would be a difficult task; and in any event, it would amount to a distinction without a difference.

[130] Second, the fact that Ms. Gravelle revoked her consent for Mr. Reeves to enter the home is again relevant in the context of the seizure: "Control, ownership, possession, and historical use have long been considered relevant to determining whether a subjective expectation of privacy is objectively reasonable" (*Marakah*, at

para. 38). Although *Marakah* makes clear that limited or non-existent control over the subject matter of a search or seizure is not necessarily fatal to a reasonable expectation of privacy, it remains the case that "[c]ontrol of access is central to the privacy concept" (*R. v. Belnavis* (1996), 29 O.R. (3d) 321 (C.A.), at p. 332, aff'd [1997] 3 S.C.R. 341). Here, since Mr. Reeves had been lawfully barred from entering the house by Ms. Gravelle, he could no longer exercise any physical control over the computer. With respect, the suggestion that Mr. Reeves' lack of control resulted from the fact that he was in police custody misses the point (majority reasons, at para. 38). Although it is true that he was in custody at the time the computer was removed from the home, this was not the reason he lacked control over the device. He lacked control as a result of his own actions, which were the reason why the no-contact order was made and, eventually, why Ms. Gravelle revoked her permission for him to access the house.

[131] Finally, there is little in the majority's reasons that would necessarily tether its conclusion to the fact that Mr. Reeves was a co-*owner* of the computer, as opposed to a person who had simply used the computer at some point in the past. The majority's focus on "the deeply intimate nature of [the] information" generated by using the device (at para. 47), its observation that Mr. Reeves' lack of control over the computer was purportedly involuntary (at para. 38), and its rejection of the argument that Ms. Gravelle's equal and overlapping privacy interest eliminated any protection for Mr. Reeves (at para. 41) all apply equally to any person who used the computer at one point or another. Indeed, taken to its logical extreme, the majority's approach

would grant s. 8 protection to *any* prior user of the computer who generated data on the hard drive by browsing the Internet — no matter how extensive the use, or how far in the past.

[132] None of this is to suggest that the police could *search* the computer without a warrant. In that context, informational privacy concerns associated with electronic data could properly be taken into account in requiring such a search to be conducted with judicial authorization (see *Vu*, at para. 2). Indeed, the police in this case did not search the hard drive's contents until they obtained a warrant (even though that warrant was ultimately found to be deficient). But with respect to the police taking the physical computer into their custody, I would find no violation of Mr. Reeves' s. 8 rights in a context where Ms. Gravelle provided her consent.

C. *Section 24(2) of the Charter*

[133] Irrespective of the fact that the police entry and seizure were, in my view, both lawful, the application judge identified other violations of law that must factor into the s. 24(2) analysis.

[134] First, the computer was held in police custody for more than four months before a search warrant was sought and executed. Section 489.1 of the *Criminal Code* requires that the seizure and detention of property by the police be reported to a justice "as soon as is practicable". The justice must then determine whether to return the property to the accused. In addition, s. 490(2) of the *Criminal Code* provides that

seized property may not be detained for longer than three months unless the justice is satisfied that it is still required or unless legal proceedings requiring the use of the property have been instituted. Continued detention of an individual's property in violation of these *Criminal Code* provisions amounts to a violation of an accused's s. 8 *Charter* rights regardless of whether the initial seizure was valid (*R. v. Garcia-Machado*, 2015 ONCA 569, 126 O.R. (3d) 737, at paras. 43-55). The police violated both *Criminal Code* provisions in this case.

[135] Second, the application judge concluded that there had been insufficient grounds to grant a search warrant for the computer in the first place (para. 40). In his view, the affidavit submitted in support of the warrant was "a goal-oriented, selective presentation of the facts" that resulted in a misleading portrayal of the situation (para. 38). In argument before the judge, Mr. Reeves emphasized a number of deficiencies, including the affiant's failure to provide information about a potential motive for prejudice on the part of Ms. Gravelle's sister, Natalie. Ultimately, the application judge concluded that the justice of the peace who granted the warrant had been deprived of "the objective, non-prejudicial information needed . . . to conclude that there were reasonable and probable grounds for granting the warrant" (para. 38).

[136] In conducting a s. 24(2) analysis, the court must consider the seriousness of the *Charter*-infringing state conduct, the impact of the breach on the accused's *Charter*-protected interests, and society's interest in the adjudication of the case on its merits (*R. v. Grant*, 2009 SCC 32, [2009] 2 S.C.R. 353, at para. 71).

[137] With respect to the seriousness of the state conduct and the impact of the breaches on Mr. Reeves, I conclude that the violations described above, when considered together, were quite serious and had a significant impact on his *Charter* rights.

[138] First, the police were required to report the seizure to a justice as soon as practicable, but they waited *more than four months* before doing so. The Crown offers no explanation for this delay. With respect, I would hesitate to describe this violation as merely technical in nature. This is not a case where the police missed a deadline by one or two days; it is a case where a prolonged failure to abide by legal requirements left Mr. Reeves unable to argue before a justice that the property should be returned to him. In sum, the *Charter* violations arising from the breaches of ss. 489.1 and 490(1) of the *Criminal Code* deprived him of his property rights without justification and shielded the police's detention of the computer from the scrutiny of a justice. In light of the clear and detailed framework established by Parliament for the seizure of property — a framework that is not at all new — these breaches were not merely trivial (see *R. v. Villaroman*, 2018 ABCA 220, 363 C.C.C. (3d) 141, at para. 22).

[139] Even if these violations were not sufficiently serious on their own to justify excluding the evidence, the application judge also determined that the search warrant itself was deficient. As the Court of Appeal noted, "[i]mplicit in [the application judge's] analysis is his conclusion that, had the relevant facts been

included and misleading statements excised, there would no longer be a reasonable basis for issuance of the warrant" (para. 84). Indeed, the Court of Appeal upheld this conclusion, holding that "the test to issue the warrant could not be met" in this case (para. 95). Even though there is no evidence that the information presented to the judge was intentionally deficient, there is likewise no explanation for what is an otherwise significant breach of s. 8. The impact of this breach on Mr. Reeves was especially serious, as the search of the data on the computer without proper judicial authorization — unlike the mere seizure of the physical device — gave the police access to exceptionally private information, including web browsing history, that lies at the "biographical core" protected by s. 8.

[140] Although the third *Grant* factor counsels in favour of admitting the evidence, I would conclude, on balance, that the significance of the *Charter* breaches, along with their impact on Mr. Reeves, lead to the conclusion that the evidence should be excluded.

III. Conclusion

[141] For the foregoing reasons, I agree that the evidence should be excluded, and the appeal should be allowed on that basis. I would therefore restore the acquittal entered at trial. However, as I have described, I disagree with the manner in which the majority has resolved (or otherwise declined to resolve) the central legal issues in this appeal.

Appeal allowed.

Solicitors for the appellant: Greenspan Partners, Toronto.

Solicitor for the respondent: Attorney General of Ontario, Toronto.

Solicitor for the intervener the Director of Public Prosecutions: Public Prosecution Service of Canada, Halifax.

Solicitor for the intervener the Director of Criminal and Penal Prosecutions: Director of Criminal and Penal Prosecutions, Montréal.

Solicitor for the intervener the Attorney General of British Columbia: Attorney General of British Columbia, Victoria.

Solicitors for the intervener the Criminal Lawyers' Association (Ontario): Brauti Thorning Zibarras, Toronto.

Solicitors for the intervener the Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic: Presser Barristers, Toronto; Markson Law Professional Corporation, Toronto.